

Деление отрезка

Часть 1.

Вводка.

Выбрано число α , и на отрезке $[0,1]$ отмечаются точки $\{\alpha\}, \{2\alpha\}, \{3\alpha\} \dots \{(n-1)\alpha\}$.

Всюду, где прямо не оговорено противное, мы считаем, что α иррационально. Если же $\alpha = p/q$, мы считаем, что $p < q$. Таким образом, каково бы ни было α , никакие две точки не совпадают.

Тем самым отрезок $[0,1]$ разделен на n частей. Далее мы всюду будем считать, что $n > 10$ и $0,3 < \{\alpha\} < 0,7$. Это ограничение несущественно, мы налагаем его, чтобы исключить некоторые тривиальные эффекты для малых чисел. Но из него, в частности, следует, что каждая часть меньше $\{\alpha\}$.

Заметим еще, что если заменить α на $n+\alpha$ или на $n-\alpha$, то части получаются точно такие же. Поэтому в задачах, где вопрос ставится о единственности, делается оговорка: $0 < \alpha < 1/2$.

Содержание задачи – исследовать, какие именно части получаются и как они расположены.

Задачи.

- Отношение длин самого длинного и самого короткого отрезков мы обозначим $L = L(\alpha, n)$.

A1. Пусть α – рациональное число, $\alpha = p/q$. Докажите, что существует n , для которого $L(n) = 1$.

A2. Для каких еще целых или рациональных $k, k > 1$, можно утверждать, что при любом рациональном α существует n такое, что $L(n) = k$?

- Далее мы отказываемся от предположения, что α рационально.

B1. Докажите, что каково бы ни было n , среди частей имеется не более трех различных по длине. (При этом, очевидно, если α иррационально, то разных длин не менее двух).

- При данном α мы будем называть число n «двойным», если при этом n имеется только две разных длины отрезков, и «тройным», если их три.

B2. Докажите, что если α иррационально, то существует бесконечно много двойных и бесконечно много тройных n .

B3. Дано иррациональное число α ; n пробегает значения $n=1, 2, \dots, m$. Докажите, что если $m \rightarrow \infty$, то доля двойных чисел среди них стремится к нулю.

Пусть $\phi(m)$ – количество двойных чисел n среди чисел $n=1, 2, \dots, m$. Оцените скорость, с которой отношение $\phi(m)/m$ стремится к нулю при $m \rightarrow \infty$.

B4. Каким должно быть α , чтобы это отношение стремилось к нулю как можно медленнее? А – чтобы оно стремилось как можно быстрее?

(Достаточно указать несколько примеров, при условии, что эти примеры будут убедительными).

B5. Дайте оценку сверху и снизу для количества двойных чисел среди первого миллиона (желательно, конечно, более или менее точную; оценки «больше трех» не принимаются).

C1. Существует ли число α , для которого $L > 10$ для всех n , начиная с $n=10$?

C2. $n = 2.000.000$. Может ли случиться так, что на некотором полуотрезке $[a, a + \frac{1}{2}]$ лежит более 1.100.000 точек? (Напомним, что по предположению $0,3 < \{\alpha\} < 0,7$).

C3. Существуют ли α , для которых L принимает

(а) бесконечное,

(б) конечное число разных значений, когда n пробегает все значения от 10 до ∞ .

Приведите примеры таких α (если они существуют).

C4. Укажите какие-нибудь достаточные условия для того, чтобы L принимало конечное (бесконечное) число значений. (Если возможно – найдите необходимое и достаточное условие; но можно также ограничиться какими-нибудь условиями).

D1. Докажите, что при любом данном иррациональном α существует такое значение, которое L принимает более тысячи раз (при различных n).

D2. Логически возможны три альтернативы:

(*) каково бы ни было α , существует значение, которое L принимает бесконечное число раз,

(**) каково бы ни было α , L принимает любое значение лишь конечное число раз,

(***) для некоторых α верно одно, а для некоторых другое.

Какая из этих альтернатив верна? Если третья, то для каких α верно первое, а для каких второе?

D3. Допустим, что для некоторого α L принимает значения A , B хотя бы по одному разу (при $n > 10$).

Верно ли, что равносильны утверждения: (*) L принимает значение A конечное число раз, (**) L принимает значение B конечное число раз ?

Деление отрезка (часть 2)

В этой части мы в основном рассматриваем задачи, связанные с конкретными значениями числа α .

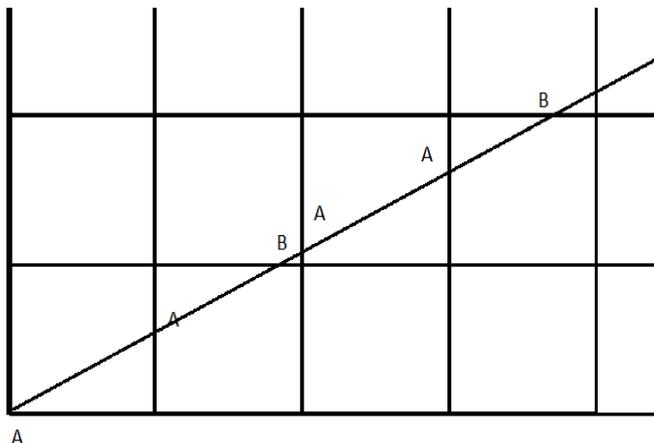
- Обозначим буквой τ золотое сечение: $\tau = \frac{1 + \sqrt{5}}{2} \approx 1,618\dots$

E1. Предлагается три способа выписать последовательность букв ААВААВАВААВ... Докажите, что все три способа дают один и тот же результат (более точно утверждение будет сформулировано ниже).

Способы таковы:

(1) На клетчатой бумаге проведен луч. Он начинается в одном из узлов и проведен под углом $\arctg \tau$ к горизонтальным линиям сетки.

В начальном узле мы пишем букву А, а затем ставим буквы в точках пересечения луча с линиями сетки: букву А на пересечении с вертикальной линией, букву В – с горизонтальной (см. рис.).



(2) Сначала пишется буква А, а затем делается несколько шагов; на каждом шагу буква А заменяется на ААВ, а буква В – на АВ. Например, после трех шагов мы получим:

сначала ААВ,

затем ААВААВАВ,

на третьем шаге ААВААВАВААВААВАВААВАВ.

Докажите, что каждая из получившихся конечных последовательностей является началом последовательности из п. (1).

(3) Отрезок $[0,1]$ разделен указанным в начале (во введении) способом, причем $\alpha = \tau$.

Последовательность получается так: для каждого n , которое является двойным числом, выпишем по порядку длины отрезков, начиная с конца (т.е. от точки 1); длинный обозначается А, короткий – В.

Докажите, что среди получившихся конечных последовательностей есть бесконечно много таких, которые являются началом последовательности из п. (1). Таковы эти последовательности при $n_1 = 3 < n_2 = 8 < \dots$

Е2. Последовательность построена по приведенному выше правилу. Пусть в ней выбрано два куска, по n букв в каждом: от $(k+1)$ -й до $(k+n)$ -й и от $(m+1)$ -й до $(m+n)$ -й буквы. Доказать, что в этих кусках букв А почти поровну, а именно: их количество может отличаться не более чем на 1.

Е3. Найдите еще какую-нибудь последовательность, которую можно аналогично построить тремя (или хотя бы двумя) способами.

- В следующем цикле задач мы полагаем, что $\alpha = \tau$.

Р1. Найдите все возможные значения L (при разных n).

Р2. Какие значения может принимать L , если n – двойное число?

Р3. Найдите все двойные числа.

Р4. Найдите количество двойных чисел среди первого миллиона, если $\alpha = \tau$. Достаточно указать ответ с точностью до 10 процентов.

- В следующем цикле задач мы полагаем, что $\alpha = \sqrt{2} \approx 1,4142\dots$

Т1. Найдите все возможные значения L (при разных n).

Т2. Какие значения может принимать L , если n – двойное число?

Т3. Найдите все возможные значения L еще для какого-нибудь числа (кроме $\alpha = \tau$ и $\alpha = \sqrt{2}$).

К1. Число α неизвестно. Однако известно, что каково бы ни было n , число L принимает только одно из двух значений. При каких α это возможно?

К2. Задача для исследования. Число α неизвестно, однако известно, что при сколь угодно большом n количество точек на любом отрезке длины $\frac{1}{2}$ отличается от $n/2$ не более чем на 10. Что можно сказать о числе α ? В частности:

(а) приведите несколько примеров таких чисел,

(б) приведите какой-нибудь достаточный признак, когда это не так: «если α есть то-то и то-то, то утверждение задачи неверно».

(в) приведите какой-нибудь признак, когда можно утверждать, что количество точек на любом отрезке длины $\frac{1}{2}$ находится в пределах от an до bn для каких-нибудь чисел a, b ($a < \frac{1}{2} < b$, и желательно, конечно, чтобы они были поближе к $\frac{1}{2}$).

К3. Дано рациональное число $\alpha = 113/248$, n принимает значения $n=1, 2, 3 \dots 246$.

Сколько среди этих n встречается двойных чисел, и сколько тройных?

К4. Указать способ, позволяющий для данного рационального α , $\alpha = p/q$, $p < q < 1.000.000$, найти количество двойных и тройных чисел, когда n пробегает значения от 1 до $q-1$, за разумное время (вручную!)

К5. Дано число $L = L(100, \alpha)$.

Как определить, имеется ли для всевозможных n и данного α только конечное, или бесконечное количество различных L ?

В частности, исследовать этот вопрос в случае:

(1) Если L – корень квадратного уравнения с целыми коэффициентами $L^2 + nL + m = 0$,

(2) Если L – корень кубического уравнения с целыми коэффициентами $L^3 + nL^2 + mL + q = 0$.

К6. Известно, что число α разлагается в цепную дробь с первыми знаменателями 3, 5, 12 (т.е. $\alpha = 1/(1+1/(3+1/(5+1/(12+\dots))))$). Найдите все двойные числа между 1 и 100.

Деление отрезка (решения и указания)

A2. Ответ: $L=2$ и $L=3$. Другие числа не годятся, что легко показать на примерах: скажем, если взять $\alpha=5/12$ и $\alpha=4/13$, то у них нет одинаковых значений L , кроме этих двух.

B1. Рассмотрим один из полученных нами на n -м шаге отрезков. Пусть его концы – точки $\{k\alpha\}$, $\{l\alpha\}$. Очевидно, он имеет ту же длину, что отрезки, ограниченные точками $\{(k-1)\alpha\}$ и $\{(l-1)\alpha\}$, $\{(k-2)\alpha\}$, и $\{(l-2)\alpha\}$ и т. д. Поскольку эта серия не может быть бесконечной, в ней есть первый элемент, пусть это $\{(k-s)\alpha\}$ и $\{(l-s)\alpha\}$. Очевидно, есть только три причины, по которым предыдущий отрезок отсутствует:

- либо $k=s$,
- либо $l=s$,
- либо, наконец, отрезок $\{(k-s-1)\alpha\}$, $\{(l-s-1)\alpha\}$ существует, но уже разбит на две части. В этом последнем случае он может разбиваться только точкой $n\alpha$, иначе отрезок с концами $\{(k-s)\alpha\}$, и $\{(l-s)\alpha\}$ тоже был бы уже разбит.

Первые две серии существуют всегда, а третья может и не существовать. В зависимости от этого мы имеем либо 2, либо 3 серии, все отрезки в каждой из них равной длины, что и требуется.

Отсюда видно также, что отрезки третьей серии (если они существуют) по длине равны сумме отрезков двух других серий. Таким образом, длины отрезков всегда равны $a < b < (a+b)$, причем третьей длины может и не быть.

Отсюда видно также, что новая точка всегда делит самый длинный отрезок $a+b$ на части a , b (в противном случае у нас бы возникло 4 разных длины, что невозможно).

Исследуем теперь вопрос о том, как меняется число L при переходе от n к $n+1$. Из сказанного выше видно, что число n остается тройным до тех пор, пока имеются отрезки типа $(a+b)$, а в тот момент, когда последний такой отрезок исчезает, остаются только a и b , т.е. число становится двойным.

Утверждение. (а) Если n и $n+1$ – тройные числа, то L не меняется.

(б) При переходе от тройного числа к двойному (n – тройное, $(n+1)$ – двойное) L заменяется на $L-1$.

(в) Переходов от двойного числа к двойному не бывает.

(г) При переходе от двойного числа к тройному возможны два случая. Пусть $a < b$ – длины коротких и длинных отрезков для n . Тогда:

(г1) если $a < b/2$, то L не меняется,

(г2) если $a > b/2$, то L заменяется на число $L/(L-1)$.

В самом деле:

(а) в первом случае как были, так и остаются отрезки трех длин: a , b , $a+b$.

(б) во втором случае исчезает последний отрезок длины $(a+b)$, остаются только $a < b$, и если раньше было $L=(a+b)/a$, то теперь $L=b/a$.

(в) В третьем случае надо вспомнить наше предположение о том, что $n > 10$ и $0,3 < \{\alpha\} < 0,7$ (без этого утверждение неверно)

(г) оба случая (г) рассматриваются так же, как (а) и (б).

B3. Из рассуждений в решении задачи B1 видно, что вслед за одним двойным числом следует столько тройных, сколько было отрезков наибольшей длины. Поскольку общее число отрезков неограниченно возрастает, довольно очевидно, что также и число отрезков наибольшей длины стремится к бесконечности, что и требуется.

B5. Оценка сверху: не более 500.000 – и она не улучшается. Чтобы получить такое количество двойных чисел, нужно взять $\alpha = 1/2 - \varepsilon$, $\varepsilon < 1/1000000$. В этом случае легко заметить, что каждое второе число – двойное.

Отсюда также видно, что доля двойных чисел может стремиться к нулю довольно медленно. А именно, пока что у нас получилось много двойных чисел в первом миллионе, зато потом они пойдут редко – через миллион или более. Но если мы возьмем, далее $\alpha = 1/2 - 1/1000000 - \varepsilon$, $\varepsilon < 1/1000000000000000000$, то окажется, что они очень долго будут идти с частотой «один на миллион», т.е. до поры до времени их доля остается стабильной. Ясно, что подобную конструкцию можно строить и дальше, взяв, к примеру, $\alpha = 1/2 - 1/10^6 - 1/10^{(10^6)} - \varepsilon$ и т.д. При этом на каждом переходе доля двойных чисел, правда, очень резко уменьшается, но зато после этого **ОЧЕНЬ**, **ОЧЕНЬ** долго остается неизменной. Именно это и означает, что последовательность стремится к нулю медленно.

Что касается наиболее быстрого стремления доли к нулю, то есть числа α , для которых эта доля убывает логарифмически (примеры будут ниже), и это, видимо, максимальная скорость. Это высокая скорость убывания, поскольку это означает, что в первом миллионе имеется всего лишь около $\ln 1000000$ двойных чисел.

C1. Ответ. Нет, не существует, поскольку из формул, по которым преобразуется число L , видно, что оно всегда принимает значения меньше 2.

C2. Ответ, да. Вот пример. Пусть $\alpha = 1/3 + \varepsilon$, где ε очень мало. Тогда все два миллиона точек лежат вблизи трех точек: точки 0, точки $1/3$ и точки $2/3$. Соответственно на полуотрезке $[0,3 \ 0,8]$ лежит примерно две трети всех точек, что много больше, чем 1.000.000.

C3. Да, существуют те и другие.

Например, если $L = \sqrt{2}$, то L принимает всего лишь 3 разных значения (подробнее этот пример разбирается ниже). С другой стороны, если L принимает какое-нибудь трансцендентное значение (к примеру, L равно числу пи), то заменяя L то на $L-1$, то на $L/L-1$, мы, очевидно, будем все время получать разные числа, т.е. их будет бесконечно много.

C4. Указание. Если L принимает лишь конечное число значений, то в какой-то момент значения L «выходят на цикл»: вновь повторяется значение, которое L принимало раньше.

Но если после нескольких преобразований (которые, напомним, имеют вид либо $L \rightarrow L-1$, либо $L \rightarrow L/L-1$) мы вновь получим значение L , которое уже встречалось, то L , как нетрудно убедиться, удовлетворяет квадратному уравнению с целыми коэффициентами.

Итак, это условие является необходимым, и соответственно, если L не является корнем такого уравнения (к примеру, если L трансцендентно), этого достаточно, чтобы L принимало бесконечно много значений.

Достаточным условием для того, чтобы L принимало конечное число значений является, например, условие:

$$L^2 - (n+2)L + n = 0.$$

Таковы, в частности, числа $\sqrt{2}$ и τ , рассматриваемые в задачах ниже.

D1. L принимает подряд одно и то же значение до тех пор, пока мы имеем дело с тройным числом, иными словами – столько раз, сколько «длинных» отрезков появилось на очередном ходе. Но их число стремится к бесконечности (как уже указывалось в решении задачи B3)

Очевидно, что когда общее число отрезков стремится к бесконечности, то и число «длинных» отрезков стремится к бесконечности

D2. Справедлива третья альтернатива.

D3. Нет, неверно.

Пусть, например, таково, что L вначале принимает значение $(100+\sqrt{2})/(99+\sqrt{2})$. Поскольку это число меньше 2, следующее значение L будет вычисляться по формуле $L/(L-1)$, то есть следующее L равно $100+\sqrt{2}$. Далее L последовательно будет принимать значения $99+\sqrt{2}$, $98+\sqrt{2}$, ... $\sqrt{2}$. После этого L принимает только значения $\sqrt{2}$, $\sqrt{2}+1$, $\sqrt{2}+2$ (и никакие другие), и эти значения принимаются бесконечное число раз.

E1. Будем сводить первое и третье определение ко второму.

Первое. Поднимем точку A , лежащую на k -й вертикали, на k единиц вверх. Очевидно, все эти точки попадают на одну прямую, которая уже образует с горизонталью угол $\arctg t$ (a не $\arcsctg t$). С другой стороны, если мы расставим после этого все точки B , как положено, то между каждыми двумя A появляется ровно одна точка B . Сделаем к тому же второе преобразование: все буквы A заменим на B , все буквы B – на A .

Таким образом, наша последовательности преобразуется по закону: A заменяется на BA , B заменяется на A . И в результате, очевидно, наша последовательность не изменится, поскольку если мы теперь отразим чертеж относительно диагонали (прямой $y=x$), то наш луч вернется на прежнее место. Остается заметить, что если произвести нашу операцию дважды, то как раз и получится, что A заменяется на AAB , B – на AB , а последовательность опять-таки не меняется.

Замечание. Фактически мы установили, что преобразование $A \rightarrow AAB$, $B \rightarrow AB$ “можно представить как произведение”: сделав сначала преобразование $A \rightarrow BA$, $B \rightarrow A$, а затем $A \rightarrow AB$, $B \rightarrow A$, мы получим данное.

Третье. Рассуждаем сходным образом. Пусть N – двойное число. Это значит, что имеется r длинных отрезков длины a и s коротких отрезков длины a/τ , $r+s=N$. Тогда следующее двойное число $M = N+r$, и продвигаясь к нему, мы делим каждый длинный отрезок на короткий и «самый короткий» длины еще в τ раз меньше.

Когда этот «цикл» закончен, мы обязаны объявить бывший короткий отрезок – длинным. При этом попеременно «бывший длинный» отрезок разбивается то на «длинный - короткий», то на «короткий - длинный». Это как раз преобразования, описанные в замечании к предыдущему рассуждению. Отсюда, кстати, видно, почему не все двойные числа годятся: их приходится брать через одно, чтобы получить «квадрат» этого преобразования.

E2. Воспользуемся первым из трех определений. Предположим, что утверждение неверно. Тогда на луче существуют два отрезка, на которых равное число букв, но на одном на 2 или более буквы B больше, чем на втором (a букв A , соответственно, меньше).

Но если на одном из отрезков на 2 буквы B больше, то его проекция на вертикальную прямую больше. Соответственно, если на нем на две буквы A меньше, то меньше и его проекция на горизонталь. Противоречие очевидно.

E3. Указание. Ключевым моментом в решении задачи E1 было то, что «поднимая» точки пересечения луча с вертикалями на соответствующее число единиц, мы получаем луч, симметричный исходному. Но можно поднять точку, лежащую на k -й вертикали, не на k , а на $2k$ единиц; легко убедиться, что полученный луч будет симметричен исходному, если α удовлетворяет уравнению $\alpha^2 + 2\alpha - 1 = 0$.

Понятно, что есть и другие возможности.

P1, P2. Если $n=2$, то имеется два отрезка, и их отношение есть золотое сечение. Далее, согласно формуле, приведенной в начале (решение задачи B1), L может быть заменено только на $L/(L-1) = L^2 = L + 1$. Следующее его значение будет $(L+1)-1 = L$, и т.д. Отсюда видно, что L принимает только два значения, а если к тому же n – двойное, то L принимает единственное значение $L = \tau$.

P3, P4. Ответ: двойные числа для данного α есть числа Фибоначчи, т.е. числа 2, 3, 5, 8, 13... (каждое следующее равно сумме двух предыдущих).

k -е число Фибоначчи приближенно равно τ^k , и их количество в первом миллионе приблизительно равно $\log 1.000.000$ по основанию τ , то есть около 28.

Можно, конечно, честно выписать первые 30 чисел Фибоначчи. 28-е число равно 832 040, а 29-е уже больше миллиона.

T1, T2. Задача аналогична предыдущей. Поскольку начальное значение L (при $n=2$) равно $(2-\sqrt{2})/(\sqrt{2}-1) = \sqrt{2}$, то все дальнейшие значения L будут равны либо $\sqrt{2}$, либо $\sqrt{2}+1$, либо $\sqrt{2}+2$ (при двойных n – только первые два варианта).

K1. Из предыдущих рассуждений видно, что L должно удовлетворять соотношению $L/(L-1) - 1 = L$, откуда L – золотое сечение. Отсюда нетрудно найти α .

K3. Указание. Разложим данное число в цепную дробь (для числа $113/248$ она имеет вид $1/(2+1/(5+1/(7+1/3)))$). Тогда двойные числа встречаются через k , где k – знаменатели частных цепных дробей для основной, то есть дробей $1, 1/2, 1/(2+1/5)=5/11, 1/(2+1/(5+1/7))=36/79$ и т.д. Итак, двойные числа встречаются вначале через 1 (т.е. каждое – при $n=2$ и $n=3$), затем идет “серия” двойных, встречающихся через 2, потом серия через 11 и через 79. При этом количество двойных чисел в серии равно очередному знаменателю исходной дроби, т.е. в первой серии их 2, затем 5 и 7.

Если бы число α было иррациональным, так продолжалось бы до бесконечности, но для рационального числа в конце закономерность иная: все числа, начиная с 169 – двойные.

Ответ:

(*) число 2,

(**) числа 3, 5, 7, 9, 11,

(***) числа 13, 24, 35 и т.д., до 90,

(****) Наконец, все числа от 169 до 248.

The division of segment

Preliminary.

Let some number α be chosen, and one marks points $\{\alpha\}, \{2\alpha\}, \{3\alpha\} \dots, \{(n-1)\alpha\}$ on segment $[0,1]$.

If the contrary isn't expressly stated, we assume that α is irrational. If $\alpha = p/q$, we assume that $n < q$. Thus, whatever α is, points do not coincide.

Thus, segment $[0,1]$ is divided into n parts. Moreover let us assume that $n > 10$ and $0.3 < \{\alpha\} < 0.7$. This limitation is irrelevant, we impose it to exclude some trivial effects for small numbers. It means, in particular, that each part of division is less than $\{\alpha\}$.

Note also that if you replace α by $n+\alpha$ or $n-\alpha$, then you get the same parts. So when the question concerns uniqueness, we suppose that $0 < \alpha < 1/2$.

The content of the task is to investigate what parts we get and how they are located.

The tasks.

The ratio of the lengths of the longest and the shortest segments, we denote by $L = L(\alpha, n)$.

A1. Let α be the rational number, $\alpha = p/q$. Prove that there exist n for which

$L(n) = 1$.

A2. Does there exist some other integer or rational $k, k > 1$, for which one may state that for any rational α there exist n such that $L(n) = k$?

Now we reject the assumption that α is rational.

B1. Prove that for any n , there exist only 3 or less parts of different length. (Obviously, if α is irrational, there are two or more different lengths).

For given α we call the number n "double number", if there are only two different lengths of segments, and "triple number" if there are three of them.

B2. Prove that if α is irrational, then there exist infinitely many double and infinitely many triple n .

B3. Given the irrational number α ; n runs values $n=1, 2, \dots, m$. Prove that if m tends to infinity, the ratio of double numbers among them tends to zero.

Let $\varphi(m)$ be a number of double numbers n among the numbers $n=1, 2, \dots, m$. Rate the speed with which the ratio $\varphi(m)/m$ tends to zero as m tends to infinity.

B4. For what numbers α this ratio tends to zero maximally slowly? And what numbers α this ratio tends to zero maximally quickly?

(You may simply give a few examples, provided that these examples will be convincing).

B5. Estimate from above and from below the number of double numbers

if $1 < n < 1.000.000$. (preferably, of course, more or less accurate; estimations like "more than three" are not accepted).

C1. Is there a number α , such that $L = L(n) > 10$ for all $n > 9$?

C2. Let $n = 2.000.000$. Can it happen that some interval $[a, a + \frac{1}{2}]$ contains more than 1.100.000 points? (Recall the assumption $0.3 < \{\alpha\} < 0.7$).

C3. Does there exist α , for which L takes

(a) the infinite,

(b) a finite number of different values, when n runs all the values from 10 to infinity.

Give examples of such α (if they exist).

C4. Find some sufficient conditions for L to take only the final (infinite) number of values. (If possible - find necessary and sufficient condition; but you can also give some sufficient conditions).

D1. Prove that for any given irrational α there exists such a value A that $L(n) = A$ more than thousand times (for different n).

D2. Logically, there are three possible alternatives:

(*) for any α there exists such value A that $L = A$ an infinite number of times,

(**) for any α and for any A , $L(n) = A$ only for finite number on n ,

(***) for some α , the first variant is true, and for some α the second.

Which of these alternatives is correct? If the third, for which α the first is true and for which – the second one?

D3. Assume that for some α L takes both values A and B at least once (for $n > 10$).

Is it true that the assertions:

(*) L takes the value A only finite number of times and

(**) L takes the value B only finite number of times

are equivalent?

P4. How many double numbers are in the interval $1 < n < 10^6$? It is sufficient to give answer up to 10%.

- In the next set of problems we assume that $\alpha = \sqrt{2} \approx 1,4142\dots$.

T1. Find all possible values of L (for different n).

T2. What values are possible for L if n is a double number?

T3. Find all possible values of L for some other α (except $\alpha = \tau$ and $\alpha = \sqrt{2}$).

Various problems

K1. You don't know α , but you know that for any $n > 10$, the number L takes only one of the two values. For which α it is possible?

K2. Let L takes some value A for some n. Prove that it takes the same value A for some double number n.

Let us formulate a «converse» statement: if L takes some value A for some n, than it takes the same value A for some triple number n. Is it true?

K3. **A problem for investigation.** You don't know α but you know that for any n the number of points on every segment of length $\frac{1}{2}$ differs from $n/2$ by at most 10. What is possible to say about number α ? In particular:

(a) give a few examples of such α ,

(b) give some sufficient condition when the situation differs: «if α is such and such, than the statement is false»,

(c) give some condition which enables us to assert that the number of points on every segment of length $\frac{1}{2}$ is between an and bn for some $a < \frac{1}{2} < b$ (desirably a, b are close enough to $\frac{1}{2}$).

K4. How many double and triple numbers are among $n=1, 2, 3\dots 246$ if $\alpha = 113/248$?

K5. Find some method that enables you to find in a reasonable time without a computer the quantity of double and triple numbers for α rational, $\alpha = p/q$, $p < q < 1.000.000$ ($n = 1, 2\dots q-1$).

K6. Given the value of L if $n=100$: $L(100) = A$. Is it possible to determine whether L takes finite or infinite number of values for all n and given fixed α ?

In particular, investigate the cases:

(1) A is a root of square equation with integer coefficients $A^2 + qA + r = 0$,

(2) A is a root of cubic equation with integer coefficients $A^3 + qA^2 + rA + s = 0$.

K7. It is known that number α decomposes in continued fraction and its first denominators are 3, 5, 12 (i.e. $\alpha = 1/(1+1/(3+1/(5+1/(12+\dots))))$). Find all double numbers between 1 and 100.

Алгоритмы и лабиринты

А.Я.Белов-Канель, И.А.Гажур, И.А.Иванов-Погодаев, А.С.Малистов

Цикл А. Это вводный цикл. Его задачи являются вспомогательными и будут сняты после промежуточного финала.

В первом (вводном) цикле задач изучается стандартный конечный автомат: робот, перемещающийся по клеточной плоскости. Робот — это механизм, производящий заранее определенный набор действий по определенной программе. Робот может делать следующее:

1. Перемещаться вперед (в соседнюю клетку);
2. Поворачиваться на месте на 90 градусов;
3. Ставить флажок в клетку, где находится (если флажок у него есть);
4. Проверять наличие флажка в своей клетке.
5. Брать флажок из своей клетки.

Наличие у робота флажков (и их количество) оговаривается заранее. Программа состоит из пронумерованного упорядоченного набора инструкций для робота, причем некоторые инструкции могут заключаться в переходе к другой инструкции. Мы будем ставить для робота задачи обхода, состоящие в том, чтобы обойти, то есть побывать в каждой клетке некоторой области. Сначала выясним некоторые возможности робота.

Пример. Докажем, что робот с двумя флажками может обойти ленту — бесконечную полосу с шириной в 1 клетку. Пусть в начале робот находится в клетке с номером 0 с двумя флажками. Построим программу робота.

- ▷ 1. Поставить флажок.
- ▷ 2. Перейти в клетку 1.
- ▷ 3. Поставить флажок.

Теперь нужно организовать «челночное» движение робота между флажками, с попутным увеличением расстояния между ними. То есть, середина отрезка между флажками остается на месте, а флажки робот «расталкивает» в разные стороны. Этого добиваемся с помощью следующей программы:

- ▷ 4. Повернуться на месте 2 раза. (разворачиваемся на 180 градусов)
- ▷ 5. Пройти вперед.
- ▷ 6. Проверить наличие флажка.
- ▷ 7. Если флажка нет — перейти к 5.
- ▷ 8. Взять флажок и перейти на одну клетку вперед.
- ▷ 9. Положить флажок и перейти к 4.

Легко видеть, что робот побывает в каждой клетке ленты.

Интересен вопрос, может ли робот без флажков обойти ленту? Ответ — нет. Чтобы доказать это, необходимо формализовать конструкцию робота. Ясно, что действие, которое робот выполнит в следующий момент, полностью зависит от номера инструкции, которую должен выполнить в данный момент робот и от наличия-отсутствия в клетке флажка. Назовем эти факторы *внутренним состоянием робота*. Ясно, что у робота конечное число возможных внутренних состояний. Выполнив какое-либо действие, робот, вообще говоря, его меняет. По принципу Дирихле, через какое-то время внутреннее состояние робота повторится. Пусть, прошло t секунд и, по сравнению с первым моментом, когда у него было такое состояние, робот сдвинулся вправо на расстояние a . Отметим, что прошло конечное время, и поэтому существует клетка K , левее начальной, где робот еще не был. Поскольку состояние робота такое же, как t секунд назад, еще через t секунд робот сдвинется еще на a вправо, опять не посетив эту клетку. Легко видеть, что далее робот будет действовать, периодически сдвигаясь вправо, и клетку K он не посетит никогда.

А0. Докажите, что робот с одним флажком ленту обойти не сможет.

Указание. Рассмотрите отдельно случаи: 1) когда робот не удаляется от флажка на расстояние большее некоторого N ; и 2) когда робот отходит от флажка сколь угодно далеко.

А1. Докажите, что робот с 4 флажками может обойти плоскость.

А2. Докажите, что робот с 3 флажками может обойти плоскость. Может ли робот с 3 флажками обойти трехмерное пространство?

А3. Пусть некоторые границы клеток непроходимы для робота. Робот может видеть барьеры между клетками (проверять на их наличие любую из сторон клетки, где он находится). Пусть непроходимая для робота линия делит плоскость на полуплоскости. Докажите, что робот с 1 флажком может обойти полуплоскость.

А4. Докажите, что робот с 1 флажком не может обойти плоскость с четырьмя разрезами (рисунок 1), а с двумя флажками — может.

А5. Пусть робот ходит по вершинам графа (возможно, бесконечного).

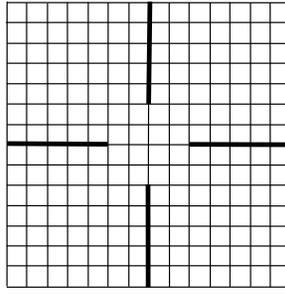


Рис. 1: Четыре разреза на бесконечной плоскости

а) Докажите, что робот с 1 флажком не может обойти бесконечное дерево (граф без циклов), каждая вершина которого имеет степень 3.

б) Докажите, что робот с 2 флажками не может обойти дерево (граф без циклов), каждая вершина которого имеет степень 3.

А6. Докажите, что робот с 2 флажками не может обойти плоскость.

Указание. Используйте идеи, применяющиеся при доказательстве в А0, А4.

Пусть робот без флажков движется в первой четверти плоскости. Границы (оси координат — непроходимые стенки и робот может их обнаруживать).

А7. Пусть в начале робот находится в клетке с координатами $(2^n, 0)$. Составьте универсальную по n (независящую от n) программу, переводящую робота в клетку $(3^n, 0)$ с последующей остановкой в ней.

Указанный в этой задаче переход будем называть *переходом от 2^n к 3^n* .

А8. По аналогии с предыдущей задачей, осуществите следующие переходы:

а) от 2^n к 6^n ;

б) от 2^n к 2^{2^n} ;

с) от $2^n \cdot 3^m$ к $2^n \cdot 3^m \cdot 5^{mn}$;

д) от $2^n \cdot 3^m$ к $2^n \cdot 3^m \cdot 5^{m+n}$;

е) от 2^n к $2^{\lfloor \sqrt{n} \rfloor}$;

ф) от 2^n к 2^{n^2} ;

г) от 2^n к 2^{k_n} , где k_n есть n -ая цифра десятичного разложения $\sqrt{2}$;

з) от 2^n к 2^{k_n} , где k_n есть n -ая цифра десятичного разложения π ?

А9. Докажите, что робот с 3 флажками может обойти n -мерное клеточное пространство.

А10. Докажите, что робот с 3 флажками может обойти бесконечное дерево, каждая вершина которого имеет степень 3.

Алгоритмы крестьянина.

Есть *мир* — ограниченное подмножество клеточной плоскости, неизвестных заранее размеров. Каждая клетка плоскости относится к одному из следующих типов:

1. Скала. Клетка, недоступная для посещения.

2. Земля. Клетка доступна для посещения.

3. Озеро. Клетки недоступны для посещения. В таких клетках можно ловить рыбу, находясь в соседней по стороне клетке. С каждой клеткой-озером связаны параметры *nibble* — клев (количество рыбы, которое вылавливается из озера за 1 раз, при применении операции лова рыбы) и *fish* — количество оставшейся в озере рыбы.

4. Дом. Уникальная клетка в мире, доступна для посещения, обычно крестьянин находится в начале в ней. Часто требуется отнести пойманную рыбу в дом.

Крестьянин перемещается по миру, переходя из клетки в клетку. Находясь в клетке, он смотрит в одну из четырех сторон (направление движения).

Областью действия крестьянина будем называть множество из двух элементов: клетку, где крестьянин находится, и клетку перед ним (соседнюю по направлению движения).

Крестьянину доступна информация о клетках из области действия. Информация о других клетках мира ему недоступна. У крестьянина есть ограниченное условиями задачи количество флажков. Он может оставлять флажки в клетках и таким образом исследовать мир. Кроме того, находясь в соседней с озером клетке, крестьянин может ловить рыбу. У него может быть при себе некоторое количество рыбы, не превышающее 10 кг.

В клетках мира могут находиться разные объекты (флаги, рыба). С объектами может быть связано несколько переменных, информация о которых доступна крестьянину. Переменные, связанные с флагами, крестьянин может менять, в том числе можно создавать новые переменные и изменять их значения.

Крестьянин обладает ограниченной памятью. Он может создавать собственные переменные и изменять их значения. Значения собственных переменных доступны крестьянину независимо от клетки, где он находится.

Формально, крестьянин может совершать следующие действия:

1. [Go] Переместиться вперед.
2. [Rotate] Повернуться на месте в любую из четырех сторон.
3. [Read] Получить информацию о переменных, связанных с объектами в клетках области действия.
4. [SetFlag] Поставить флажок в клетку области действия или убрать флажок из нее. Также можно создавать переменные, связанные с флагом, и изменять их значения.
5. [CheckFlag] Проверить наличие флажка в области действия.
6. [Fishing] Ловить рыбу в клетке перед ним.
7. [GetPutFish] Оставлять и забирать рыбу в области действия.
8. [Write] Создавать собственную переменную и изменять ее.
9. [Math] Проводить арифметические и логические операции над переменными. В частности, можно проверить равенство некоторых переменных.

Течение времени. Время течет дискретно, по тактам. Если не указано иного, выполнение Go, Fishing и GetPutFish прерывают текущий такт времени (происходит переход на следующий такт). Остальные операции Rotate, Read, SetFlag, CheckFlag, Write, Math не занимают времени, но если в текущем такте выполняется 500 таких операций, такт прерывается. Кроме того, выполнение SetFlag второй раз за такт прерывает текущий такт.

В задачах ниже требуется предъявить алгоритм крестьянина для их решения. Алгоритмы (в виде блок-схем) можно составлять и запускать в специальной программе «VillagerLife», доступ к которой вы получите.

В каждой задаче существует предельное допустимое время работы алгоритма. Размер карты заранее неизвестен. Если не сказано иное, крестьянин умеет определять край карты (если находится на краю). Под обходом карты мы понимаем посещение каждой ее клетки.

Цикл В. В этом цикле запрещается использовать собственные переменные.

V1. С помощью четырех флагов обойти конечное прямоугольное поле без скал и озер, при условии, что крестьянин не умеет определять, что находится на краю.

V2. На карте без скал и озер стоят два флага: один в клетке с координатами $(x, 0)$, второй в клетке с координатами $(0, y)$. Третий флаг находится у крестьянина, который стартует в начале координат. Требуется установить любой флаг в клетку с координатами $(x + y, 0)$. x, y – положительные числа.

V3. Пусть теперь могут быть скалы и озера. Обойти карту с произвольным числом флажков (поставить флаг в каждую доступную клетку).

V4. Решить задачу V3 за $2n$ тактов, где n – число доступных клеток.

Цикл С. В этом цикле разрешено использовать собственные переменные.

S1. Найти число доступных клеток и записать его в переменную SPACE. Потратить на это не более $2n$ тактов, где n – число доступных клеток.

S2. Найти число клеток-озер, доступных со стартовой позиции и записать его в переменную WATER.

S3. Найти кратчайшее расстояние из начального положения до флага, в котором переменная TARGET=THIS. Записать ответ в переменную DIST.

S4. Найти клетку-озеро с наибольшим клевом. Записать координаты клетки в переменные NIBBLE_X и NIBBLE_Y, а само значение клева в переменную NIBBLE.

S5. Для каждой клетки-озера определим параметр полезности равный максимальному удельному количеству рыбы, которое можно принести домой (отношение максимального количества рыбы, которое можно взять в озере, к минимальному количеству тактов, требующихся для ловли и доставки домой). Найти клетку-озеро с наибольшей полезностью. Записать координаты клетки в переменные USEFULNESS_X и USEFULNESS_Y, а само значение полезности в переменную USEFULNESS.

S6. Накопить n кг рыбы в доме. Значение n записано в переменной FishReq, связанной с домом.

S7. На карте есть дом с другим крестьянином, который тоже умеет ловить рыбу (но не умеет воровать ее из нашего дома). Требуется накопить n кг рыбы в доме. Значение n записано в переменной FishReq, связанной с домом.

S8. На карте есть дом с другим крестьянином, который тоже умеет ловить и воровать рыбу. Требуется накопить n кг рыбы в доме. Значение n записано в переменной FishReq, связанной с домом.

Алгоритмы и лабиринты. Дополнительные задачи.

А.Я.Белов-Канель, И.А.Гажур, И.А.Иванов-Погодаев, А.С.Малистов

Цикл А.

A11. (Предложил И.Митрофанов) На плоскости в произвольных клетках находятся два робота, каждый с двумя флажками. Можно ли задать каждому программу так, что при синхронном запуске роботы через какое-то время встретятся?

A12*. Аналогичный A11 вопрос для случая, когда роботы расположены в произвольных точках трехмерного пространства.

A13. Пусть есть лабиринты L_1, L_2 и программы P_1, P_2 для робота без флажков, что робот с программой P_i обходит L_i . Верно ли, что существует программа, обходящая каждый из лабиринтов L_1, L_2 ?

A14. Может ли робот с четырьмя флажками обойти n -мерное пространство за полиномиальное время? Обходом за полиномиальное время называется такой обход, когда существуют такие k и C , что любая клетка на расстоянии d от начала обхода будет посещена роботом через время не большее, чем $C \times d^k$ после старта обхода.

A15*. Может ли робот с тремя флажками обойти n -мерное пространство за полиномиальное время?

Цикл С.

C9. Удалить все флаги с карты. В конце записать в переменную FINISH значение 1.

C10. На карте есть озеро. Найти кратчайший путь вокруг озера (петлю, содержащую озеро внутри). В конце записать длину пути в переменную PATH.

Возможно, будут добавлены еще задачи. Следите за обновлениями.

Алгоритмы и лабиринты. Решения А0-А10

А. Я. Белов -Канель, И. А. Гажур, И. А. Иванов -Погодаев, А. С. Малистов.

10 августа 2014 г.

Проведем исследование возможностей робота, из которого будут следовать решения задач А0-А10.

Упражнение. а) Если Робот движется вдоль клетчатой прямой, то он не покинет некоторого луча.

б) Если же Робот гуляет по клетчатой плоскости, то он не покинет полуполосу ограниченной ширины, расположенной вдоль прямой L с рациональным углом наклона. Угловым коэффициентом этой прямой равен бесконечности или есть рациональное число $\alpha = p/q$, и если p/q - несократимо, то $|p| + |q|$ не превосходит числа состояний Робота.

Под *обходом* бесконечного графа Γ мы будем понимать такое поведение Робота, что для любой вершины Γ он рано или поздно в нее попадет. Поведение одного Робота обычно тривиально и мы будем снабжать его флажками. Робот может нести с собой один или несколько флажков, оставлять флажок в вершине и проверять, находится ли рядом флажок и если да – то забирать его с собой. С помощью двух флажков Робот может обойти всю клетчатую ленту: он будет курсировать между ними и их расталкивать (см. рис.).

Приведем программу:

1. ВПЕРЕД; 2. ЕСЛИ РЯДОМ ФЛАГ ТО ВЗЯТЬ ИНАЧЕ ГОТО 1; 3. ВПЕРЕД; 4. ПОЛОЖИТЬ ФЛАГ; 5. РАЗВЕРНУТЬСЯ; 6. ГОТО 1;

Плоскость обходится с помощью трех флажков аналогично. Они помещаются в вершинах равнобедренного прямоугольного треугольника и расталкиваются (см.рис.)

Упражнения. а) Напишите соответствующую программу.

б) Напишите программу обхода полуплоскости для Робота с одним флажком. (Указание. см. рис.)

Интересно, что ни неограниченную плоскость, ни ограниченную с двух сторон полосу нельзя обойти с помощью только одного флажка!

Доказательства невозможности осуществить обход используют идею виртуального автомата. Рассмотрим для примера клетчатую прямую – т.е. полосу единичной ширины. Случаи полосы ширины k , а также неограниченной плоскости аналогичны и будут предоставлены читателю. Итак, почему Робот с одним только флажком не сможет обойти всю клетчатую прямую?

Возможны два случая.

Случай 1. Робот удаляется от своего флажка сколь угодно далеко.

Случай 2. Расстояние между Роботом и флажком ограничено.

В первом случае рассуждения те же, что и в задаче про закраску только центра листа: если Робот далеко уйдет от флажка, больше чем на $10 \cdot x$, x – число состояний, то какое-то состояние повторится в процессе удаления дважды, причем к моменту повторения он удалится от флажка. Причем в промежутке между этими повторениями он не встретит флажок. Но тогда Робот будет неограниченно удаляться от своего флажка и значит, обойдет не больше полупрямой.

Идея виртуального автомата возникает во втором случае. Если расстояние между Роботом и флажком ограничено, то система Робот–флажок имеет конечное число состояний (не больше чем число внутренних состояний Робота \times максимальное расстояние). Эта система и есть виртуальный автомат. Он конечен, а для конечного автомата невозможность обойти ленту уже доказана.

Упражнения. а) Уточните рассмотрение случая 1. Докажите, что если Робот удалится на расстояние $x + 1$ от флажка, то он будет удаляться от него неограниченно. (Указание. Рассмотрите положения Робота в период, заканчивающийся положением на расстоянии $x + 1$ от флажка и начинающийся моментом, когда он перед этим последний раз отойдет от флажка.)

б) Докажите, что Робот с одним флажком на неограниченной плоскости не покинет полуполосы ограниченной ширины. Докажите также, что числитель и знаменатель углового коэффициента наклона ограничены кубом числа внутренних состояний Робота.

Упражнение. Изучается поведение Робота с двумя флажками на неограниченной плоскости. Докажите, что существует программа, позволяющая

а) Обойти внутренность угла 90° .

б) Посетить все внутренние клетки заданного угла ,меньшего развернутого. (Возможно, что при обходе придется выходить за его пределы.)

Доказательства невозможности осуществить обход используют идею виртуального автомата. Рассмотрим для примера клетчатую прямую – т.е. полосу единичной ширины. Случаи полосы ширины k , а также неограниченной плоскости аналогичны и будут предоставлены читателю. Итак, почему Робот с одним только флажком не сможет обойти всю клетчатую прямую?

Возможны два случая.

Случай 1. Робот удаляется от своего флажка сколь угодно далеко.

Случай 2. Расстояние между Роботом и флажком ограничено.

В первом случае рассуждения те же, что и в задаче про закраску только центра листа: если Робот далеко уйдет от флажка, больше чем на $10 \cdot x$, x – число состояний, то какое-то состояние повторится в процессе удаления дважды, причем к моменту повторения он удалится от флажка. Причем в промежутке между этими повторениями он не встретит флажок. Но тогда Робот будет неограниченно удаляться от своего флажка и значит, обойдет не больше полупрямой.

Идея виртуального автомата возникает во втором случае. Если расстояние между Роботом и флажком ограничено, то система Робот–флажок имеет конечное число состояний (не больше чем число внутренних состояний Робота \times максимальное расстояние). Эта система и есть виртуальный автомат. Он конечен, а для конечного автомата невозможность обойти ленту уже доказана.

Упражнения. а) Уточните рассмотрение случая 1. Докажите, что если Робот удалится на расстояние $x + 1$ от флажка, то он будет удаляться от него неограниченно. (**Указание.** Рассмотрите положения Робота в период, заканчивающийся положением на расстоянии $x + 1$ от флажка и начинающийся моментом, когда он перед этим последний раз отойдет от флажка.)

б) Докажите, что Робот с одним флажком на неограниченной плоскости не покинет полуполосы ограниченной ширины. Докажите также, что числитель и знаменатель углового коэффициента наклона ограничены кубом числа внутренних состояний Робота.

Упражнение. Изучается поведение Робота с двумя флажками на неограниченной плоскости. Докажите, что существует программа, позволяющая

а) Обойти внутренность угла 90° .

б) Посетить все внутренние клетки заданного угла, меньшего развернутого. (Возможно, что при обходе придется выходить за его пределы.)

Итак, значительный кусок плоскости, почти что половину, с помощью двух флажков посетить можно! Оказывается, однако, что всю неограниченную плоскость двумя флажками не посетить. Более того, множество положений Робота и флажков за всю историю можно покрыть углом, строго меньшим развернутого в то время как ограниченную полуплоскость – т.е. внутренность развернутого угла обойти можно! И необходимый минимум для обхода плоскости – три флага. Чтобы это доказать, нужны новые идеи, которые мы извлечем из решения более простых задач.

Одна из идей состоит в том, чтобы определять состояние системы Робот–флажок–лабиринт не вообще, а в подходящий момент. Вот два примера работы этой идеи:

Задача. На плоскости проведено 4 барьера, непроходимых для Робота, но распознаваемых им. (см. рис.) Может ли Робот все обойти?

Докажем невозможность. Для этого достаточно заметить, что Робот бесконечно много раз должен пройти через одно из центральных полей – иначе начиная с какого-то момента он будет все время находиться только в одной четвертинке и нигде больше.

Но тогда повторится его состояние в момент прохождения этого поля и Робот будет все время топтаться на месте!

Упражнения. а) Докажите, что с двумя флажками Робот обойдет нашу область.

б) Докажите, что одного флажка мало. (**Указание.** Разберите два случая: когда флажок бесконечно много раз пронесется через центр и когда он все время остается в одной из четвертинок, а через центр проходит только Робот)

Задача (А.В.Аджанс). На клетчатой ленте можно один раз записать символы. Робот их может читать, но не может ни писать, ни стирать. Можно ли расписать ленту и запрограммировать Робота так, чтобы он ее всю обошел?

Решение. Докажем, что это сделать нельзя; предположим противное. Возможны два случая. Либо Робот только конечное число раз проходит через нулевую позицию – тогда с какого-то момента он останется только в одной полупрямой. Ясно, что тогда он не обойдет всю прямую. Во втором случае Робот бесконечно много раз пройдет через нулевую позицию и тогда какие-то два его состояния в этой позиции повторятся. Далее рассуждаем как в предыдущей задаче.

Упражнение. Докажите, что один флажок здесь Роботу не поможет. (Решается аналогично предыдущему упражнению. Требуется рассмотреть проносы флажка через нулевую позицию.)

Теперь, когда мы располагаем двумя необходимыми идеями – идеей виртуального автомата и идеей состояния в нужном месте, можно приступить к доказательству невозможности обхода клетчатой плоскости с помощью только двух флажков. Мы приведем только схему разбора случаев со ссылкой на идеи, которыми эти случаи делаются. Этапы доказательства обозначены большими цифрами. Данное доказательство принадлежит А.В.Аджансу.

Значит, он бесконечное число раз далеко уходит от каждого флажка. А если Робот далеко ушел от данного флажка, то будет удаляться и дальше (см. решение задачи...) пока не наткнется на другой. Значит, далеко уйдя от одного флажка, он должен попасть к другому.

Пусть X – число его внутренних состояний.

Завершим доказательство. Итак, мы имеем режим работы Робота, как в упражнении...: Он курсирует между флажками, расположенными в полосе ширины H с данным рациональным углом наклона α . Дойдя до флажка Робот "взаимодействует" с ним и сдвигает его на ограниченное неким числом d расстояние; затем идет к другому. Сдвиги флажков устроены так, что оба все время находятся в некоторой полосе указанного вида (при этом сама покрывающая их полоса может только сдвигаться).

Воспользуемся идеей "повторения состояний в подходящем месте": рассмотрим состояния системы в момент нахождения Робота, скажем, у левого флажка, под "состоянием" будем понимать внутреннее состояние Робота плюс проекцию на нормаль к полосе. Пусть два состояния повторились, причем между этими повторениями других повторений нет. За это время он не более $2 \times H$ раз прошелся туда – обратно от одного флажка к другому, и, стало быть, сдвинул каждый флажок на расстояние не больше $2 \times H^2$. Мы имеем следующий режим: флажки расталкиваются и сдвигаются. Как легко видеть, положения Робота заметают угол (см.рис.).

Задача. Найдите ошибку в приведенных рассуждениях и исправьте ее.

Периодичность и остатки.

Ошибка в решении предыдущей задачи заключена в последней его части. Пусть два состояния Робота в момент подхода к первому флажку повторились. Пусть при этом повторилась проекция пары флажков на нормаль к полосе. В обоих случаях взаимодействие Робота с первым флажком а стало быть и отход ко второму флажку будут одинаковыми. Но это не значит, что и приход ко второму флажку будет таким же!

В чем же здесь дело? Пусть Робот отойдя от левого флажка и двигаясь, как нам известно, периодическим образом, пришел к правому. От чего зависит взаимодействие?

Дело в том, что встреча, вообще говоря, может произойти в любом месте периода. Значит, состояния Робота в момент встречи с правым флажком могут различаться, даже если начальные состояния в момент отхода и совпадали. Соответственно, разным может оказаться и взаимодействие Робота с правым флажком, а затем – и обратный приход к левому.

Как исправить ошибку? Поймем, когда одинаковость отхода ведет к одинаковости прихода. Это произойдет, если путь Робота в обоих случаях отличается только на целое число периодов.

И значит, в понятие "состояние" системы следует включить еще и "остаток от вектора \vec{F} , соединяющего флажки по модулю периода" а затем убедиться, что число таких "остатков" конечно. Впрочем, нужно еще определить смысл слов "остаток от вектора по модулю периода". Под словом "период" в этот момент нам удобнее понимать вектор \vec{t} , на который сдвигается Робот. ¹ Этот вектор параллелен полосе. Уточним понятие "остаток". Будем вычитать из вектора \vec{F} вектор \vec{t} , пока не получится вектор с минимальной проекцией на направление полосы. Длина этого вектора не больше чем $|\vec{t}| + H$ (H – ширина полосы) и, значит, число таких векторов или остатков ограничено числом $4 \cdot (|\vec{t}| + H)^2$. Значит, если в понятие "состояние системы" включить еще и этот остаток, то число состояний останется ограниченным и наше доказательство невозможности обхода плоскости двумя флажками пройдет.

Следующие задачи очень похожи на только что рассмотренную:

Задача. Докажите, что бесконечное дерево степени 3 нельзя обойти

- а) без флажков.
- б) с помощью только одного флажка.
- в) с помощью только двух флажков.

В дальнейшем мы увидим как с помощью трех флажков обойти это дерево.

Задача. С помощью одного только флажка нельзя обойти полупространство. Скажем больше: множество всех положений Робота можно покрыть конечным числом полос (полоса – это H – окрестность плоскости), имеющих общую прямую, вдоль которой движется флажок. (ср. с упражнением ...)

В конце решения задачи про два флажка на плоскости нам встретились остатки. Постараемся осознать, с чем мы столкнулись. В начале книги мы изучали остатки с помощью идеи периодичности. Здесь же мы наоборот, изучаем периодичность с помощью идеи остатка! Остаток выступил не как математическое понятие, а как идея. (Заметим, что остаток в задаче про флажки – это не совсем тот остаток, к которому мы привыкли. В процессе решения он возник не как четкое понятие, и только потом был формализован.)

Роль идеи остатка при изучении периодичности заключается в том, что состояние процесса в момент времени t управляется остатком от деления t на величину периода.

Применяя это соображение мы видим, что если рассматривать несколько процессов как один, то период общего процесса есть наименьшее общее кратное периодов составляющих процессов (а предпериод равен максимуму предпериодов). Как видите и более сложное понятие наименьшего общего кратного может выступать как идея.

На плоскости движение Робота прямолинейно и равномерно. На полуплоскости его движение тоже не сложно: "с высоты птичьего полета" будет наблюдаться "равномерный" подход к границе (если только он к ней подходит), взаимодействие с ней ("рассеивание") и затем равномерный отход от границы (возможно, в другом режиме) либо Робот будет путешествовать вдоль границы (он будет "захвачен" ею), и его движение будет опять-таки равномерным.

А как движется Робот по четвертинке плоскости? Нет ли и тут периодичности, подобной той, которую мы уже наблюдали в задаче про два флажка: не будут ли его состояния при ударе, скажем, о нижний край, периодически повторяться? Попробуем это доказать, рассуждая похожим образом.

Если Робот не взаимодействует с краями, то его движение ничем не отличается от движения по неограниченной плоскости; если Робот только конечное число раз ударяется об один из краев, то его движение в конце ничем не отличается от движения по полуплоскости. Итак, достаточно изучить случай, когда Робот бесконечное число раз ударяется об оба края. Докажем периодичность смены состояний Робота при ударе о нижний край листа.

Рассмотрим его состояния в момент соударения с нижним краем. Ясно, что два состояния повторятся. Для повторения состояний Робота при следующем ударе, надо чтобы приход к другому краю и взаимодействие осуществились тем же местом периода, как мы это уже видели при разборе задачи про два флажка. Чтобы это обеспечить, включим

¹а не то, что мы понимали до сих пор и будем понимать после этого места – повторяющийся кусок последовательности состояний.

в понятие "состояние" еще и остаток от координаты Робота от деления на число N , которое мы выберем так: возьмем все режимы движения Робота, и пусть (x_i, y_i) – соответствующие векторы сдвига. И пускай $N = \prod_i x_i!y_i!$. Теперь-то уж заведомо, если повторились еще и остатки по модулю N , то осуществится не только одинаковый отход от нижнего края, но и одинаковый приход к левому краю и наоборот. Итак, периодичность поведения Робота – т.е. смены его состояний возле нижнего края, установлена!

Задача. Найдите ошибку в предыдущих рассуждениях. (Движения Робота могут быть и неперiodичными.)

Когда я работал над Чертежником вместе с М.В.Сапиром, он сообщил мне

Удивительный факт. Пусть A_1, A_2, \dots , – последовательность натуральных чисел, и существует программа, по которой ЭВМ (с бесконечной памятью) для каждого n вычисляет A_n . Тогда существует программа для Чертежника, по которой он для любого n , начав из положения на рис.3 при $K = 2^n$, закрасит полоску из 2^{A_n} клеток, если лист бумаги – четверть плоскости.

Для умеющих возводить в степень и логарифмировать Чертежник может заменить компьютер. (Это значит, говоря на Строгом Языке Логиков, что с его помощью можно вычислять любую Вычислимую Функцию $A(N)$.) Из этого факта можно извлечь алгоритмическую неразрешимость ряда утверждений – например, уже упомянутую теорему Матиясевича.

Таким образом, Чертежника, который совсем "не знаком" с числами, можно научить "вычислять" все, что может вычислить ЭВМ с бесконечной памятью, например, цифры в десятичном разложении корня из двух (подробнее об алгоритмах см. книгу В. А. Успенского "Машина Поста").

Однако у меня поначалу возникло сомнение в "удивительном факте" и я попытался его опровергнуть. Рассуждения были такими: докажем, к примеру, невозможность перехода от 2^n к 2^{n^2} или, еще проще, перехода от 2^n к 3^n . Если число n – очень большое, то, в процессе перехода Чертежнику придется очень много раз удариться о край (это действительно так. Советуем доказать), а дальше последовало уже описанное рассуждение о периодичности поведения Чертежника на четвертинке плоскости. Это рассуждение, вместе с найденной в нем ошибкой дало возможность понять и доказать "удивительный факт". Поэтому постарайтесь сами ее найти.

Так все-таки в чем же ошибка?

Постараемся разобраться. Пусть два состояния Робота на нижнем краю повторились, x_1 и x_2 – соответствующая координата, причем по условию $x_1 \equiv x_2 \pmod{N}$. Когда Робот перейдет на левый край, соответствующие координаты будут y_1 и y_2 . Приход к левому краю произойдет тем же местом периода, соответственно одинаковым будет и взаимодействие. Однако может получиться так, что $y_1 \not\equiv y_2 \pmod{N}$. И после нового прихода к нижнему краю не только $x'_1 \not\equiv x'_2 \pmod{N}$, но, более того, в момент следующего прихода к нижнему краю могут различиться и внутренние состояния Робота, и, соответственно, разным окажется взаимодействие с краем. Здесь и заключена ошибка.

Посмотрим на примере что происходит, и заодно постараемся осуществить переход $2^n \rightarrow 3^n$. Пусть Робот идет три раза вверх и два раза влево. Тогда если x – его начальная координата внизу, то его координата y после прихода на левую сторону угла будет равна $3/2 \cdot x$. Пусть затем Робот возвращается к оси OX под углом в 45° ; тогда $x' = y = 3/2x$ и $(x_1 - x'_1) = 3/2 \cdot (x_2 - x'_2)$. Так что если x_1 и x_2 и были сравнимы по модулю N , то сравнимость x'_1 и x'_2 может нарушиться, более того, расстояние между $x_1^{(k)}$ и $x_2^{(k)}$ может стать нечетным. После этого приход Робота к краю осуществится другим местом периода и продолжать вести себя тем же образом Робот не сможет.

Теперь попробуем осуществить переход $2^n \rightarrow 3^n$. Если вначале Робот находится на расстоянии $x = 2^n$ от вершины угла, то $x' = 3/2 \cdot x = 3 \cdot 2^{n-1}$, $x'' = 3^2 \cdot 2^{n-2}, \dots, x^{(n)} = 3^n$. Однако для осуществления перехода нам надо остановить Робота на расстоянии 3^n от начала. Как это сделать? Надо на обратном пути к оси OX всякий раз проверять четность, для чего считать число тактов по модулю 2. Под тактом следует понимать пару сдвижений: на одну клетку вправо и на одну клетку вниз. Для слежения за тактами Роботу хватит одной дополнительной ячейки памяти. Итак, разобравшись с ошибкой мы осуществили переход $2^n \rightarrow 3^n$.

Исследуем поведение Робота на четвертинке. Теперь ясно, как для взаимно простых q_1 и q_2 создать программу для перехода Робота $q_1^n \rightarrow q_2^n$, программу универсальную по n . Надо действовать аналогично, сдвигаясь на q_2 полей вверх и на q_1 полей влево. Тогда координата y прихода на левый край с координатой x отхода от нижнего края будет связана равенством $y = x \cdot q_2/q_1$. Возвращаясь под углом в 45° к левому краю, следует проверять число тактов по модулю q_1 . Число состояний Робота будет, разумеется, зависеть от q_1 и q_2 , но не от n . А что если q_1 и q_2 не взаимно просты? Надо взять q_3 , взаимно простое с q_1, q_2 и осуществить переход в два этапа:

$$q_1^n \rightarrow q_3^n \rightarrow q_2^n$$

Можно осуществить и более сложные переходы.

Задача. Осуществить переход $2^n \rightarrow 2^{2^n}$ универсально по n .

Схема перехода.

Как видите, поведение Робота на четвертинке плоскости может быть очень сложным; "удивительный факт" означает, что оно может имитировать работу компьютера с неограниченной памятью. Постараемся во всем этом разобраться.

Простые числа играют роль регистров, а показатель степени при данном простом – содержимого соответствующего регистра. Нас интересуют прежде всего положения Робота на нижнем краю. Такое положение Робота на расстоянии $2^a 3^b 5^c 7^d$ от вершины угла, к примеру, мы рассматриваем как четыре числа a, b, c, d , которые записаны в регистры, помеченные символами 2, 3, 5, 7. Эта кодировка называется Геделевой нумерацией. Обозначать регистр простого p мы будем \mathfrak{P} .

Заметьте, что всего лишь из двух регистров – координат x и y Робота мы научились извлекать любое, наперед заданное число регистров!

Что можно делать с регистрами? Движение вдоль прямой с угловым коэффициентом наклона $-p$ или $-1/p$ дает возможность увеличивать или уменьшать содержимое регистра \mathfrak{R} на единичку. Проверка делимости расстояния от края на p означает проверку того, записан ли в регистре \mathfrak{R} ноль или нет. Содержимое одного регистра \mathfrak{R}_0 мы можем, как это было подробно показано для двойки и тройки, переписать в другой регистр \mathfrak{R}_1 и, более того, сразу в несколько регистров $\mathfrak{R}_1, \mathfrak{R}_2, \dots, \mathfrak{R}_n$. Для этого достаточно повторять, пока это возможно, следующее действие: вычитание единички из \mathfrak{R}_0 с последующим добавлением по единичке в каждый регистр \mathfrak{R}_i . С помощью этих операций содержимое каждого регистра можно увеличивать в несколько раз, копировать в другой регистр ($p_0^n \rightarrow p_2^n \rightarrow p_0^n p_1^n$), складывать содержимое двух регистров ($p_0^n p_1^n \rightarrow p_0^n p_1^m p_3^n \rightarrow p_0^n p_1^m p_3^{n+m}$), а также сбрасывать содержимое регистра ($p^n M \rightarrow M$).

Обратимся снова к схеме 1. Как осуществлялся переход $2^n \rightarrow 2^{2^n}$? После перехода $2^n \rightarrow 2 \cdot 3^n$ мы n раз удваивали содержимое регистра 2. Это было организовано с помощью регистра 3, выступившего в качестве счетчика: после каждого удвоения регистра 2 вычиталась единичка из регистра 3, и делалось это пока возможно. Мы осуществили цикл с $i = n, \dots, 0$. В общем случае, пусть мы можем сделать некоторую операцию, не затрагивающую регистр \mathfrak{R} , в котором записано число n . Тогда эту операцию можно повторить n раз: завершая ее, вычитаем, если это возможно, из регистра \mathfrak{R} единичку и снова возобновляем. Поскольку $a \times b = a + \dots + a$ (раз), и $a^b = a \times a \times \dots \times a$ (раз), то можно умножать содержимое двух регистров и возводить в степень. Кроме того, содержимое двух регистров можно сравнивать ($p_1^n p_2^m \rightarrow p_1^n p_2^m p_3^n p_4^m$, далее вычитать, пока можно, по единичке из регистров \mathfrak{R}_3 и \mathfrak{R}_4 , и посмотреть, в каком из них впервые появится ноль. Потом содержимое буферных регистров \mathfrak{R}_3 и \mathfrak{R}_4 можно сбросить).

Если мы умеем вычислять функцию $f(x)$, с помощью сравнения содержимого регистров, можно вычислять и обратную функцию $f^{-1}(y)$: будем последовательно вычислять $f(1), f(2), \dots$, пока при некотором x $f(x)$ не окажется равным y .

Следующий переход понадобится при обходе дерева с тремя флажками:

$$2^x 3^y 5^z \rightarrow 2^x 3^{\lfloor x/3 \rfloor} 5^{3z + \bar{y}}, \text{ где } \bar{y} \in \{0, 1, 2\} - \text{остаток числа } y \text{ по модулю } 3.$$

Приведем примеры объектов, эквивалентных Роботу на четвертинке плоскости:

1. (М.В.Сапир) Имеется две неограниченных справа проволоочки с костяшками счет и конечный автомат, который может перебрасывать каждую костяшку налево-направо и проверять, кончились слева костяшки, или нет.

2. Конечный автомат, снабженный двумя счетчиками. Счетчик – это регистр внешней памяти, к содержимому которого можно прибавлять или вычитать единичку, а также проверять, записан 0 или не 0. Содержимым счетчика может быть только натуральное число.

3. Робот на прямой, снабженный тремя флажками.

4. (М.В.Сапир) Робот на четвертинке плоскости, который может двигаться только под углом 45° к осям, на две клетки вверх и одну влево, на три клетки вверх и одну влево либо наоборот. По прежнему разрешена проверка наличия края.

Что понимается под словами *эти объекты эквивалентны Роботу на четвертинке плоскости*? Поясним это на третьем примере. Каждой программе для Робота на четвертинке плоскости соответствует программа для Робота на прямой следующим образом. Роль координат x и y будут играть расстояния между левым и средним и между правым и средним флажками. Роль проверки условия "ВПЕРЕДИ КРАЙ" будет играть проверка того, находятся ли два флажка в одном месте. Вместо перемещения по координате x или y мы будем двигаться до соответствующего флажка и его сдвигать. Сказанное означает, что система "Робот на четвертинке плоскости" интерпретируется системой "Робот на прямой с тремя флажками".

Упражнение. Постройте аналогичную интерпретацию объектами 1, 2, 4.

Мы рассмотрели подробнее третий объект, поскольку он нам понадобится для обхода лабиринтов. Общая идея такова: ставятся три флажка в ряд и организуется Машина Минского – т.е. компьютер с еограниченной памятью, для которого и пишется программа обхода лабиринта. При этом следует проследить за тем чтобы не потерять память – в прямом и переносном смысле – т.е. надо двигаться вместе со своими флажками сохраняя при этом информацию, заключенную в расстояниях. Рассмотрим простейший пример – обход плоскости с помощью трех флажков. Конечно, это делается гораздо проще, но нам интересен только пример рассуждений. Расположим вначале флажки вдоль оси OX так, чтобы расстояние между средним и левым было бы равно 0, а расстояние между средним и правым – скажем, восьми, т.е. 2^3 . Организуем, как обычно, регистры 2 и 3. Перегоняя единичку из регистра 2 будем подниматься на 1 шаг вверх вместе с флажками. Это осуществляется так: доходим до самого левого, передвигаем его на 1 шаг вверх, возвращаемся вниз и идем направо, проделывая то же с двумя другими флажками. (Дойдя до последнего, разворачиваемся.)

Итак, будем подниматься вместе с флажками, пока содержимое 2 не перегонится в 3. Затем, перегоняя содержимое 3 в содержимое 2 и опускаясь, вернемся в исходное положение – на ось OX . Мы обошли область сверху этой оси. Область под ней обходится аналогично, после чего к содержимому 2 добавляем единичку и повторяем весь процесс.

Для обхода трехмерного пространства можно воспользоваться регистрами 2 и 3 для движения вдоль оси OY , а регистрами 5 и 7 – для движения вдоль оси OZ . Всякий раз, перегоняя единичку из 5 в 7, мы обходим кусок слоя с помощью регистров 2 и 3 и смещаемся вдоль оси OZ нужным образом.

Упражнение. Нарисуйте схему программы для обхода Роботом с тремя флажками k -мерной решетки. Число его состояний может зависеть от k .

Займемся теперь более интересным обходом свободного дерева степени, скажем, 3 с помощью трех флажков. (см. рис.)

Вначале покажем, как обходит это дерево компьютер с неограниченной памятью. Пусть O – начальная вершина. Программа обхода состоит в переборе всех конечных путей, выходящих из O . Проходя каждый путь, компьютер возвращается назад в точку O и переходит к прохождению нового пути. Каждый путь кодируется последовательностью цифр 0, 1, 2 которая записывается троичным разложением одного числа X . 0 соответствует команде "НАЗАД 1 – "НАЛЕВО 2 – "НАПРАВО". Переход к рассмотрению нового пути соответствует добавлению единицы к числу X . Чтобы вернуться обратно нам надо помнить в процессе движения также число Y , кодирующее путь, обратный к пройденному отрезку пути, и число Z – кодирующее оставшуюся часть пути. После каждого смещения числа Y и Z изменяются так: $Z' = [Z/3]$, $Y' = 3Y + Z$, где $Z \in \{0, 1, 2\}$ – остаток от Z по модулю 3. (При обратном движении с помощью информации, закодированной в числе Y , 1 соответствует повороту "НАПРАВО а 2 – "НАЛЕВО".) Пункт в) упражнения ... позволяет осуществить этот алгоритм на машине Минского.

Но как реализовать саму машину Минского на дереве с помощью трех флажков? Поставим флажки в ряд, если идти по "правилу правой руки" – т.е. все время поворачивать направо. Это дает возможность реализовать машину Минского, однако как двигаться, чтобы не впасть в беспамятство? Как не потерять флажки и информацию, связанную с ними в процессе движения? Идея такого смещения показана на рисунке:

Упражнение. Нарисуйте схему программы обхода свободного дерева степени k .

Замечание. Робот, снабженный датчиком случайных чисел с помощью всего лишь двух флажков может обойти решетку любой размерности. И это несмотря на то, что без такого датчика ему не обойти даже плоской решетки! Идея состоит в организации Машины Минского в плоскости, параллельной плоскости XOY . Пусть один из флажков это вовсе и не флажок, а прожектор, который светит вдоль осей OX и OY . В этом случае Машина Минского организуется как и при движении Робота на четвертинке листа – попадание под луч соответствует удару о край. Чтобы обойтись без прожектора, достаточно уметь определять взаимное расположение двух флажков. Для этого достаточно пройти от одного к другому монотонным путем (т.е. не содержащим движений в противоположных направлениях). Этого добиваемся так: пусть Робот блуждает вдоль плоскости, где расположены флажки. Рано или поздно он отойдет от первого и придет ко второму флажку, в силу теоремы о возвращении. Будем наблюдать такие прохождения не трогая флажки, пока Робот не пройдет от одного к другому монотонным путем. Поскольку возвращение к исходной точке при случайном блуждании по плоскости происходит неограниченное число раз, такое явление неизбежно, что и позволяет симитировать прожектор.

Лабиринт, который не обойти.

Итак, Машина Минского равносильна компьютеру с бесконечными ресурсами. Нам удавалось организовать ее в довольно сложных ситуациях, например, на дереве. Создается впечатление, что если есть много флажков, а тем более взаимодействующих Роботов, то можно обойти все, что угодно. Однако это не так. Справедлива

Теорема. *Существует бесконечный связный граф, такой, что любое конечное семейство из флажков и взаимодействующих Роботов не сможет покинуть конечной области.*

Чтобы привести пример такого графа, нам потребуется ввести несколько новых понятий (их сводка – см. приложение).

Образующие группы G – это элементы, через произведение которых и обратных к ним можно выразить любой элемент группы. Нас будут интересовать только *конечно-порожденные* группы, т.е. группы, имеющие конечный набор образующих. По группе G с фиксированным набором образующих можно построить $\Gamma(G)$ – граф группы G . (Один из таких графов и даст нам искомый пример.) Пусть, например, G имеет две образующие – a и b . Вершинами этого графа будут элементы группы G , два элемента g_1 и g_2 соединены ребром \iff выполнено одно из равенств: $g_1 = g_2 a^{\pm 1}$ или $g_1 = g_2 b^{\pm 12}$

Простейший пример: a и b есть параллельные переносы на единичные векторы \vec{e}_x и \vec{e}_y . Тогда G есть группа переносов на целочисленные векторы и $\Gamma(G)$ есть обычная целочисленная решетка. Вот более сложный пример.

Пример. *Свободная группа с двумя образующими* – это множество слов, состоящих из символов a, b, a^{-1}, b^{-1} . Слова умножаются простым приписыванием, с последующим сокращением букв с обратными буквами. Пусть, к примеру, $u = abab^{-1}ab, v = b^{-1}a^{-1}ba^2b$. Тогда $vu = b^{-1}a^{-1}ba^2babab^{-1}ab$, а $uv = aba^3b$ ($a^n = a \dots a$). Как видите, $uv \neq vu$. Пустое слово Λ , не содержащее символов, соответствует единице группы. $\Lambda = aa^{-1} = bb^{-1}$. Граф $\Gamma(G, a, b)$ показан на рисунке:

Упражнения. Расстояние между двумя вершинами графа – это минимальное число звеньев пути, их соединяющего. (Если такого пути нет, то расстояние считают бесконечным.)

а) Докажите, что выбор других образующих может изменить расстояния в $\Gamma(G)$ только в ограниченное число раз.

б) Докажите, что $\Gamma(G)$ всегда связан и однороден, т.е. любую его вершину можно перевести в любую другую подходящим автоморфизмом графа (автоморфизм – это изоморфизм на себя, уважающий ребра). Как устроен этот автоморфизм?

в) Если в определении графа группы соединять ребром вершины, отличающиеся только левым умножением на образующую (ранее мы соединили вершины, отличающиеся только правым умножением), то получится граф Γ' , совпадающий с Γ , тогда и только тогда, когда G – коммутативна. Докажите, что и в общем случае графы Γ и Γ' изоморфны.

²Иногда мы будем писать $\Gamma(G, \{a_i\})$, где $\{a_i\}$ – набор образующих.

Элемент $g \in G$ группы G называется *периодическим*, если при некотором $n \geq 1$ $g^n = e$ - единице группы G , иначе g называется *непериодическим*. Группа G называется *периодической*, если все ее элементы периодические. Иначе, т.е. если в G имеется непериодический элемент x , то G называется *непериодической*.

Задача. Пусть G – непериодическая группа. Расположив три флажка по направлению степеней непериодического элемента x и действуя как в задаче ... нарисуйте схему обхода ее графа с помощью трех флажков.

А вот можно ли обойти граф периодической группы? Если она конечна – то без сомнения. Однако имеет место следующий

Факт. (Теорема Бернсайда) *Существует бесконечная конечно-порожденная (даже 2-порожденная) периодическая группа G .*

Так вот, граф группы G – это то, что нам надо. Справедлива

Теорема. $\Gamma(G)$, вне зависимости от выбора набора образующих G не обходится никаким конечным семейством Роботов и флажков. Более того, всегда можно указать конечную область в $\Gamma(G)$, которую заданное конечное семейство роботов и флажков никогда не покинет.

Доказательство. Посмотрим сначала, как движется Робот по Γ один, без флажков. Поскольку наш граф в каждой своей вершине устроен одинаково, то Робот заикнется, а значит, его движения начнут периодически повторяться. Посмотрим, каково смещение за период. Из вершины $g \in G$ Робот идет в вершину $ga_i^{\pm 1}$, в зависимости от своего внутреннего состояния. Когда пройдет период и два его состояния повторятся, Робот придет в вершину $g \cdot h$, где

$$h = a_{i_1}^{\varepsilon_1} \cdots a_{i_n}^{\varepsilon_n},$$

$\varepsilon_i = \pm 1$, a_i и ε_i определяются внутренним состоянием Робота в соответствующий момент. Когда минуют два периода, Робот перейдет в вершину $g \cdot h^2$, а когда $n - g \cdot h^n$. Но раз G периодична, то при некотором n $h^n = e$ и, стало быть, Робот ходит по кругу! Он не может далеко уйти от того места, куда его поместили изначально! (А если у Робота есть предпериод, то его траектория суть "цикл с хвостом".) Итак, имеется функция F , такая, что автомат, имеющий только n внутренних состояний, не покинет области диаметром $F(n)$, вне зависимости от его начального положения.

Теперь посмотрим, помогут ли Роботу флажки выйти из заколдованного круга. Посмотрим сперва, как меняет дело один флажок. А никак! Ведь Робот не может далеко уйти от флажка и, стало быть, система Робот-Флажок может принимать только конечное число состояний и ее можно рассматривать как виртуальный конечный автомат! Можно (хотя и не обязательно) оценить число его внутренних состояний. Пусть k – число образующих группы G . Тогда вершин в графе Γ , находящихся на расстоянии не выше l от заданной не более чем $(2k)^l$. Поэтому число состояний виртуального автомата не более, чем $n \cdot (2k)^{F(n)}$ и система робот-флажок не покинет области диаметром $F(n \cdot (2k)^{F(n)})$.

Рассмотрим случай двух флажков. Если расстояние между ними ограничено, то проходит идея виртуального автомата с теми же рассуждениями. Иначе Робот должен далеко разнести флажки и, стало быть, далеко идти только с одним флажком, что, как мы уже доказали, разбирая случай одного флажка, невозможно.

Упражнение. Уточните приведенные рассуждения. Докажите, что система "Робот с двумя флажками" не покинет области диаметра

$$F\left(n \cdot F(n \cdot (2k)^{F(n)})^3\right)$$

Теперь общий случай, когда флажков много, скажем 2004. Сделав предположение индукции, мы можем считать, что система "Робот менее чем с 2004 флажками" не покинет ограниченной области размера $H(n)$ (n – число внутренних состояний Робота). А дальше рассуждать аналогично: либо расстояния между флажками неограниченно – тогда система Робот менее чем с 2004 флажками совершает неограниченное путешествие, что невозможно. Либо, если такое расстояние ограничено то применим идею виртуального автомата.

Недаром герои сказок в заколдованном лесу хоят по кругу, мечтая найти прямой путь!

Упражнение. а) Получите оценки, аналогичные предыдущему упражнению.

б) Проведите те же рассуждения для общей системы из нескольких Роботов и флажков.

Мы расскажем теперь, как додуматься до того, чтобы взять граф бесконечной периодической группы в качестве непроходимого лабиринта? Ясно, что конструкцию графа группы, понятие периодической группы и формулировку теоремы Бернсайда надо было знать заранее. Для непроходимости лабиринта нужно, чтобы на флажках нельзя было бы организовать Машину Минского, а Робот ее организует, как мы это видели на примере задачи ... , ставя флажки вдоль своей траектории. Поэтому у Робота не должно быть длинных путей, что можно обеспечить заикливанием. Из эстетических соображений хочется, чтобы граф был бы одинаково устроенным во всех вершинах, т.е. однородным, а в качестве однородного графа естественно брать граф группы. Чтобы пути заиклились, группа должна быть периодической, а чтобы Робот ее не обошел - бесконечной.

Если рассуждение содержательно, пусть ошибочно, то его обычно можно исправить и получить результаты, правда не те, которые ожидался первоначально.

Вы, вероятно, заметили одну странность в кодировке Машины Минского: когда нам требовалось запомнить несколько чисел a_1, \dots, a_k , мы рассматривали число $2^{a_1} 3^{a_2} \dots p_k^{a_k}$ (где $2, 3, \dots, p_k$ – последовательные простые числа). Операция возведения в квадрат тоже производилась как-то странно: мы рассматривали переход $2^n \rightarrow 2^{2^n}$. Встает вопрос: а нельзя ли все это делать естественнее, например написать программу для непосредственного перехода от n к n^2 ?

Оказывается, такие переходы невозможны. Чтобы это доказать, нам понадобится то самое рассуждение с периодическим поведением Робота на четвертинке плоскости, которое в тот раз оказалось ошибочным, теперь же мы его подправим.

Приглядимся к нему повнимательнее. Пусть два внутренних состояния Робота совпали на нижнем крае, и, кроме того, соответствующие координаты x_1 и x_2 оказались сравнимыми по модулю N (которое делится на все, что нужно). В этом случае приход к другой стенке и взаимодействие с ней будут одинаковыми. Правда, соответствующие координаты y_1 и y_2 окажутся, вообще говоря, по модулю N несравнимыми и дальнейшее поведение Робота может измениться. Однако, если x_1 и x_2 будут сравнимы по модулю N^2 , то y_1 и y_2 будут сравнимы по модулю N .

Покажем это. Из леммы ... следует, что $y = a/b \cdot x + c$, где числа a, b, c не превосходят по модулю числа внутренних состояний Робота. Поэтому $y_1 - y_2 = a/b \cdot (x_1 - x_2)$. По выбору N число b делит N .

В этом случае повторится и следующее взаимодействие со стенкой. Точно так же, если x_1 и x_2 сравнимы по модулю N^3 , то $y_1 \equiv y_2 \pmod{N^2}$ и $x'_1 \equiv x'_2 \pmod{N}$ и уже взаимодействие со стенкой в точках y'_1 и y'_2 будет одинаковым. Аналогичным образом, если $x_1 \equiv x_2 \pmod{N^{2k}}$, то $x_1^{(i)} \equiv x_2^{(i)} \pmod{N^{2(n-i)}}$ и взаимодействие со стенками, а, значит, и поведение Робота в точках $x_1, x'_1, \dots, x_1^{(n)}$ и $x_2, x'_2, \dots, x_2^{(n)}$ соответственно, будет одинаковым.

Задача. Найдите ошибку в этих рассуждениях.

Ошибка в том, что мы не учли эффект угла. Взаимодействие Робота со стенкой может зависеть и от того, встретит ли он по ходу дела еще и другую стенку. Однако если Робот все время далек от угла (т.е. все $x_i^{(j)}$ и $y_i^{(j)}$ больше удвоенного числа его внутренних состояний), то такого эффекта не возникает.

Таким образом, поведение Робота для начальных точек x и $x + aN^{2k}$ при любых x и a до осуществления $2k$ -го удара о стенку будет одинаковым, за исключением только что сделанной оговорки.

Теперь мы можем доказать, что программы перехода от n к n^2 , универсальной по n для Робота с ограниченным числом состояний не существует.

В самом деле: предположим, что такая программа существует. Пусть l – число внутренних состояний Робота. Прежде всего заметим, что приближение Робота к углу будет происходить только для конечного числа начальных позиций n , так что весь путь Робота, начинающийся с достаточного большого n будет лежать достаточно далеко от угла и соответствующих эффектов не будет. В противном случае из-за конечности числа полей, близких к вершине угла, на какое-то из них Робот придет в одном и том же состоянии, но из разных начальных положений n_1 и n_2 . В этом случае его дальнейшее поведение, а, значит, и финальное положение будет одинаковым. Но $n_1^2 \neq n_2^2$! Противоречие.

Итак, пусть n – достаточно большое число и пусть в процессе перехода от n к n^2 произошло k ударов о стенки. Возьмем $n_1 = n, n_2 = n_1 + a \cdot N^k$. В результате из новой позиции n_2 . Робот произведет те же k ударов о стенку и точно так же остановится. И все режимы его движения между ударами будут в точности такими же!

В первом случае Робот совершил переход $n \rightarrow n^2$. Из точки $n + aN^k$ Робот должен перейти в точку $n^2 + 2naN^k + a^2N^{2k}$ при любом a за те же k ударов!

Почему это невозможно? Потому, что расстояние выросло в $n + aN^k$ раз, а за один удар оно может измениться не более чем в l раз (почему?) и при $a > l^k$ такое невозможно. Как видите, рассуждение может иметь ценность само по себе, хотя в одних случаях оно может оказаться ошибочным, в других – нет.

Задачи.

1. Докажите, что не существует программы перехода $n \rightarrow n!$, универсальной по n .
2. Докажите, что не существует программы, позволяющей Роботу, стартующему с начального положения n , приходиться на исходную позицию, если n – степень двойки, а в противном случае – приходиться в вершину угла.
3. Пусть N – то самое число, делящее всевозможные периоды Робота. Пусть Робот осуществил переход $X \rightarrow Y$, сделав k ударов о края, и ни разу не приблизился к вершине угла в том смысле, который обсуждался выше. Докажите, что из начального положения $X + l \cdot N^k$ он осуществит переход в положение $Y + l \cdot \lambda \cdot N^k$, где λ – рациональное число, не зависящее от l .

Другой близкий сюжет связан с *распознаванием*. Пусть Робот путешествует по прямоугольнику $n \times k$. Его цель – проверить, удовлетворяют или нет n и k данному соотношению. Например, идя под углом в 45° Робот легко проверит справедливость равенства $k = n$. Выходя же из левого верхнего угла и идя 2 раза вправо и 1 раз вниз он проверит справедливость или несправедливость равенства $k = n/2$.

С помощью Леммы... решается следующее

Упражнение. а) Пусть $\alpha, \beta \in \mathbf{Q}$. Докажите, что существует Робот, распознающий равенство $k = \alpha \cdot n + \beta$. Число его состояний зависит от α и β , но не зависит от n и k .

б) Аналогичным образом, докажите, что для заданной системы \mathfrak{R} линейных уравнений и неравенств с рациональными коэффициентами от двух переменных, распознается ее выполнимость на k и n .

в) Если $k \leq n$, то справедливость равенства $k = 2^l$ тоже распознается.

Итак, "линейные вещи" распознаются. А вот распознаются ли другие, более сложные равенства, например, равенство $k = n^2$? Длина программы не должна зависеть от n и k .

Оказывается, даже такое простое равенство не распознается и идея доказательства близка к идее доказательства невозможности перехода $n \rightarrow n^2$. Дадим **набросок доказательства**.

Посмотрим, как движется Робот, имеющий l внутренних состояний вдоль полосы шириной n . Его состояния периодически повторяются, причем период не превосходит $n \cdot l$, если же последовательно выписать его состояния только на данном расстоянии от края, то период смены таких состояний не больше l . За каждое соударение он сдвигается вдоль

полосы на $\alpha_i n + \beta_i$, а, стало быть, раз когда его состояния на данном расстоянии от края повторятся, произойдет не более $2l$ ударов о края и Робот сдвинется на число указанного вида. При этом величины α_i и β_i рациональны и для них есть только конечное число возможных значений в зависимости от l . Рассмотрим всевозможные величины сдвигов Робота менее чем с l состояниями в полосе ширины n соответствующие ближайшим повторениям его состояний. Пусть $k_1 \equiv k_2$ по всем таким модулям. Если $l \cdot n < k_1 < k_2$, то эффекта предпериода не возникает и прямоугольники $n \times k_1$ и $n \times k_2$ не различаются Роботом. Ясно, что при больших n $n \cdot l < n^2$ и всегда найдется число k , большее n^2 сравнимое с n^2 по данному набору модулей, тогда прямоугольники $n \times k$ и $n \times k^2$ неразличимы. Точно так же доказывается нераспознаваемость равенств $k = n^3$ и $k = n!$

Упражнение. а) Оформите набросок в доказательство. Говоря точнее, при $k > 2ln$ существует такое t , зависящее от n и l , что при $m \in \mathbf{N}$ прямоугольники вида $n \times k$ и $n \times (k + mt)$ не различаются Роботом, в куда бы его не поместили изначально.

б) Рассмотрим движение Робота в параллелепипеде $n \times m \times k$. Пусть $k > 2lmn$. Тогда при некотором t зависящим от l, m, n для любого i , если $k' = k + i \cdot t$, то параллелепипеды $n \times m \times k$ и $n \times m \times k'$ неразличимы.

в). Исследуйте другие случаи возможности и невозможности распознать.

Алгоритмы и лабиринты. Решения.

А.Я.Белов-Канель, И.А.Гажур, И.А.Иванов-Погодаев, А.С.Малистов

A11. Приведем решение для случая, когда роботы видят флажки друг друга. Пусть каждый робот расталкивает свои флажки по стандартному алгоритму обхода ленты, но первый – по вертикали, а второй по горизонтали. Кроме того, если робот увидел чужой флажок, то он останавливается и ждет. Пусть вертикаль и горизонталь пересекаются в точке O . Если роботы в начале находятся на одинаковом расстоянии от O , они придут в нее одновременно и встретятся. Пусть, теперь, для определенности, робот A в начале находится на большем расстоянии от O чем робот B . В этом случае, в момент прихода робота A в O , он будет находиться между двумя чужими флажками на ленте, по которой ходит B . В соответствии с алгоритмом обхода, A поставит в клетку O флажок, а учитывая, что роботы начали одновременно и следуют одному и тому же алгоритму обхода, за то время пока A добежит до другого своего флажка и вернется назад, робот B проделает путь от одного своего флажка до другого и, следовательно, пройдет через клетку O . Таким образом, он увидит чужой флаг и остановится. Через какое-то время к нему подойдет второй робот.

Задачу также можно решить для случая, когда роботы не видят чужие флаги. Ее решение оставляем читателю.

A12. В трехмерном пространстве Роботы уже могут не пересечься.

Докажем это. Нам потребуется следующее утверждение, описывающее систему “Робот– 2 флажка”:

Лемма. Дана система “Робот– 2 флажка” в n -мерном пространстве. Тогда имеют место следующие возможности:

- 1. Расстояние между флажками не стремится к бесконечности. Расстояние между Роботом и флажками не стремится к бесконечности. Система Робот-Флажки движется также, как Робот без флажков (возможно, с большим числом состояний, чем исходный Робот – прямолинейно и равномерно, вдоль прямой L , параллельной некоторому рациональному вектору. При этом расстояние от Робота до L ограничено.*
- 2. Расстояние между флажками не стремится к бесконечности. Расстояние между Роботом и флажками стремится к бесконечности. Робот движется прямолинейно и равномерно, удаляясь от флажков вдоль прямой L , параллельной рациональному вектору (координаты которого не превосходят числа внутренних состояний Робота). При этом расстояние от Робота до L ограничено.*
- 3. Расстояние между флажками стремится к бесконечности. Робот только конечное число раз встречает один флажок F_1 . Робот движется прямолинейно и равномерно, удаляясь от F_1 вдоль прямой L , параллельной некоторому рациональному вектору. При этом расстояние от Робота и обеих флажков до L ограничено.*
- 4. Расстояние между флажками стремится к бесконечности. Робот бесконечное число раз встречает оба флажка F_i . В этом случае существует такая константа D вектор \vec{e} , координаты которого не превосходят числа внутренних состояний Робота, прямая $L(T)$, параллельная \vec{e} , такая, что:*
 - Робот и флажки находятся от прямой $L(t)$ на расстоянии, не превосходящем D .*
 - Робот движется прямолинейно и равномерно между двумя флажками вдоль \vec{e} , отражаясь от одного флажка и возвращаясь к другому.*
 - Типов таких движений между соударениями конечное число, и эти типы периодически повторяются.*
 - Существует пара векторов $\vec{\lambda} = (\vec{\lambda}_1, \dots, \vec{\lambda}_n)$ и $\vec{\delta} = (\vec{\delta}_1, \dots, \vec{\delta}_n)$ и константа E такие, что прямая $L(t)$, Робот находится на расстоянии, не превосходящем E от отрезка $[\vec{\lambda}\sqrt{t}, \vec{\delta}\sqrt{t}]$, флажок F_1 находится на расстоянии, не превосходящем E от $\vec{\lambda}\sqrt{t}$, флажок F_1 находится на расстоянии, не превосходящем E от $\vec{\delta}\sqrt{t}$.*

Перейдем к **решению задачи A12**. Построим фазовую диаграмму пространство-время, введем ось T и рассмотрим мировые линии Робота и флажков. Переформулируем нашу лемму.

Дана система “Робот– 2 флажка” в n -мерном пространстве-времени. Тогда существует константа G такая, что имеют место следующие возможности

- 1. В ситуации 1) мировые линии Робота и флажков находятся на расстоянии $< G$ от некоторой прямой пространства-времени.*

2. В ситуациях 2)–3) мировые линии Робота и флажков находятся на расстоянии $< G$ от некоторой пары прямых пространства-времени, при этом одна из них задается условием “пространственная координата – константа”.
3. В ситуации 4) Робот и флажки находятся на расстоянии $< G$ от поверхности, состоящей из точек вида $\{(X, T) | X \in [\bar{\lambda}\sqrt{t}, \bar{\delta}\sqrt{t}]\}$.

Решение задачи A12 вытекает из такого наблюдения: любые два множества, описанные в предыдущей лемме, можно так сдвинуть вдоль вектора, перпендикулярного оси времени, чтобы они не пересеклись.

A13. Нет, это не верно. В качестве контрпримера двух лабиринтов можно взять две полуленты. Для них существуют очевидные программы обхода: для ленты бесконечной направо алгоритм обхода следующий: «двигаться налево пока не найдешь стенку впереди, после этого двигаться направо». Аналогичный алгоритм есть для бесконечной налево полуленты.

Допустим, существует универсальный алгоритм для обеих полулент. Запустим его на бесконечной в обе стороны ленте. В какой-то момент состояния повторятся. После этого робот будет удаляться либо вправо по ленте, либо влево. Значит, выбрать такую полуленту, бесконечную только в одну сторону, что она накроет все клетки, где когда либо был робот, плюс еще несколько клеток где он никогда не будет. При обходе этой полуленты робот не сможет отличить ее от полной ленты и поэтому обойти всю не сможет.

A14. Решение этой задачи разбирается в прилагаемой статье Даниила Гусева (файл gusev.pdf).

A15. Решение этой задачи жюри пока не известно.

Циклы В и С.

Решениями задач в циклах В и С являются алгоритмы-схемы, которые можно запускать в специальном приложении VillagerLife (оно прилагается).

В прилагаемых материалах находятся папки, по одной на каждую задачу. В них находятся несколько тестовых карт (названия test1.vlm, test2.vlm и т.д.), а также алгоритмы, решающие данную задачу. Мы приводим алгоритмы, которые написали участники конференции, их имена указаны в названии файла. Если имен не указано, алгоритм был составлен жюри.

Интересные алгоритмы для приведенных задач составили Дмитрий Беликов и Константин Хадаев (совместно), Данила Байгушев, и Брайан Чен, который является единственным участником, решившим сложную задачу C10.

Задачи C5-C7 фактически являются служебными к C8, поэтому тесты и программы для них не приведены.

Для задачи C8 есть два варианта тестов: против двух AI программ. Также приведен алгоритм, составленный Дмитрием Беликовым и Константином Хадаевым.

Algorithms and labyrinths

A. Belov-Kanel, I. Gazhur, I. Ivanov-Pogodaev, A. Malistov

Section A. This is an introductory section. These supporting problems will be removed after intermediate finish.

In the first problems of this section we will examine a standard finite automatic machine: a robot moving on a square grid. The robot can do some actions defined by his program. These actions are:

1. Move forward (to the next cell);
2. Rotate in the current cell;
3. Drop a flag into the current cell (if the robot has a flag);
4. Look for a flag in the current cell;
5. Pick up a flag from the current cell.

Every problem defines how many flags the robot has. The program consists of numerated list with instructions for the robot. Some of these instructions are jumps to another instructions (like GOTO operator in computer languages). We will discuss the opportunities of walking through some sets of cells. By *walking through* or *investigating* the set of cells we mean that the robot using his program can walk through *every* cell in this set.

First of all we should examine some of the robot's skills

Example. Let us prove that the robot with two flags can explore the tape — an infinite tape with width 1. Let the robot be in the cell 0 with two flags. Let us write the robot's program.

1. Drop a flag.
2. Go to cell 1.
3. Drop a flag.

Now we are going to organize a shuttle-moving of the robot between these two flags. Besides, the robot will increase the distance between the flags by «pushing» them. We can obtain this by using the program below:

4. Turn around. (turning at 180 degrees)
5. Move forward.
6. Look for a flag.
7. If there is no flag then go to 5.
8. Pick up the flag and move forward.
9. Drop flag and go to 4.

It is easy to see that the robot will explore all the cells on the tape.

Could the robot explore the tape without any flags? The answer is «no». In order to prove this we should formalize construction of a robot. It is easy to see that every robot's action depends on the number of the current instruction and the presence of a flag in the current cell. Let us call these factors by *the robot's inner condition*. Obviously, there is a finite number of various inner conditions of the robot. In most cases, the robot changes his inner condition after an action. According to the Dirichlet Principle, some inner condition of the robot will happen again. So, let it take t seconds. The robot has moved right for a cells. It is easy to see that in another t seconds the robot will also move right for another a cells. It is clear that the robot cannot reach some cells placed to the left of his starting position.

A0. Prove that the robot with one flag cannot explore the tape.

Hint. You should consider two cases: 1) the robot does not go away from his flag at the distance more then some N ; 2) the robot goes away from his flag at any distance.

A1. Prove that the robot with 4 flags can explore the plane.

A2. Prove that the robot with 3 flags can explore the plane. Could the robot with 3 flags explore the three dimensional space?

Let some borders of cells be impassable. The robot can see these barriers between the cells, when he is situated in one of these cells.

A3. The border of the half-plane is impassable line. Prove that the robot with 1 flag can explore the half-plane.

A4. Prove that the robot with 1 flag cannot explore the plane with four cuts. (picture 1) Prove that the robot with 2 flags can do this.

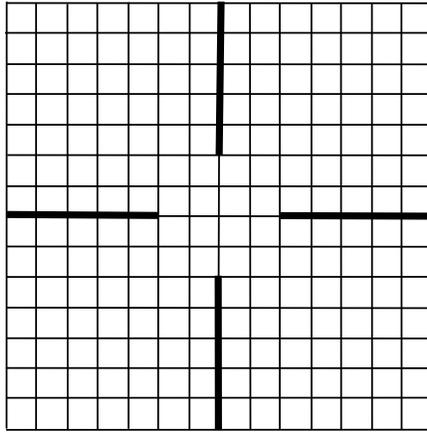


Fig. 1: Four cuts on the infinite plane

The robot is moving on the vertices of the graph. This graph may be infinite.

A5. a) *The graph is called tree if there are no cycles. Let a tree be infinite. Suppose that any vertex of the tree has degree 3. Prove that the robot with 1 flag cannot explore this tree.*

b) *The same question for the robot with 2 flags.*

A6. *Prove that the robot with 2 flags cannot explore the plane.*

Hint. Use the ideas of the problems A0 and A4.

The robot without any flags is moving on the first quarter of the plane. The borders are impassable walls. The robot can see a wall then he is in the cell with this wall.

A7. *Let the robot be in the cell with coordinates $(2^n, 0)$. Write a universal (not depending on n) program, for moving the robot into the cell $(3^n, 0)$ with stopping in that cell.*

Let us call the transition above as *transition from 2^n to 3^n* .

A8. *Write the programs for the robot to make transitions below:*

a) *from 2^n to 6^n ;*

b) *from 2^n to 2^{2^n} ;*

c) *from $2^n \cdot 3^m$ to $2^n \cdot 3^m \cdot 5^{mn}$;*

d) *from $2^n \cdot 3^m$ to $2^n \cdot 3^m \cdot 5^{m+n}$;*

e) *from 2^n to $2^{\lfloor \sqrt{n} \rfloor}$;*

f) *from 2^n to 2^{n^2} ;*

g) *from 2^n to 2^{k_n} , the k_n is the n -th decimal digit of the $\sqrt{2}$;*

h) *from 2^n to 2^{k_n} , the k_n is the n -th decimal digit of the π ;*

A9. *Prove that the robot with 3 flags can explore n -dimensional space.*

A10. *Prove that the robot with 3 flags can explore a tree with degree of each vertex equal to 3.*

Villager's algorithms.

In this section we will explore a *world* – connected subset of cellular plane. Usually, we don't know its size. Every cell on the plane has one of the following types:

1. Rock. The villager could not visit this cell.

2. Ground. The villager can walk through it.

3. Lake. This cell is impassable, but the villager can fishing here from some neighboring cell. There are following parameters for each lake-call: **nibble** (the amount of fish that villager can get from lake using special «fishing» operation); and **fish** - the amount of remaining fish in the lake.

4. House. This is the unique cell in the world. Usually, villager starts here. In some problems the villager should bring home his fish.

The villager can walk thorough cell to another neighboring cell. Being in some cell he looks to the one of four possible directions.

Villager's *action area* is a set of two elements: a cell with the villager and a neighboring by villager's direction cell.

The villager can use information from his action area's cells. But he knows nothing about other cells. Also he has some number of flags (limited by specific problem's conditions). He can drop down these flags in some places and explore the world. The villager can fish on the neighboring lake-cell. Also he can bring some amount of fish limited by 10 kg.

Cells in the world can contain some objects (flags or fish). These objects include some variables. The villager can read this information. Also, he can change flag's variables or create the new ones.

The villager has limited memory. He can create self variables and change its values. The villager can use self variables and its values independently of his location.

Formally, the villager can do the following actions:

1. [Go] Go forward.
2. [Rotate] Rotate to some direction.
3. [Read] Read some information about variables on the objects in his action area.
4. [SetFlag] Set flag in the action area's cell. Or take flag from it. Also it is possible to create some variables on the flags and change its values.
5. [CheckFlag] Check out some flags in the action area.
6. [Fishing] Fishing in the neighboring cell (in the forward direction).
7. [GetPutFish] Get or put down some fish in the action area.
8. [Write] Create self variable or change its value.
9. [Math] Make arithmetic and logic operations using variables. For example, it is possible to check an equality of some variables.

Passing of time. The time in the world is a sequence of *time beats*. If there are no special instructions, each execution of Go, Fishing and GetPutFish operations interrupt the current beat (and we proceed to the next beat). Other operations Rotate, Read, SetFlag, CheckFlag, Write, Math take no time but if there are 500 such operations in the current beat, we proceed to the next beat too. Also, execution of CheckFlag second time in the same beat also interrupt this beat.

In the following problems one should find an villager's algorithms. You can construct and run your own algorithms (flowcharts) using special simulation application «VillagerLife». You will get access to this application.

There are some maximum working time for every problem. The size of maps is unknown. If there are no special conditions, the villager can check the edge of the map (if he is located on the edge cell). The villager can explore a map if he can visit every approachable cell using some algorithm.

Section B. In this section we could not use self variables.

B1. *Explore finite rectangular map (without lakes and rocks) using four flags. In this problem villager could not check an edge of a map.*

B2. *There are two flags on the map (without lakes and rocks) : one in the cell with coordinates $(x, 0)$, second in the cell $(0, y)$. The villager has a third flag and starts in origin $(0, 0)$. How the villager can set any flag to the cell $(x + y, 0)$? x, y – are some positive integers.*

B3. *Now our maps contain rocks and lakes. Explore a map using any number of flags. (As much as villager need). Put a flag in every approachable cell..*

B4. *Solve the previous problem using $2n$ time beats, there n is the number of approachable cells.*

Section C. In this section we can use self variables.

C1. *Find the number of approachable cells and write it to the SPACE variable. Time is limited by $2n$ beats, there n - is the number of approachable cells.*

C2. *Find the number of approachable lake-cells and write it to the WATER variable.*

C3. *Find the shortest distance from house to a flag with variable TARGET=THIS. Write this distance to the variable DIST.*

C4. *Find the approachable lake-cell with maximal nibble. Write its coordinates to the variables NIBBLE_X and NIBBLE_Y. Write the value of nibble to the variable NIBBLE.*

C5. *Let us define a usefulness of lake-cell. This is a specific maximal amount of fish that villager can bring home (ratio of maximal amount of fish can be obtained in this lake and minimal number of beats used for fishing and bring fish home). Find the lake-sell with maximal usefulness. Write its coordinates to the variables USEFULNESS_X and USEFULNESS_Y. Write the value of usefulness to the variable USEFULNESS.*

C6. *Collect n kg of fish in the house. The value of n is recorded in variable FishReq on the house.*

C7. *There is another villager with house in the map. He can fishing too but could not steal it from our house. Collect n kg of fish in the house. The value of n is recorded in variable FishReq on the house.*

C8. *There is another villager with house in the map. He can fishing too and can steal it from our house. Collect n kg of fish in the house. The value of n is recorded in variable FishReq on the house.*

Algorithms and labyrinths. Additional problems.

A. Belov-Kanel, I. Gazhur, I. Ivanov-Pogodaev, A. Malistov

Section A.

A11. (I.Mitrofanov) *There are two robots on the plane. Each robot has two flags. Robots start simultaneously using their own programs. Can we construct the programs such that the robots would meet?*

A12*. *The same (as A11) question for 3-dimensional space.*

A13. *Suppose that there exist labyrinths L_1, L_2 and programs P_1, P_2 for robot without any flags such that robot with P_i explores L_i . Is there exists a program which explores each of the labyrinths L_1, L_2 ?*

A14. *Can the robot with 4 flags explore n -dimensional space in polynomial time? This means that there exists k and C , such that any cell on the distance d from origin would be visited by the robot by a running time of $C \times d^k$.*

A15*. *Can the robot with 3 flags explore n -dimensional space in polynomial time?*

Section C.

C9. *Remove all flags from the map. At the end, write 1 to the variable FINISH .*

C10. *There is a lake on the map. Find the shortest path around this lake (make a loop around this lake). At the end, write the length of this path to the variable PATH.*

Probably, some problems would be presented. Stay tuned for updates.

Комбинаторная геометрия и раскраски графов: от алгебры к вероятности

А.М. Райгородский, а также В. Буланкина и А. Гусев

1 Определения и обозначения

Один из самых известных и ярких объектов в комбинаторной геометрии — это *хроматическое число пространства*. Прежде чем ввести его, напомним, что пространство \mathbb{R}^n , называемое *n-мерным евклидовым пространством*, — это просто множество всех “точек” \mathbf{x} , каждая из которых есть последовательность, состоящая из n действительных чисел: $\mathbf{x} = (x_1, \dots, x_n)$. При этом между любыми двумя точками $\mathbf{x} = (x_1, \dots, x_n)$ и $\mathbf{y} = (y_1, \dots, y_n)$ можно померить расстояние по формуле

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

В частности, при $n = 1$ получаем обычную прямую, при $n = 2$ — обычную плоскость, при $n = 3$ — обычное пространство.

Так вот, хроматическое число \mathbb{R}^n — это величина, обозначаемая $\chi(\mathbb{R}^n)$ и равная минимальному количеству цветов, в которые можно так раскрасить все точки пространства \mathbb{R}^n , чтобы между точками одного цвета не было расстояния 1.

Нам предстоит пройти довольно большой путь от простейших фактов, которые известны многим, хотя и не всем, до весьма продвинутых результатов, полученных буквально в последние месяцы перед ЛКТГ. И методы, которые нам предстоит узнать, будут разнообразны и нетривиальны — от линейной алгебры до теории вероятностей и случайных графов!

2 Задачи до промежуточного финиша

2.1 Простейшие оценки хроматического числа

Задача 1. Докажите, что $\chi(\mathbb{R}^1) = 2$.

Задача 2. Докажите, что $\chi(\mathbb{R}^2) \geq 4$.

Задача 3. Докажите, что $\chi(\mathbb{R}^2) \leq 7$.

Задача 4. Докажите, что $\chi(\mathbb{R}^3) \leq 27$.

Задача 5. Докажите, что $\chi(\mathbb{R}^3) \geq 5$.

Задача 6. Докажите, что $\chi(\mathbb{R}^n)$ конечно при любом n .

Задача 7*. Докажите, что $\chi(\mathbb{R}^n) \leq (\lceil \sqrt{n} \rceil + 1)^n$.

Задача 8. Докажите, что в \mathbb{R}^n есть множество из $n + 1$ точек, попарные расстояния между которыми равны 1, а стало быть, $\chi(\mathbb{R}^n) \geq n + 1$.

Задача 9*. Докажите, что $\chi(\mathbb{R}^n) \geq n + 2$.

2.2 Дистанционные графы специального вида, их простейшие свойства и связь с хроматическим числом пространства

Напомним, что скалярное произведение векторов $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n)$ в \mathbb{R}^n — это выражение

$$(\mathbf{x}, \mathbf{y}) = x_1 y_1 + \dots + x_n y_n.$$

Нетрудно проверить, что всегда

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}). \quad (1)$$

Пусть даны натуральные числа r, s . Для каждого $n \in \mathbb{N}$ обозначим $G(n, r, s)$ граф, у которого множество вершин — это

$$V(n, r) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = r\},$$

а множество ребер — это

$$E(n, r, s) = \{\{\mathbf{x}, \mathbf{y}\} : (\mathbf{x}, \mathbf{y}) = s\}.$$

Иными словами, вершины — это все возможные векторы из нулей и единиц, в каждом из которых ровно r единиц и $n - r$ нулей, а ребрами соединены те и только те пары вершин, скалярное произведение которых равно s . За счет формулы (1) можно сказать, что ребра — это те и только те пары вершин, расстояние между которыми равно $\sqrt{2r - 2s}$. Именно поэтому графы $G(n, r, s)$ называются *дистанционными*. Удобно также иметь следующую интерпретацию графа $G(n, r, s)$. Его вершинами можно считать все возможные r -элементные подмножества множества $\mathcal{R}_n = \{1, 2, \dots, n\}$, а ребрами — пары подмножеств, мощность пересечения которых равна s . Осознайте это!

Напомним, что *независимое множество* вершин графа — это множество, в котором любые две вершины не соединены ребром. *Число независимости* $\alpha(G)$ графа G — это количество вершин в любом его максимальном по мощности независимом множестве. *Хроматическое число* $\chi(G)$ графа G — это минимальное количество цветов, в которые можно так покрасить все вершины графа, чтобы между вершинами одного цвета не было ребер.

Задача 10. Докажите, что для любых n, r, s выполнено $\chi(\mathbb{R}^n) \geq \chi(G(n, r, s))$.

Задача 11. Докажите, что для любого графа $G = (V, E)$ выполнено $\chi(G) \geq \frac{|V|}{\alpha(G)}$.

Задача 12. Найдите $\alpha(G(n, 3, 1))$. Выведите из полученного результата значительное усиление оценки из задачи 9.

Задача 13*. Найдите $\chi(G(n, 3, 1))$ при $n = 2^k$. **Указание.** Воспользуйтесь задачами 11 и 12, а также следующей леммой и индукцией по k .

Лемма 1. Пусть n — четное число и P_n — множество всех неупорядоченных пар $\{a, b\}$ натуральных чисел, не превосходящих n . Тогда найдутся такие множества пар B_1, \dots, B_{n-1} , что

$$P_n = B_1 \sqcup \dots \sqcup B_{n-1},$$

при этом для любого $i = 1, \dots, n-1$ никакие две пары из B_i не содержат общий элемент. Для нечетного n верно разложение

$$P_n = B_1 \sqcup \dots \sqcup B_n,$$

и также для любого $i = 1, \dots, n$ никакие две пары из B_i не содержат общий элемент.

Задача 14.** Найдите как можно более точные оценки (в идеале — формулу) для $\chi(G(n, 3, 1))$ при любых n .

Задача 15. Докажите, что $\alpha(G(n, r, s)) \geq C_{n-s-1}^{r-s-1}$.

Задача 16*. Докажите, что $\alpha(G(n, r, 0)) = C_{n-1}^{r-1}$, если $2r \leq n$.

Задача 17. Докажите, что $\chi(G(n, r, 0)) \leq n - 2r + 2$, если $2r \leq n$.

Задача 18. Докажите, что $\chi(G(n, r, s)) \leq C_r^s C_{n-r}^{r-s} + 1$.

Задача 19. Докажите, что $\chi(G(n, r, s)) \leq C_n^{s+1}$.

Задача 20*. Пусть $k = \lceil \frac{r-1}{s} \rceil$. Докажите, что $\chi(G(n, r, s)) \leq k \cdot C_{\lfloor \frac{n}{k} \rfloor}^{s+1}$.

Задача 21*. Докажите, что $n-r+1 \leq \chi(G(n, r, r-1)) \leq n$ при $n = 2^k$. **Указание.** Воспользуйтесь леммой 1 и индукцией по r и k .

Задача 22.** Найдите $\chi(G(n, r, r-1))$ или хотя бы уточните оценки из задачи 21.

Убедитесь в том, что ни один из полученных Вами результатов не позволяет улучшить нижние оценки величины $\chi(\mathbb{R}^n)$, найденные в задачах 9, 12. Ввиду задачи 11 хорошо бы научиться делать верхние оценки чисел независимости графов $G(n, r, s)$. Оказывается, многие из них получаются с помощью линейно-алгебраического метода. Поэтому в следующем разделе мы напомним базовые понятия линейной алгебры.

2.3 Основы линейной алгебры и ее применения

Скажем, что векторы $\mathbf{x}_1, \dots, \mathbf{x}_t$ в \mathbb{R}^n *линейно независимы*, если равенство $c_1 \mathbf{x}_1 + \dots + c_t \mathbf{x}_t = 0$ возможно лишь при условии, что $c_1 = \dots = c_t = 0$.

Задача 23. Докажите, что максимальное число линейно независимых векторов в \mathbb{R}^n равно n .

Задача 24. Докажите, что если $\mathbf{x}_1, \dots, \mathbf{x}_n$ — любая максимальная система линейно независимых векторов в \mathbb{R}^n , то любой вектор $\mathbf{x} \in \mathbb{R}^n$ можно представить в виде $\mathbf{x} = c_1 \mathbf{x}_1 + \dots + c_n \mathbf{x}_n$, где c_1, \dots, c_n — действительные числа. (Система $\mathbf{x}_1, \dots, \mathbf{x}_n$ называется *базисом* пространства, а выражение $c_1 \mathbf{x}_1 + \dots + c_n \mathbf{x}_n$ — *линейной комбинацией* векторов $\mathbf{x}_1, \dots, \mathbf{x}_n$ с *коэффициентами* c_1, \dots, c_n . В этих терминах любой вектор $\mathbf{x} \in \mathbb{R}^n$ можно представить в виде линейной комбинации векторов базиса.)

Пусть p — простое число, а \mathbb{Z}_p — множество вычетов по модулю p . Пространство \mathbb{Z}_p^n , подобно пространству \mathbb{R}^n , — это просто множество всех последовательностей чисел из \mathbb{Z}_p . Операции сложения “векторов” $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^n$ и умножения их на элементы \mathbb{Z}_p осуществляются, как обычно, — по координатно, — но при этом каждая координата берется по модулю p .

Понятия линейной независимости, линейной комбинации и базиса для \mathbb{Z}_p^n определяются так же, как для \mathbb{R}^n . Только в них все числа c_i — это элементы \mathbb{Z}_p — не \mathbb{R} , — а равенство нулю понимается как равенство нулю по модулю p .

Задача 25. Докажите, что максимальное число линейно независимых векторов в \mathbb{Z}_p^n равно n и что любая максимальная система образует базис.

Задача 26. Пусть $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ — любое независимое множество вершин графа $G(n, 3, 1)$. Докажите, что векторы $\mathbf{x}_1, \dots, \mathbf{x}_t$ линейно независимы в \mathbb{Z}_2^n , откуда $\alpha(G(n, 3, 1)) \leq n$ и это лишь чуть-чуть слабее результата задачи 12!

Пусть $F \in \{\mathbb{R}, \mathbb{Z}_p\}$. Пусть x_1, \dots, x_n — “переменные”. *Одночленом* от этих n переменных называется выражение вида $x_1^{a_1} \cdot \dots \cdot x_n^{a_n}$, где a_1, \dots, a_n — некоторые неотрицательные целые числа. *Многочлен* — это любая линейная комбинация одночленов. При этом многочлен P принадлежит $F[x_1, \dots, x_n]$, если коэффициенты в нем — это элементы F . Складывают и умножают многочлены по обычным правилам. Также, если $P \in F[x_1, \dots, x_n]$, то его можно умножить на любой элемент F . В любом случае правила сложения и умножения коэффициентов многочленов определяются правилами сложения и умножения чисел в множестве F . *Степень* одночлена — это сумма степеней переменных, входящих в него. Степень многочлена — это максимум степеней его одночленов. Многочлен $P \in F[x_1, \dots, x_n]$ равен нулю, если все его коэффициенты равны нулю в F . Многочлены $P_1 \in F[x_1, \dots, x_n], \dots, P_t \in F[x_1, \dots, x_n]$ линейно независимы над F , если $c_1 P_1 + \dots + c_t P_t = 0$ лишь в случае, когда все числа $c_1 \in F, \dots, c_t \in F$ равны нулю в F . Очевидно, что любой многочлен порождается *базисом*, состоящим из одночленов.

Задача 27. Докажите, что если многочлены линейно независимы над своим F , то их количество не превосходит числа одночленов в базисе, которым все эти многочлены порождаются.

Задача 28. Пусть $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ — любое независимое множество вершин графа $G(n, 5, 2)$. Пусть многочлены $P_1 \in \mathbb{Z}_3[y_1, \dots, y_n], P_2 \in \mathbb{Z}_3[y_1, \dots, y_n], \dots, P_t \in \mathbb{Z}_3[y_1, \dots, y_n]$ задаются формулами

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1), \quad i = 1, \dots, t.$$

Например, если $\mathbf{x}_1 = (1, 1, 1, 1, 1, 0, \dots, 0)$, $\mathbf{x}_2 = (0, \dots, 0, 1, 1, 1, 1, 1)$, то

$$P_1(y_1, \dots, y_n) = (y_1 + y_2 + y_3 + y_4 + y_5)(y_1 + y_2 + y_3 + y_4 + y_5 - 1) = y_1^2 + \dots + y_5^2 + 2y_1 y_2 + \dots + 2y_4 y_5 - y_1 - \dots - y_5,$$

$$\begin{aligned} P_2(y_1, \dots, y_n) &= (y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n)(y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n - 1) = \\ &= y_{n-4}^2 + \dots + y_n^2 + 2y_{n-4} y_{n-3} + \dots + 2y_{n-1} y_n - y_{n-4} - \dots - y_n. \end{aligned}$$

Докажите, что многочлены P_1, \dots, P_t линейно независимы над \mathbb{Z}_3 , а стало быть, $\alpha(G(n, 5, 2)) \leq C_n^2 + 2C_n^1$.

Задача 29. Пусть в условиях предыдущей задачи многочлены P_i заменены многочленами P'_i по следующему правилу: каждый одночлен вида y_i^2 преобразован к виду y_i , после чего приведены подобные слагаемые. Докажите, что многочлены P'_1, \dots, P'_t , отвечающие векторам из независимого множества вершин W графа $G(n, 5, 2)$, так же линейно независимы над \mathbb{Z}_3 , как и исходные многочлены P_1, \dots, P_t . Выведите из этого факта оценку $\alpha(G(n, 5, 2)) \leq C_n^2$ и сравните ее с оценкой из задачи 15.

Задача 30. Выведите из результата предыдущей задачи нижнюю оценку для $\chi(\mathbb{R}^n)$, которая значительно уточняет оценку из задачи 12. Убедитесь в том, однако, что ввиду задачи 19 существенных дальнейших продвижений за счет графа $G(n, 5, 2)$ мы не получим.

Задача 31. Пусть $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ — любое независимое множество вершин графа $G(n, 9, 4)$. Пусть многочлены $P_1 \in \mathbb{Z}_5[y_1, \dots, y_n]$, $P_2 \in \mathbb{Z}_5[y_1, \dots, y_n]$, \dots , $P_t \in \mathbb{Z}_5[y_1, \dots, y_n]$ задаются формулами

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1)((\mathbf{x}_i, \mathbf{y}) - 2)((\mathbf{x}_i, \mathbf{y}) - 3), \quad i = 1, \dots, t.$$

Докажите, что многочлены P_1, \dots, P_t линейно независимы над \mathbb{Z}_5 .

Задача 32. Какая верхняя оценка для $\alpha(G(n, 9, 4))$ вытекает из предыдущей задачи?

Задача 33. Пусть в условиях задачи 31 многочлены P_i заменены многочленами P'_i по следующему правилу: каждый одночлен в них, получающийся после раскрытия скобок и приведения подобных слагаемых, конечно, имеет вид $y_1^{a_1} \cdot \dots \cdot y_n^{a_n}$; если среди чисел a_i есть большие либо равные двойке, то заменяем все их единицами, после чего приводим подобные слагаемые. Например, одночлен $y_1^2 y_2^2$ превратится в $y_1 y_2$, и то же самое будет с одночленами $y_1^2 y_2, y_1 y_2^2$, и т.д. Докажите, что многочлены P'_1, \dots, P'_t , отвечающие векторам из независимого множества вершин W графа $G(n, 9, 4)$, так же линейно независимы над \mathbb{Z}_5 , как и исходные многочлены P_1, \dots, P_t . Выведите из этого факта оценку $\alpha(G(n, 9, 4)) \leq C_n^4 + C_n^3 + C_n^2 + C_n^1 + C_n^0$ и сравните ее с оценкой из задачи 15.

Задача 34. Выведите из результата предыдущей задачи нижнюю оценку для $\chi(\mathbb{R}^n)$, которая значительно уточняет оценку из задачи 30. Убедитесь в том, однако, что ввиду задачи 19 существенных дальнейших продвижений за счет графа $G(n, 9, 4)$ мы не получим.

Задача 35. Пусть r и s таковы, что $r - s = p$, где p — простое число, причем $r - 2p < 0$. Докажите, что тогда $\alpha(G(n, r, s)) \leq \sum_{k=0}^{p-1} C_n^k$. Сравните эту оценку с оценкой из задачи 15.

Задача 36*. Исследуйте нижние оценки величины $\chi(\mathbb{R}^n)$, которые вытекают из результатов предыдущей задачи. Как эти оценки соотносятся с оценками из задачи 19?

3 Задачи после промежуточного финиша

До промежуточного финиша мы убедились в том, насколько важны числа независимости графов для получения нижних оценок хроматического числа пространства. При этом мы рассматривали разные последовательности дистанционных графов — последовательности $\{G(n, r, s)\}_{n=1}^{\infty}$ с заданными наперед r и s . Интересно понять: а как изменятся числа независимости, если, вместо графов $G(n, r, s)$, брать их “остовные” подграфы, т.е. вершины сохранять, а ребра частично удалять. Кажется очевидным, что числа независимости должны сильно вырасти, коль скоро мы удалим много ребер. Однако, удивительным образом, иногда это так, а иногда и совершенно иначе! Для того, чтобы получить соответствующие результаты, займемся немного случайными графами и теорией вероятностей.

3.1 Случайный граф Эрдеша–Реньи и некоторые его вероятностные характеристики

Пусть $V_n = \{1, \dots, n\}$ — множество вершин. Теоретически на нем можно построить C_n^2 ребер, если запретить кратные ребра, петли и ориентацию. Давайте каждое из этих C_n^2 потенциальных ребер проводить с вероятностью $p \in [0, 1]$, общей для всех ребер. При этом появляться или не появляться ребра будут независимо друг от друга. Пусть $G = (V_n, E)$ — какой-то граф, который может случайно возникнуть в результате описанной только что вероятностной процедуры. Обозначим вероятность его возникновения $\mathbb{P}(G)$. Понятно, что она равна $p^{|E|}(1-p)^{C_n^2-|E|}$. Если A — какое-то свойство графа, то его вероятность — $\mathbb{P}(A)$ — это сумма по всем графам G , обладающим свойством A , вероятностей этих графов.

Обозначим Ω_n множество всех графов на вершинах V_n . Любая функция X , определенная на Ω_n и принимающая действительные значения, называется *случайной величиной*. Например, число треугольников в графе или число его связных компонент, или его число независимости — это случайные величины. При этом надо четко понимать, что величины случайны лишь потому, что априори мы не знаем, какой граф появится на свет. Когда граф уже возник, значение X определено однозначно!

У случайных величин есть “средние значения” — так называемые *математические ожидания*. Математическое ожидание величины X — это число $\mathbb{M}X$, определяемое по формуле $\mathbb{M}X = \sum_{G \in \Omega_n} X(G)\mathbb{P}(G)$. Мы просто складываем значения функции X на графах, помноженные на вероятности этих графов. Естественно, это некое взвешенное среднее (веса — вероятности) — своего рода центр масс. Давайте научимся считать математические ожидания и применять полученные результаты для изучения свойств случайных графов.

Задача 37. Докажите, что если случайная величина — это константа c , то $\mathbb{M}c = c$.

Задача 38. Пусть X_1, X_2 — случайные величины, а c_1, c_2 — фиксированные числа. Разумеется, $c_1X_1 + c_2X_2$ — это тоже случайная величина. Докажите, что ее математическое ожидание равно $c_1\mathbb{M}X_1 + c_2\mathbb{M}X_2$. Это свойство называется *линейностью* математического ожидания.

Задача 39. С помощью линейности математического ожидания найдите математические ожидания а) числа треугольников в случайном графе; б) числа связных компонент случайного графа, каждая из которых является циклом на k вершинах (k — фиксированное заданное наперед число); в) числа независимых множеств вершин в случайном графе, каждое из которых имеет мощность k (k — фиксированное заданное наперед число).

Задача 40. Докажите *неравенство Маркова*: если X — случайная величина, принимающая неотрицательные значения, и дано положительное число a , то $\mathbb{P}(X \geq a) \leq \frac{\mathbb{M}X}{a}$.

Задача 41. Докажите с помощью неравенства Маркова, что если $p = \frac{1}{2}$, то $\mathbb{P}(\alpha(G) \leq 2 \log_2 n) \rightarrow 1$ при $n \rightarrow \infty$ (говорят “почти наверное $\alpha(G) \leq 2 \log_2 n$ ”).

Заметим, что на самом деле при $p = \frac{1}{2}$ почти наверное $\alpha(G) \geq (2 - \varepsilon) \log_2 n$ при сколь угодно малом наперед заданном $\varepsilon > 0$. Точнее, — и это нам понадобится позже, — справедлива

Теорема 1. Для любого $\varepsilon > 0$ при больших n выполнено неравенство

$$\mathbb{P}(\alpha(G) \geq (2 - \varepsilon) \log_2 n) > 1 - 2^{-n}.$$

Таким образом, при $p = \frac{1}{2}$ почти наверное число независимости — это примерно $2 \log_2 n$. Иными словами, что происходит? Мы берем полный граф на n вершинах и часть его ребер удаляем с вероятностью $\frac{1}{2}$. У типичного графа, который остается в результате этой процедуры, примерно $\frac{C_n^2}{2}$ ребер — вдвое меньше, чем у полного графа. И у типичного же графа число независимости в логарифм раз больше числа независимости исходного полного графа (у него-то оно равно 1). Что ж, ребер вдвое меньше, и число независимости выросло: вполне естественно! Оказывается, что для некоторых $G(n, r, s)$ при случайном удалении ребер имеет место точно такой же “ожидаемый” результат (число независимости возрастает в примерно логарифм от числа вершин раз). Но чудо в том, что так получается не всегда! Для многих $G(n, r, s)$ число независимости вовсе не изменяется! Ниже мы вместе изучим примеры обеих ситуаций.

3.2 Случайные подграфы графа $G(n, 3, 0)$

Пусть $G_{1/2}(n, 3, 0)$ — случайный подграф графа $G(n, 3, 0)$, полученный взаимно независимым удалением ребер из графа $G(n, 3, 0)$, каждого — с вероятностью $1/2$.

Задача 42. Если у Вас получилась задача 16, то вспомните просто, что $\alpha(G(n, 3, 0)) = C_{n-1}^2$. Иначе попробуйте решить этот частный случай той задачи.

В серии следующих ниже задач мы докажем, что почти наверное $\alpha(G_{1/2}(n, 3, 0)) \leq C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. Это и есть то самое удивительное явление: никакого роста в логарифм раз нет; если и есть рост, то лишь в такое количество раз, которое само стремится к 1 при $n \rightarrow \infty$! Можно доказать и гораздо более сильные факты, но это уже совсем трудно, а нам бы суть почувствовать!

В дальнейшем мы будем для краткости опускать целые части у величин, которые должны быть целыми. Например, запись $C_{\log_2 n}^k$ означает, смотря по контексту, что на самом деле речь идет о верхней или нижней целой части числа $\log_2 n$. Ни одна из выкладок от такого огрубления не пострадает.

Задача 43. Положим $k = C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. Считаем, что k целое (ср. замечание перед задачей). Пусть $A \subset V(n, 3)$ — произвольное множество вершин графа $G(n, 3, 0)$, имеющее мощность k . Обозначим $r(A)$ количество ребер графа $G(n, 3, 0)$, оба конца которых попадают в A . Поскольку $|A| = k > \alpha(G(n, 3, 0))$, ясно, что $r(A) > 0$. Пусть X_k — случайная величина, равная числу независимых множеств размера k в графе $G_{1/2}(n, 3, 0)$. Докажите, что

$$\mathbb{M}X_k = \sum_{A \subset V(n, 3): |A|=k} \left(\frac{1}{2}\right)^{r(A)}. \quad (2)$$

Задача 44. Докажите, что наша цель будет достигнута, едва мы докажем, что $\mathbb{M}X_k \rightarrow 0$ при $n \rightarrow \infty$.

Ясно, что надо научиться оценивать *снизу* величины $r(A)$. Для каждого A обозначим $B = B(A)$ любое (раз и навсегда избранное) подмножество множества A , которое является независимым в $G(n, 3, 0)$ и имеет максимальную мощность среди всех подобных подмножеств множества A .

Задача 45. Пусть $A \subset V(n, 3)$, $|A| = k$. Пусть $B = B(A)$. Заметим, что $k \approx \frac{n^2}{2}$. Предположим, что $|B|$ значительно меньше k : например, пусть $|B| < n^{1.9}$ (здесь странное число 1.9 взято почти с потолка, лишь бы строго меньше, чем 2). Докажите, что тогда при больших n заведомо выполнено неравенство $r(A) \geq \frac{k^2}{3|B|}$ (при правильном подходе тройку в знаменателе можно “почти” заменить на двойку, но да Бог с ним).

Задача 46. Пусть $A \subset V(n, 3)$, $|A| = k$. Пусть $B = B(A)$. Пусть $|B| > 9n$, а еще лучше (в дополнение к предыдущей задаче), $|B| \geq n^{1.9}$. Докажите, что $r(A) \geq (|B| - 9n)(|A| - |B|)$.

Задача 47. Разбейте сумму (2) на две части: в первой части будут лишь те A , для которых $|B| < n^{1.9}$; во второй — все остальные. К слагаемым в обеих частях примените оценки из соответствующих задач и убедитесь, что вся сумма (2) таки стремится к нулю, и все получилось! На что в выкладках можно было заменить порог $n^{1.9}$?

3.3 Случайные подграфы графа $G(n, 3, 1)$

Пусть $G_{1/2}(n, 3, 1)$ — случайный подграф графа $G(n, 3, 1)$, полученный взаимно независимым удалением ребер из графа $G(n, 3, 1)$, каждого — с вероятностью $1/2$. Казалось бы, все то же, что и с графами $G(n, 3, 0)$. Ан нет!

Вспомним, что $\alpha(G(n, 3, 1)) \approx n$ (см. задачу 12).

Задача 48*. Напишите аналог равенства (2) и докажите аналог оценки из задачи 45. Убедитесь в итоге, что существует $c > 0$, с которым почти наверное $\alpha(G_{1/2}(n, 3, 1)) \leq cn \log_2 n$.

Задача 49. Докажите, что в графе $G(n, 3, 1)$ есть примерно $\frac{n}{2}$ полных подграфов, в каждом из которых примерно $\frac{n}{4}$ вершин и каждые два из которых не соединены ребрами.

Задача 50. С помощью предыдущей задачи и теоремы 1 докажите, что для любого $\varepsilon > 0$ почти наверное $\alpha(G_{1/2}(n, 3, 1)) \geq (1 - \varepsilon)n \log_2 n$.

Таким образом, для $G_{1/2}(n, 3, 1)$, как и для случайного графа Эрдеша–Реньи, имеем снова увеличение числа независимости в примерно логарифм от числа вершин раз. Такие вот удивительные эффекты!

Задача 51*. Попробуйте улучшить в константу раз результат задачи 50.

3.4 Случайные подграфы графа $G(n, 2, 1)$

Задача 52. Найдите $\alpha(G(n, 2, 1))$.

Задача 53. Пусть $r(A)$ имеет тот же смысл, что и аналогичная величина в формуле (2). Докажите, что всегда $r(A) \geq \frac{2|A|^2}{n} - |A|$.

Задача 54. Выведите из предыдущей задачи неравенство $\alpha(G_{1/2}(n, 2, 1)) \leq (\frac{1}{2} + \varepsilon)n \log_2 n$, справедливое при каждом $\varepsilon > 0$ почти наверное.

Задача 55*. Докажите нижнюю оценку для $\alpha(G_{1/2}(n, 2, 1))$, имеющую порядок роста $cn \log_2 n$ с некоторым $c > 0$.

Задача 56.** Найдите константу c в утверждении: для любого $\varepsilon > 0$ почти наверное

$$(c - \varepsilon)n \log_2 n \leq \alpha(G_{1/2}(n, 2, 1)) \leq (c + \varepsilon)n \log_2 n.$$

Список цитированной литературы

- [1] А.М. Райгородский, *Хроматические числа*, Москва, МЦНМО, 2003.
- [2] А.М. Райгородский, *Линейно-алгебраический метод в комбинаторике*, Москва, МЦНМО, 2007.
- [3] А.М. Райгородский, *Вероятность и алгебра в комбинаторике*, Москва, МЦНМО, 2010.
- [4] А.М. Райгородский, *Модели случайных графов*, Москва, МЦНМО, 2011.

Комбинаторная геометрия и раскраски графов: от алгебры к вероятности

А.М. Райгородский, а также В. Буланкина и А. Гусев

1 Определения и обозначения

Один из самых известных и ярких объектов в комбинаторной геометрии — это *хроматическое число пространства*. Прежде чем ввести его, напомним, что пространство \mathbb{R}^n , называемое *n-мерным евклидовым пространством*, — это просто множество всех “точек” \mathbf{x} , каждая из которых есть последовательность, состоящая из n действительных чисел: $\mathbf{x} = (x_1, \dots, x_n)$. При этом между любыми двумя точками $\mathbf{x} = (x_1, \dots, x_n)$ и $\mathbf{y} = (y_1, \dots, y_n)$ можно померить расстояние по формуле

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

В частности, при $n = 1$ получаем обычную прямую, при $n = 2$ — обычную плоскость, при $n = 3$ — обычное пространство.

Так вот, хроматическое число \mathbb{R}^n — это величина, обозначаемая $\chi(\mathbb{R}^n)$ и равная минимальному количеству цветов, в которые можно так раскрасить все точки пространства \mathbb{R}^n , чтобы между точками одного цвета не было расстояния 1.

Нам предстоит пройти довольно большой путь от простейших фактов, которые известны многим, хотя и не всем, до весьма продвинутых результатов, полученных буквально в последние месяцы перед ЛКТГ. И методы, которые нам предстоит узнать, будут разнообразны и нетривиальны — от линейной алгебры до теории вероятностей и случайных графов!

2 Задачи до промежуточного финиша

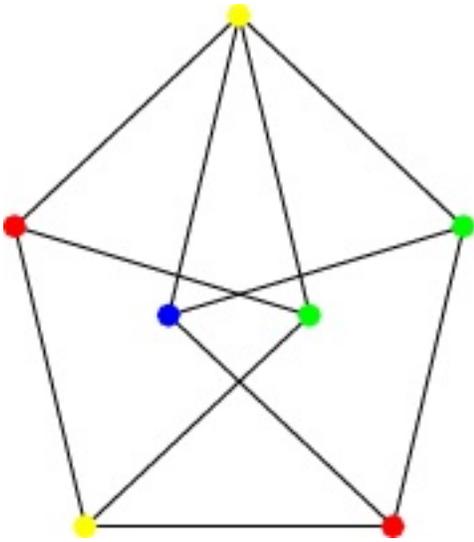
2.1 Простейшие оценки хроматического числа

Задача 1. Докажите, что $\chi(\mathbb{R}^1) = 2$.

Решение. Очевидно, что в один цвет раскрасить нельзя, поскольку точки 1 и 2 должны быть разных цветов. А в два можно. Для этого разобьем всю прямую на полуинтервалы $[a; a + 1)$ для всех целых точек a и раскрасим эти интервалы по очереди в черный и белый цвета.

Задача 2. Докажите, что $\chi(\mathbb{R}^2) \geq 4$.

Решение. Очевидно, что приведенную ниже фигуру нельзя правильным образом раскрасить в 3 цвета.



Задача 3. Докажите, что $\chi(\mathbb{R}^2) \leq 7$.

Решение. Каждый желающий без труда может убедиться, что подходит следующая раскраска:



Задача 4. Докажите, что $\chi(\mathbb{R}^3) \leq 27$.

Решение. Задача является частным случаем задачи 7.

Задача 5. Докажите, что $\chi(\mathbb{R}^3) \geq 5$.

Решение. Задача является частным случаем задачи 9.

Задача 6. Докажите, что $\chi(\mathbb{R}^n)$ конечно при любом n .

Решение. Давайте сразу решим задачу 7, а 6 будет из нее очевидным следствием.

Задача 7*. Докажите, что $\chi(\mathbb{R}^n) \leq (\lceil \sqrt{n} \rceil + 1)^n$.

Решение. Зафиксируем два числа $k \in \mathbb{N}$ и $p \in \mathbb{R}$, после чего разобьем пространство \mathbb{R}^n на кубики с ребром kp . Теперь каждый кубик разделим на k^n меньших кубиков, с ребром p у каждого.

Зафиксируем один большой кубик и все маленькие кубики внутри него раскрасим каждый в свой цвет (всю внутренность и грани, прилегающие к вершине с наименьшей суммой координат. В этот же цвет красим соединяющие их рёбра, при этом вершину красим только одну, как раз ту, у которой наименьшая сумма координат), после чего точно такими же цветами и в таком же порядке раскрасим все маленькие кубики внутри остальных больших кубов. Тогда, чтобы раскраска была правильной, необходимо, чтобы выполнялось два неравенства: $p\sqrt{n} \leq 1$, $(k-1)p \geq 1$.

Но для $k = \lceil \sqrt{n} \rceil + 1$ и $p = \frac{1}{\sqrt{n}}$ эти неравенства, очевидно, выполнены.

Задача 8. Докажите, что в \mathbb{R}^n есть множество из $n+1$ точек, попарные расстояния между которыми равны 1, а стало быть, $\chi(\mathbb{R}^n) \geq n+1$.

Решение. Давайте построим такое множество точек в явном виде. Положим

$$\begin{aligned} A_1 &= \left(\frac{\sqrt{2}}{2}; 0; 0; \dots; 0; 0 \right) \\ A_2 &= \left(0; \frac{\sqrt{2}}{2}; 0; \dots; 0; 0 \right) \\ &\quad \dots \\ A_n &= \left(0; 0; 0; \dots; 0; \frac{\sqrt{2}}{2} \right) \end{aligned}$$

Понятно, что попарные расстояния между этими n точками равны по 1. А $(n+1)$ -ю точку найдем в виде $S = (a; a; a; \dots; a; a)$.

$$\begin{aligned} SA_i &= \sqrt{(n-1)a^2 + \left(a - \frac{\sqrt{2}}{2}\right)^2} = 1 \\ na^2 - \sqrt{2}a - \frac{1}{2} &= 0. \end{aligned}$$

Несложно убедиться, что дискриминант этого квадратного уравнения положителен. И у нас найдутся сразу две точки S_1 и S_2 , от каждой из которых до любой A_i расстояние равно 1.

Задача 9*. Докажите, что $\chi(\mathbb{R}^n) \geq n+2$.

Решение. Возьмем две фигуры, аналогичные построенным в задаче 8, $S_1S_2A_1 \dots A_n$ и равную ей $T_1T_2B_1 \dots B_n$. Разместим их в пространстве так, чтобы точка S_1 совпала с точкой T_1 , а расстояние S_2T_2 равнялось 1. Если мы захотим раскрасить пространство в $n+1$ цвет, то точки S_1 и S_2 будут одного цвета, и точки T_1 и T_2 будут одного цвета. Значит S_2 и T_2 будут одного цвета, но это невозможно.

2.2 Дистанционные графы специального вида, их простейшие свойства и связь с хроматическим числом пространства

Напомним, что скалярное произведение векторов $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n)$ в \mathbb{R}^n — это выражение

$$(\mathbf{x}, \mathbf{y}) = x_1y_1 + \dots + x_ny_n.$$

Нетрудно проверить, что всегда

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}). \quad (1)$$

Пусть даны натуральные числа r, s . Для каждого $n \in \mathbb{N}$ обозначим $G(n, r, s)$ граф, у которого множество вершин — это

$$V(n, r) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = r\},$$

а множество ребер — это

$$E(n, r, s) = \{(\mathbf{x}, \mathbf{y}) : (\mathbf{x}, \mathbf{y}) = s\}.$$

Иными словами, вершины — это все возможные векторы из нулей и единиц, в каждом из которых ровно r единиц и $n - r$ нулей, а рёбрами соединены те и только те пары вершин, скалярное произведение которых равно s . За счет формулы (1) можно сказать, что рёбра — это те и только те пары вершин, расстояние между которыми равно $\sqrt{2r - 2s}$. Именно поэтому графы $G(n, r, s)$ называются *дистанционными*. Удобно также иметь следующую интерпретацию графа $G(n, r, s)$. Его вершинами можно считать все возможные r -элементные подмножества множества $\mathcal{R}_n = \{1, 2, \dots, n\}$, а рёбрами — пары подмножеств, мощность пересечения которых равна s . Осознайте это!

Напомним, что *независимое множество* вершин графа — это множество, в котором любые две вершины не соединены ребром. *Число независимости* $\alpha(G)$ графа G — это количество вершин в любом его максимальном по мощности независимом множестве. *Хроматическое число* $\chi(G)$ графа G — это минимальное количество цветов, в которые можно так покрасить все вершины графа, чтобы между вершинами одного цвета не было ребер.

Задача 10. Докажите, что для любых n, r, s выполнено $\chi(\mathbb{R}^n) \geq \chi(G(n, r, s))$.

Решение. Если сделать гомотетию графа $G(n, r, s)$ с коэффициентом $\frac{1}{\sqrt{2(r-s)}}$, то все его ребра станут равны по 1. И при этом он будет вложен в пространство \mathbb{R}^n . Поэтому, если мы сможем раскрасить все пространство в k цветов, то мы все вершины графа $G(n, r, s)$ и подавно сможем раскрасить.

Задача 11. Докажите, что для любого графа $G = (V, E)$ выполнено $\chi(G) \geq \frac{|V|}{\alpha(G)}$.

Решение. Каждый цвет будет являться независимым множеством, поэтому его размер не превосходит $\alpha(G)$. Но тогда если мы количество вершин каждого цвета увеличим до $\alpha(G)$, то суммарное количество вершин у нас увеличится и их станет $\chi(G) \cdot \alpha(G) \geq |V|$.

Задача 12. Найдите $\alpha(G(n, 3, 1))$. Выведите из полученного результата значительное усиление оценки из задачи 9.

Решение. Ответ зависит от того, с чем сравнимо n по модулю 4. Будем доказывать по индукции, что

$$\begin{aligned} n \equiv 0 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n, \\ n \equiv 1 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n - 1, \\ n \equiv 2 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n - 2, \\ n \equiv 3 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n - 2. \end{aligned}$$

База для $k = 1, 2, 3, 4$ не представляет сложности. Будем делать переход от всех $k \leq n - 1$ к $k = n$.

Будем помнить, что вершины нашего графа можно трактовать и как вектора, и как 3-элементные подмножества. Каждый вектор состоит из нулей и единиц. Зафиксируем любое независимое множество. Любые две вершины в нём либо не пересекаются, либо пересекаются ровно по двум элементам.

Рассмотрим две пересекающиеся вершины из независимого множества. Без ограничения общности можем считать, что это вектора (и соответствующие им 3-элементные подмножества)

$$(1, 1, 1, 0, \dots, 1) \text{ и } (1, 1, 0, 1, 0, \dots, 0).$$

Если с этими двумя вершинами больше никакие не пересекаются, то у нас есть две вершины и осталось $n - 4$ элемента. И дальше по предположению индукции получаем утверждение задачи. Если есть еще одна вершина, пересекающаяся с этими двумя, то это одна из трех вершин

$$(1, 1, 0, 0, 1, 0, \dots, 0), (1, 0, 1, 1, 0, \dots, 0) \text{ или } (0, 1, 1, 1, 0, \dots, 0)$$

В первом случае все остальные вершины, имеющие элементны среди первых четырех, имеют вид $(1, 1, 0, 0, \dots, 0, 1, 0, \dots, 0)$. Если таких вершин k , то на них уйдет $k + 2$ элемента, по предположению индукции мы легко закончим оценку.

Во втором и третьем случае, если есть вершины, в которых присутствуют элементы среди первых четырех, то это лишь вершины, дополняющие систему до набора

$$\begin{aligned} (0, 1, 1, 1, 0, \dots, 0), \\ (1, 0, 1, 1, 0, \dots, 0), \\ (1, 1, 0, 1, 0, \dots, 0), \\ (1, 1, 1, 0, 0, \dots, 0). \end{aligned} \tag{1}$$

Таким образом количество элементов уменьшилось на 4, а вершин увеличилось не более, чем на 4. И снова по предположению индукции заканчиваем оценку.

Для завершения доказательства осталось привести пример. Давайте и его построим по индукции. Читатель без труда самостоятельно построит примеры для $k = 1, 2, 3, 4$. Мы же давайте покажем, как переходить от $k \rightarrow k + 4$. Но для этого достаточно на первых четырех координатах построить 4 вектора, как в (1).

Оценка на хроматическое число пространства получается такая:

$$\chi(\mathbb{R}^n) \geq \chi(G(n, 3, 1)) \geq \frac{C_n^3}{\alpha(G(n, 3, 1))} \geq \frac{(n-1)(n-2)}{6}.$$

Задача 13*. Найдите $\chi(G(n, 3, 1))$ при $n = 2^k$. **Указание.** Воспользуйтесь задачами 11 и 12, а также следующей леммой и индукцией по k .

Решение. Решение данной задачи вы можете прочитать в статье [6].

Лемма 1. Пусть n — четное число и P_n — множество всех неупорядоченных пар $\{a, b\}$ натуральных чисел, не превосходящих n . Тогда найдутся такие множества пар B_1, \dots, B_{n-1} , что

$$P_n = B_1 \sqcup \dots \sqcup B_{n-1},$$

при этом для любого $i = 1, \dots, n-1$ никакие две пары из B_i не содержат общий элемент. Для нечетного n верно разложение

$$P_n = B_1 \sqcup \dots \sqcup B_n,$$

и также для любого $i = 1, \dots, n$ никакие две пары из B_i не содержат общий элемент.

Задача 14.** Найдите как можно более точные оценки (в идеале — формулу) для $\chi(G(n, 3, 1))$ при любых n .

Решение. Задача с двумя звездочками, а это значит, что в случае её решения вы получили бы новый результат.

Задача 15. Докажите, что $\alpha(G(n, r, s)) \geq C_{n-s-1}^{r-s-1}$.

Решение. Рассмотрим лишь те вершины, у которых на первых $s+1$ координатах стоят 1. Всего таких вершин C_{n-s-1}^{r-s-1} . И понятно, что скалярное произведение любых двух векторов не меньше $s+1$, поэтому никакие две вершины не соединены ребром.

Задача 16*. Докажите, что $\alpha(G(n, r, 0)) = C_{n-1}^{r-1}$, если $2r \leq n$.

Решение. Доказательство данной задачи вы можете прочитать в статье [6].

Обозначим через B любое (раз и навсегда выбранное) подмножество множества вершин $V(n, r)$, которое является независимым в $G(n, r, 0)$ и имеет мощность $\alpha(G(n, r, 0))$.

Лемма. Для каждого $s, 1 \leq s \leq n$, рассмотрим множество $A_s = \{s, s+1, \dots, s+r-1\}$, где сумма берется по модулю n . Тогда в B не может содержаться более r множеств A_s .

Доказательство. Зафиксируем некоторое A_s из B . Из всех остальных множеств A_k , пересекающих A_s , составим $r-1$ пар $\{A_{s-i}, A_{s+r-i}\}$, где $1 \leq i \leq r-1$. Утверждение леммы теперь вытекает из того, что B не может содержать более одного элемента из каждой пары.

Теперь из леммы выведем утверждение задачи. Выберем случайным образом перестановку σ на множестве $\{1, 2, \dots, n\}$ и число $i \in \{1, 2, \dots, n\}$. Пусть $A = \{\sigma(i), \sigma(i+1), \dots, \sigma(i+r-1)\}$, где сумма, как и раньше, берется по модулю n . В силу произвольности выбора σ из леммы вытекает, что $P(A \in B) \leq \frac{r}{n}$. Но A выбирается равновероятно из всех r -элементных подмножеств. Поэтому,

$$\frac{r}{n} \geq \mathbb{P}(A \in B) = \frac{|B|}{C_n^r}$$

и

$$|B| \leq \frac{r}{n} C_n^r = C_{n-1}^{r-1}.$$

Задача 17. Докажите, что $\chi(G(n, r, 0)) \leq n - 2r + 2$, если $2r \leq n$.

Решение. Давайте в первый цвет покрасим все вершины, у которых первая координата равна 1. Во второй цвет покрасим все нераскрашенные вершины, у которых вторая координата равна 1. И так далее, до $(n - 2r + 1)$ -го цвета. Понятно, что тогда среди вершин одного цвета рёбер не будет. У нас остался еще один цвет. Какие вершины остались не покрашены? Лишь те, у которых все единички среди последних $2r - 1$ координат. Но понятно, что никакие две такие вершины не соединены ребром. Поэтому мы можем все оставшиеся вершины покрасить в последний цвет.

Задача 18. Докажите, что $\chi(G(n, r, s)) \leq C_r^s C_{n-r}^{r-s} + 1$.

Решение. Что такое $C_r^s C_{n-r}^{r-s}$? Это просто степень каждой вершины графа $G(n, r, s)$. Но понятно, что если в графе степень каждой вершины не превосходит d , то его можно раскрасить в $d + 1$ цвет. Действительно, давайте поочередно красить все вершины графа. Для любой вершины, которую мы хотим раскрасить, существует минимум 1 цвет, с которым она не соединена. Давайте в этот цвет и раскрасим.

Задача 19. Докажите, что $\chi(G(n, r, s)) \leq C_n^{s+1}$.

Решение. Выберем из \mathcal{R}_n все $(s + 1)$ -элементные подмножества и занумеруем их от 1 до C_n^{s+1} . А теперь покрасим в первый цвет все вершины, содержащие первое подмножество, во второй – все непокрашенные вершины, содержащие второе подмножество, и так далее. Понятно, что все вершины таким образом будут покрашены, и внутри одного цвета рёбер не будет.

Задача 20*. Пусть $k = \lfloor \frac{r-1}{s} \rfloor$. Докажите, что $\chi(G(n, r, s)) \leq k \cdot C_{\lfloor \frac{n}{k} \rfloor}^{s+1}$.

Решение Доказательство данной задачи вы можете прочитать в статье [6].

Задача 21*. Докажите, что $n - r + 1 \leq \chi(G(n, r, r - 1)) \leq n$ при $n = 2^k$. **Указание.** Воспользуйтесь леммой 1 и индукцией по r и k .

Решение. Для получения нижней оценки достаточно заметить, что в графе есть клика размера $n - r + 1$. Для этого рассмотрим те вершины, у которых на первых $r - 1$ координатах стоят единички. Таких вершин ровно $n - r + 1$ и все они попарно соединены ребром.

Рассмотрим случай $r = 2$. Покажем, что из леммы 1 следует неравенство $\chi(G(n, 2, 1)) \leq n$. В самом деле, вершины графа $G(n, 2, 1)$ можно отождествить с множеством пар натуральных чисел $1, \dots, n$, при этом две вершины соединены ребром тогда и только тогда, когда соответствующие пары имеют общий элемент. Таким образом, если взять в качестве цветов $\chi_i = B_i$ из леммы 1, то весь граф окажется покрашенным в $n - 1$ цвет для $n = 2m$ и в n цветов для $n = 2m + 1$.

Доказательство верхней оценки мы будем проводить индукцией по параметру r . База индукции доказана выше. Пусть верхняя оценка верна для всех $r < k$. Докажем шаг индукции, для этого покрасим граф $G(n, k, k - 1)$.

Пусть $n = 2^l$. Граф $G(n, k, k-1)$ мы будем красить индукцией по параметру l . Для доказательства базы индукции рассмотрим максимальное l_0 такое, что $2^{l_0} < k$. При таком l_0 имеем $\chi(G(2^{l_0}, k, k-1)) = 0$, и верхняя оценка выполнена. Предположение индукции: $\chi(G(2^{l-1}, k, k-1)) \leq 2^{l-1}$. Разобьем множество элементов на две части:

$$\begin{aligned} A_1 &= \{1, \dots, n/2\}, \\ A_2 &= \{n/2 + 1, \dots, n\}. \end{aligned}$$

Разобьем все вершины нашего графа на $k+1$ непересекающихся множеств

$$V_j = \{v \in V(G(n, k, k-1)) : |v \cap A_1| = j\}, \quad j = 0, \dots, k.$$

Отметим, что при $l = l_0 + 1$ некоторые V_j пусты. Это только улучшит результат, поэтому дальнейшие рассуждения будем проводить так, как будто все V_j не пусты.

Рассмотрим граф $G(n/2, j, j-1)$ при $j = 1, \dots, k-1$. По предположению индукции $\chi(G(n/2, j, j-1)) \leq n/2$, и все j -элементные подмножества множества A_1 можно так покрасить в $n/2$ цветов $\varphi_1, \dots, \varphi_{n/2}$, что любые два таких подмножества одного цвета не пересекаются по $j-1$ элементу. Обозначим $W_{j,1}^\nu$ семейство всех таких подмножеств, покрашенных в цвет φ_ν . Также введем граф $G(n/2, k-j, k-j-1)$, построенный на множестве элементов A_2 . Тогда все $(k-j)$ -элементные подмножества множества A_2 так красятся в цвета $\psi_1, \dots, \psi_{n/2}$, что покрашенные в один цвет подмножества не пересекаются по $k-j-1$ элементу. Обозначим $W_{k-j,2}^\mu$ семейство $(k-j)$ -элементных подмножеств A_2 , покрашенных в цвет ψ_μ .

Для $\nu \in \{1, \dots, n\}$ положим $U_j^{1,\nu} = \{w_1 \sqcup w_2 : w_1 \in W_{j,1}^\nu, w_2 \in W_{j,2}^\nu\}$. Пусть $U_j^1 = \bigsqcup_{\nu=1}^{n/2} U_j^{1,\nu}$. Понятно,

что любые два множества из набора U_j^1 не пересекаются по $k-1$ элементу. Допустим, что это не так, то есть найдутся вершины $v, w \in U_j^1$, для которых $|v \cap w| = k-1$. Тогда либо $v \cap A_1 = w \cap A_1$, либо $v \cap A_2 = w \cap A_2$, то есть не совпадающие “половинки” этих вершин покрашены в одинаковый цвет. Пусть, например, $v \cap A_1 = w \cap A_1$, тогда $v \cap A_2$ и $w \cap A_2$ имеют не более $k-j-2$ общих элементов. Стало быть, вершины v и w не могут пересекаться по $k-1$ элементу, противоречие. Аналогично разбирается случай, когда $v \cap A_2 = w \cap A_2$.

Таким же образом можно получить набор U_j^2 , объединяя множества из $W_{j,1}^1$ с множествами $W_{k-j,2}^2$, множества из $W_{j,1}^2$ с множествами $W_{k-j,2}^3, \dots$, множества из $W_{1,j}^{n/2}$ с множествами $W_{k-j,2}^1$. Аналогично, с помощью циклических сдвигов определяются $U_j^3, \dots, U_j^{n/2}$. Здесь по-прежнему $j = 1, \dots, k-1$. Из предположения индукции по параметру n существуют наборы U_0^i и U_k^i , состоящие соответственно из подмножеств A_2 и A_1 , не пересекающихся по $k-1$ элементу при каждом $i = 1, \dots, n/2$.

Окончательно определим при $i = 1, \dots, n/2$ цвет χ_i как объединение наборов с четными индексами:

$$\chi_i = U_0^i \cup U_2^i \cup U_4^i \cup \dots$$

При $i = n/2 + 1, \dots, n$ объединим наборы с нечетными индексами:

$$\chi_i = U_1^{i-n/2} \cup U_3^{i-n/2} \cup U_5^{i-n/2} \dots$$

Очевидно, что мы потратили не более n цветов для раскраски нашего графа, что завершает индукцию по параметру n , а стало быть, и по параметру r . Тем самым мы получаем верхнюю оценку.

Задача 22.** Найдите $\chi(G(n, r, r - 1))$ или хотя бы уточните оценки из задачи 21.

Решение. Задача с двумя звездочками, а это значит, что в случае её решения вы получили бы новый результат.

Убедитесь в том, что ни один из полученных Вами результатов не позволяет улучшить нижние оценки величины $\chi(\mathbb{R}^n)$, найденные в задачах 9 и 12. Ввиду задачи 11 хорошо бы научиться делать верхние оценки чисел независимости графов $G(n, r, s)$. Оказывается, многие из них получаются с помощью линейно-алгебраического метода. Поэтому в следующем разделе мы напомним базовые понятия линейной алгебры.

2.3 Основы линейной алгебры и её применения

Скажем, что векторы $\mathbf{x}_1, \dots, \mathbf{x}_t$ в \mathbb{R}^n *линейно независимы*, если равенство $c_1\mathbf{x}_1 + \dots + c_t\mathbf{x}_t = 0$ возможно лишь при условии, что $c_1 = \dots = c_t = 0$.

Задача 23. Докажите, что максимальное число линейно независимых векторов в \mathbb{R}^n равно n .

Решение. Очевидно, что базисные вектора $\mathbf{e}_i = (0, 0, \dots, 0, 1, 0, \dots, 0)$, где 1 стоит на i -ом месте, которые мы берём по всем i от 1 до n , линейно независимы, поскольку $c_1\mathbf{e}_1 + c_2\mathbf{e}_2 + \dots + c_n\mathbf{e}_n = (c_1, c_2, \dots, c_n)$. Докажем индукцией по n , что любые $n + 1$ векторов в \mathbb{R}^n линейно зависимы. База при $n = 1$ очевидна. Докажем переход от n к $n + 1$. Если у всех $n + 2$ векторов $(n + 1)$ -ая координата равна нулю, то, отбросив её, по предположению индукции можно найти нулевую линейную комбинацию этих $n + 2$ векторов с коэффициентами не всеми равными нулю, которая очевидно равна нулю и при возвращении отброшенной координаты. Если же у какого-то вектора \mathbf{x}_i $(n + 1)$ координата не равна нулю, то перейдём к векторам $\mathbf{x}'_1, \mathbf{x}'_2, \dots, \mathbf{x}'_n$, где $\mathbf{x}'_j = \mathbf{x}_j - (a_j/a_i)\mathbf{x}_i$, где a_k — $(n + 1)$ -ая координата вектора \mathbf{x}_k . Тогда по предположению индукции для векторов $\mathbf{x}'_1, \dots, \mathbf{x}'_{i-1}, \mathbf{x}'_{i+1}, \dots, \mathbf{x}'_{n+2}$ существуют коэффициенты c_1, \dots, c_{n+1} не все равные нулю такие, что $0 = c_1\mathbf{x}'_1 + \dots + c_{i-1}\mathbf{x}'_{i-1} + c_i\mathbf{x}'_{i+1} + \dots + c_{n+1}\mathbf{x}'_{n+2} = c_1(\mathbf{x}_1 - (a_1/a_i)\mathbf{x}_i) + \dots + c_{n+1}(\mathbf{x}_{n+2} - (a_{n+2}/a_i)\mathbf{x}_i) = c_1\mathbf{x}_1 + \dots + c_{i-1}\mathbf{x}_{i-1} + (-c_1(a_1/a_i) - c_2(a_2/a_i) - \dots - c_{i-1}(a_{i-1}/a_i) - c_i(a_{i+1}/a_i) - \dots - c_{n+1}(a_{n+2}/a_i)) + c_i\mathbf{x}_{i+1} + \dots + c_{n+1}\mathbf{x}_{n+2}$. То есть мы нашли равную нулю линейную комбинацию наших векторов в которой не все коэффициенты равны нулю. Противоречие.

Задача 24. Докажите, что если $\mathbf{x}_1, \dots, \mathbf{x}_n$ — любая максимальная система линейно независимых векторов в \mathbb{R}^n , то любой вектор $\mathbf{x} \in \mathbb{R}^n$ можно представить в виде $\mathbf{x} = c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n$, где c_1, \dots, c_n — действительные числа. (Система $\mathbf{x}_1, \dots, \mathbf{x}_n$ называется *базисом* пространства, а выражение $c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n$ — *линейной комбинацией* векторов $\mathbf{x}_1, \dots, \mathbf{x}_n$ с *коэффициентами* c_1, \dots, c_n . В этих терминах любой вектор $\mathbf{x} \in \mathbb{R}^n$ можно представить в виде линейной комбинации векторов базиса.)

Решение. Допустим обратное. Тогда существует вектор \mathbf{x} , не представимый в виде линейной комбинации векторов $\mathbf{x}_1, \dots, \mathbf{x}_n$. Но в этом случае система векторов $\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{x}$ будет линейно независимой и большей, чем исходная, что противоречит максимальной исходной системы векторов. Действительно, если $c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n + c\mathbf{x} = 0$, то либо $c = 0$ и тогда все c_i равны нулю в силу независимости системы векторов \mathbf{x}_i , либо $c \neq 0$, но тогда $\mathbf{x} = (c_1/c)\mathbf{x}_1 + \dots + (c_n/c)\mathbf{x}_n$, что противоречит предположению.

Пусть p — простое число, а \mathbb{Z}_p — множество вычетов по модулю p . Пространство \mathbb{Z}_p^n , подобно пространству \mathbb{R}^n , — это просто множество всех последовательностей чисел из \mathbb{Z}_p . Операции сложения

“векторов” $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^n$ и умножения их на элементы \mathbb{Z}_p осуществляются, как обычно, — по координатам, — но при этом каждая координата берется по модулю p .

Понятия линейной независимости, линейной комбинации и базиса для \mathbb{Z}_p^n определяются так же, как для \mathbb{R}^n . Только в них все числа c_i — это элементы \mathbb{Z}_p — не \mathbb{R} , — а равенство нулю понимается как равенство нулю по модулю p .

Задача 25. Докажите, что максимальное число линейно независимых векторов в \mathbb{Z}_p^n равно n и что любая максимальная система образует базис.

Решение. Доказательство абсолютно аналогично доказательству двух предыдущих задач. Заметим, что при их решении мы пользовались только тем, что любое действительное число можно поделить на любое другое отличное от нуля. Но это свойство верно и в \mathbb{Z}_p , если понимать под делением домножение на обратный элемент.

Задача 26. Пусть $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ — любое независимое множество вершин графа $G(n, 3, 1)$. Докажите, что векторы $\mathbf{x}_1, \dots, \mathbf{x}_t$ линейно независимы в \mathbb{Z}_2^n , откуда $\alpha(G(n, 3, 1)) \leq n$, и это лишь чуть-чуть слабее результата задачи 12!

Решение. Предположим противное. Тогда существуют коэффициенты c_1, \dots, c_t из \mathbb{Z}_2 такие, что $c_1\mathbf{x}_1 + \dots + c_t\mathbf{x}_t = 0$ и не все c_1, \dots, c_t равны 0. Без ограничения общности можно считать, что $c_1 \neq 0$. Домножим обе части равенства скалярно на \mathbf{x}_1 . Заметим, что скалярное произведение двух векторов, у которых все координаты кроме трёх равны нулю, а оставшиеся три равны 1, может быть равно 3, если эти вектора равны, и 0, 1 или 2 в остальных случаях. Так как наше множество независимо, то скалярное произведение не может быть равно 1. А следовательно, в левой части первое слагаемое будет равно 1 (можем так считать, поскольку $3 \equiv 1 \pmod{2}$), а остальные — 0, что противоречит тому, что в правой части очевидно получится 0.

Пусть $F \in \{\mathbb{R}, \mathbb{Z}_p\}$. Пусть x_1, \dots, x_n — “переменные”. *Одночленом* от этих n переменных называется выражение вида $x_1^{a_1} \cdot \dots \cdot x_n^{a_n}$, где a_1, \dots, a_n — некоторые неотрицательные целые числа. *Многочлен* — это любая линейная комбинация одночленов. При этом многочлен P принадлежит $F[x_1, \dots, x_n]$, если коэффициенты в нём — это элементы F . Складывают и умножают многочлены по обычным правилам. Также, если $P \in F[x_1, \dots, x_n]$, то его можно умножить на любой элемент F . В любом случае правила сложения и умножения коэффициентов многочленов определяются правилами сложения и умножения чисел в множестве F . *Степень* одночлена — это сумма степеней переменных, входящих в него. Степень многочлена — это максимум степеней его одночленов. Многочлен $P \in F[x_1, \dots, x_n]$ *равен нулю*, если все его коэффициенты равны нулю в F . Многочлены $P_1 \in F[x_1, \dots, x_n], \dots, P_t \in F[x_1, \dots, x_n]$ *линейно независимы* над F , если $c_1P_1 + \dots + c_tP_t = 0$ лишь в случае, когда все числа $c_1 \in F, \dots, c_t \in F$ равны нулю в F . Очевидно, что любой многочлен порождается *базисом*, состоящим из одночленов.

Задача 27. Докажите, что если многочлены линейно независимы над своим F , то их количество не превосходит числа одночленов в базисе, которым все эти многочлены порождаются.

Решение. Каждый многочлен представляется линейной комбинацией базисных одночленов. Следовательно, каждому многочлену можно сопоставить набор из n коэффициентов из F , где n — количество базисных одночленов. То есть, каждый многочлен можно рассматривать как вектор в

пространстве F^n . Тогда по задаче 24 максимальное количество линейно независимых векторов в этом пространстве равно n , что и составляет утверждение задачи.

Задача 28. Пусть $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ — любое независимое множество вершин графа $G(n, 5, 2)$. Пусть многочлены $P_1 \in \mathbb{Z}_3[y_1, \dots, y_n]$, $P_2 \in \mathbb{Z}_3[y_1, \dots, y_n]$, \dots , $P_t \in \mathbb{Z}_3[y_1, \dots, y_n]$ задаются формулами

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1), \quad i = 1, \dots, t.$$

Например, если $\mathbf{x}_1 = (1, 1, 1, 1, 1, 0, \dots, 0)$, $\mathbf{x}_2 = (0, \dots, 0, 1, 1, 1, 1, 1)$, то

$$P_1(y_1, \dots, y_n) = (y_1 + y_2 + y_3 + y_4 + y_5)(y_1 + y_2 + y_3 + y_4 + y_5 - 1) = y_1^2 + \dots + y_5^2 + 2y_1y_2 + \dots + 2y_4y_5 - y_1 - \dots - y_5,$$

$$\begin{aligned} P_2(y_1, \dots, y_n) &= (y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n)(y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n - 1) = \\ &= y_{n-4}^2 + \dots + y_n^2 + 2y_{n-4}y_{n-3} + \dots + 2y_{n-1}y_n - y_{n-4} - \dots - y_n. \end{aligned}$$

Докажите, что многочлены P_1, \dots, P_t линейно независимы над \mathbb{Z}_3 , а стало быть, $\alpha(G(n, 5, 2)) \leq C_n^2 + 2C_n^1$.

Решение. По аналогии с задачей 26 предположим противное и подставим в полученное равенство вместо \mathbf{y} один из \mathbf{x}_i , соответствующий P_i , перед которым в линейной комбинации стоит ненулевой коэффициент. Получим, что в правой части по-прежнему останется ноль, а в левой все многочлены, кроме P_i , обнулятся. Действительно, посмотрим чему может быть равно скалярное произведение $(\mathbf{x}_i, \mathbf{y})$. Оно может быть равно 0, 1, 3 или 4, и тогда многочлен по модулю 3 обнуляется. Двойке скалярное произведение быть равно не может, так как множество взятых вершин независимо. А 5 оно может быть равно только в случае совпадения векторов, что и даёт единственное ненулевое слагаемое.

Очевидно, что множество рассмотренных многочленов порождается базисом из одночленов вида попарных произведений $y_i y_j$, квадратов y_i^2 и одночленов y_i , которых как раз $C_n^2 + 2C_n^1$, что даёт нам необходимое ограничение на размер независимого множества.

Задача 29. Пусть в условиях предыдущей задачи многочлены P_i заменены многочленами P'_i по следующему правилу: каждый одночлен вида y_i^2 преобразован к виду y_i , после чего приведены подобные слагаемые. Докажите, что многочлены P'_1, \dots, P'_t , отвечающие векторам из независимого множества вершин W графа $G(n, 5, 2)$, так же линейно независимы над \mathbb{Z}_3 , как и исходные многочлены P_1, \dots, P_t . Выведите из этого факта оценку $\alpha(G(n, 5, 2)) \leq C_n^2$ и сравните её с оценкой из задачи 15.

Решение. В решении предыдущей задачи для доказательства линейной независимости мы пользовались только значениями многочленов в точках, где каждая переменная была равна либо 0, либо 1. Очевидно, что значения новых многочленов в этих точках будут совпадать со значениями многочленов, используемых в предыдущей задаче, а следовательно, работает то же доказательство.

Осталось заметить, что после раскрытия скобок и соответствующей замены в каждом многочлене останутся только попарные произведения переменных, а следовательно, базис, состоящий из образующих одночленов этих многочленов, содержит не более, чем C_n^2 мономов, что и даёт нам необходимую оценку.

Сравнивая с оценкой, полученной в задаче 15, получаем, что $\alpha(G(n, 5, 2)) \sim \frac{1}{2}n^2$.

Задача 30. Выведите из результата предыдущей задачи нижнюю оценку для $\chi(\mathbb{R}^n)$, которая значительно уточняет оценку из задачи 12. Убедитесь в том, однако, что ввиду задачи 19 существенных дальнейших продвижений за счет графа $G(n, 5, 2)$ мы не получим.

Решение. По задаче 11 для сгомтетированного с коэффициентом $1/\sqrt{6}$ графа $G(n, 5, 2)$ получим, что $\chi(\mathbb{R}^n) \geq \frac{|V|}{\alpha(G(n,5,2))} \geq C_n^5/C_n^2 = \frac{1}{60}n^3 + O(n^2)$. С другой стороны, из этого графа мы не сможем получить оценку на хроматическое число лучше, чем C_n^3 , что по порядку величины совпадает с найденной оценкой.

Задача 31. Пусть $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ — любое независимое множество вершин графа $G(n, 9, 4)$. Пусть многочлены $P_1 \in \mathbb{Z}_5[y_1, \dots, y_n]$, $P_2 \in \mathbb{Z}_5[y_1, \dots, y_n]$, \dots , $P_t \in \mathbb{Z}_5[y_1, \dots, y_n]$ задаются формулами

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1)((\mathbf{x}_i, \mathbf{y}) - 2)((\mathbf{x}_i, \mathbf{y}) - 3), \quad i = 1, \dots, t.$$

Докажите, что многочлены P_1, \dots, P_t линейно независимы над \mathbb{Z}_5 .

Решение. По аналогии с задачей 28, будем действовать от противного: рассмотрим нулевую линейную комбинацию с каким-то коэффициентом, отличным от нуля. Подставив в неё вектор, соответствующий ненулевому слагаемому линейной комбинации, мы получим слева одно ненулевое слагаемое, соответствующее этому многочлену, а справа — тождественный ноль, чего быть не может.

Задача 32. Какая верхняя оценка для $\alpha(G(n, 9, 4))$ вытекает из предыдущей задачи?

Решение. Для получения оценки нужно посчитать количество одночленов, которыми порождаются все вектора P_1, P_2, \dots, P_t . Но для этого достаточно взять одночлены вида

$$y_i y_j y_k y_l, y_i^2 y_j y_k, y_i y_j y_k, y_i^3 y_j, y_i^2 y_j^2, y_i^2 y_j, y_i y_j, y_i^4, y_i^3, y_i^2, y_i, \text{const.}$$

Таким образом видно, что количество таких одночленов равно $C_n^4 + 4C_n^3 + 6C_n^2 + 4C_n^1 + 1$, а, значит, этой величиной и оценивается $\alpha(G(n, 9, 4))$.

Задача 33. Пусть в условиях задачи 31 многочлены P_i заменены многочленами P'_i по следующему правилу: каждый одночлен в них, получающийся после раскрытия скобок и приведения подобных слагаемых, конечно, имеет вид $y_1^{a_1} \cdot \dots \cdot y_n^{a_n}$; если среди чисел a_i есть большие либо равные двойке, то заменяем все их единицами, после чего приводим подобные слагаемые. Например, одночлен $y_1^2 y_2^2$ превратится в $y_1 y_2$, и то же самое будет с одночленами $y_1^2 y_2, y_1 y_2$, и т.д. Докажите, что многочлены P'_1, \dots, P'_t , отвечающие векторам из независимого множества вершин W графа $G(n, 9, 4)$, так же линейно независимы над \mathbb{Z}_5 , как и исходные многочлены P_1, \dots, P_t . Выведите из этого факта оценку $\alpha(G(n, 9, 4)) \leq C_n^4 + C_n^3 + C_n^2 + C_n^1 + C_n^0$ и сравните её с оценкой из задачи 15.

Решение. В задаче 31 для доказательства линейной независимости многочленов мы пользовались только подстановкой в некоторое равенство значений y_i , равных 0 или 1. В обоих случаях при совершении описанной в условии задачи операции значение многочлена не изменится. Следовательно, доказательство останется верным, и мы получим оценку числа таких многочленов через количество образующих одночленов, которое как раз и равно $C_n^4 + C_n^3 + C_n^2 + C_n^1 + C_n^0$. В задаче 15 мы получили асимптотически такую же оценку снизу.

Задача 34. Выведите из результата предыдущей задачи нижнюю оценку для $\chi(\mathbb{R}^n)$, которая значительно уточняет оценку из задачи 30. Убедитесь в том, однако, что ввиду задачи 19 существенных дальнейших продвижений за счет графа $G(n, 9, 4)$ мы не получим.

Решение. По аналогии с задачей 30 получаем оценку $\chi(\mathbb{R}^n) \geq C_n^9/C_n^4 = \frac{4!}{9!}n^5 + O(n^4)$. С другой стороны, по утверждению из задачи 19 мы не сможем получить за счет этого графа оценку лучше, чем C_n^5 , что даёт ту же асимптотическую точность.

Задача 35. Пусть r и s таковы, что $r - s = p$, где p — простое число, причём $r - 2p < 0$. Докажите, что тогда $\alpha(G(n, r, s)) \leq \sum_{k=0}^{p-1} C_n^k$. Сравните эту оценку с оценкой из задачи 15.

Решение. Для любого независимого множества $W = \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ достаточно рассмотреть многочлены $P_i \in \mathbb{Z}_p[y_1, \dots, y_n]$, заданные формулами

$$P_i(\mathbf{y}) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1) \dots ((\mathbf{x}_i, \mathbf{y}) - (p - 1)).$$

Проведя для них аналогичные приведённым выше рассуждения, получим необходимую оценку. Оценка из задачи 15 даёт нам ту же асимптотику только с другой стороны, что позволяет сделать оценку $\alpha(G(n, r, s)) \sim \frac{1}{(p-1)!}n^{p-1}$.

Задача 36*. Исследуйте нижние оценки величины $\chi(\mathbb{R}^n)$, которые вытекают из результатов предыдущей задачи. Как эти оценки соотносятся с оценками из задачи 19?

Решение. С учетом обозначений предыдущей задачи имеем

$$\chi(\mathbb{R}^n) \geq \chi(G(n, r, s)) \geq \frac{|V(n, r)|}{\alpha(G(n, r, s))} \geq \frac{C_n^r}{\sum_{k=0}^{p-1} C_n^k} = (1 + o(1)) \left(\frac{C_n^r}{C_n^{r-s-1}} \right),$$

то есть существует некая константа c_1 , что $\chi(G(n, r, s)) \geq c_1 n^{s+1}$, но с другой стороны из задачи 19 мы знаем, что $\chi(G(n, r, s)) \leq c_2 n^{s+1}$ для некой константы c_2 . То есть для графов $G(n, r, s)$, у которых $r - s = p$, где p — простое число, причём $r - 2p < 0$, нам удаётся установить порядок хроматического числа.

3 Задачи после промежуточного финиша

До промежуточного финиша мы убедились в том, насколько важны числа независимости графов для получения нижних оценок хроматического числа пространства. При этом мы рассматривали разные последовательности дистанционных графов — последовательности $\{G(n, r, s)\}_{n=1}^{\infty}$ с заданными наперед r и s . Интересно понять: а как изменятся числа независимости, если, вместо графов $G(n, r, s)$, брать их “остовные” подграфы, т.е. вершины сохранять, а ребра частично удалять. Кажется очевидным, что числа независимости должны сильно вырасти, коль скоро мы удалим много ребер. Однако, удивительным образом, иногда это так, а иногда и совершенно иначе! Для того, чтобы получить соответствующие результаты, займемся немного случайными графами и теорией вероятностей.

3.1 Случайный граф Эрдеша–Реньи и некоторые его вероятностные характеристики

Пусть $V_n = \{1, \dots, n\}$ — множество вершин. Теоретически на нем можно построить C_n^2 ребер, если запретить кратные ребра, петли и ориентацию. Давайте каждое из этих C_n^2 потенциальных рёбер проводить с вероятностью $p \in [0, 1]$, общей для всех ребер. При этом появляться или не появляться ребра будут независимо друг от друга. Пусть $G = (V_n, E)$ — какой-то граф, который может случайно возникнуть в результате описанной только что вероятностной процедуры. Обозначим вероятность его возникновения $\mathbb{P}(G)$. Понятно, что она равна $p^{|E|}(1-p)^{C_n^2-|E|}$. Если A — какое-то свойство графа, то его вероятность — $\mathbb{P}(A)$ — это сумма по всем графам G , обладающим свойством A , вероятностей этих графов.

Обозначим Ω_n множество всех графов на вершинах V_n . Любая функция X , определенная на Ω_n и принимающая действительные значения, называется *случайной величиной*. Например, число треугольников в графе или число его связных компонент, или его число независимости — это случайные величины. При этом надо четко понимать, что величины случайны лишь потому, что априори мы не знаем, какой граф появится на свет. Когда граф уже возник, значение X определено однозначно!

У случайных величин есть “средние значения” — так называемые *математические ожидания*. Математическое ожидание величины X — это число $\mathbb{M}X$, определяемое по формуле

$$\mathbb{M}X = \sum_{G \in \Omega_n} X(G)\mathbb{P}(G).$$

Мы просто складываем значения функции X на графах, помноженные на вероятности этих графов. Естественно, это некое взвешенное среднее (веса — вероятности) — своего рода центр масс. Давайте научимся считать математические ожидания и применять полученные результаты для изучения свойств случайных графов.

Задача 37. Докажите, что если случайная величина — это константа c , то $\mathbb{M}c = c$.

Решение. Что такое среднее значение константы? Это, очевидно, и есть сама эта константа.

Задача 38. Пусть X_1, X_2 — случайные величины, а c_1, c_2 — фиксированные числа. Разумеется, $c_1X_1 + c_2X_2$ — это тоже случайная величина. Докажите, что её математическое ожидание равно $c_1\mathbb{M}X_1 + c_2\mathbb{M}X_2$. Это свойство называется *линейностью* математического ожидания.

Решение.

$$\begin{aligned} \mathbb{M}(c_1X_1 + c_2X_2) &= \sum_G (c_1X_1(G) + c_2X_2(G))\mathbb{P}(G) = c_1 \sum_G X_1(G)\mathbb{P}(G) + c_2 \sum_G X_2(G)\mathbb{P}(G) = \\ &= c_1\mathbb{M}X_1 + c_2\mathbb{M}X_2. \end{aligned}$$

Задача 39. С помощью линейности математического ожидания найдите математические ожидания а) числа треугольников в случайном графе;

Решение. Понятно, что всего наборов из трех вершин C_n^3 , и каждый из них будет треугольником с вероятностью p^3 . И из линейности следует, что $\mathbb{M}X = C_n^3 p^3$, где X — искомая случайная величина.

б) числа связных компонент случайного графа, каждая из которых является циклом на k вершинах (k — фиксированное заданное наперёд число);

Решение. Понятно, что всего наборов из k вершин в графе C_n^k , и каждый из них может образовать $\frac{(k-1)!}{2}$ циклов (в зависимости от порядка вершин внутри цикла). Ну а вероятность, с которой упорядоченный набор из k вершин станет циклом, равна $p^k(1-p)^{C_k^2-k+k(n-k)}$, поскольку рёбер внутри этого набора должно быть ровно k и рёбер из этих вершин в остальные идти не должно. И из линейности следует, что $\mathbb{M}X = C_n^k \frac{(k-1)!}{2} p^k (1-p)^{C_k^2-k+k(n-k)}$, где X — искомая случайная величина.

в) числа независимых множеств вершин в случайном графе, каждое из которых имеет мощность k (k — фиксированное заданное наперед число).

Решение. Всего наборов из k вершин C_n^k и каждый из них станет независимым с вероятностью $(1-p)^{C_k^2}$. Поэтому $\mathbb{M}X = C_n^k (1-p)^{C_k^2}$, где X — искомая случайная величина.

Задача 40. Докажите *неравенство Маркова*: если X — случайная величина, принимающая неотрицательные значения, и дано положительное число a , то $\mathbb{P}(X \geq a) \leq \frac{\mathbb{M}X}{a}$.

Решение.

$$\mathbb{M}X = \sum_z z \mathbb{P}(X = z) = \sum_{z \geq a} z \mathbb{P}(X = z) + \sum_{z < a} z \mathbb{P}(X = z) \geq \sum_{z \geq a} a \mathbb{P}(X = z) = a \mathbb{P}(X \geq a).$$

Это эквивалентно неравенству Маркова.

Задача 41. Докажите с помощью неравенства Маркова, что если $p = \frac{1}{2}$, то $\mathbb{P}(\alpha(G) \leq 2 \log_2 n) \rightarrow 1$ при $n \rightarrow \infty$ (говорят “почти наверное $\alpha(G) \leq 2 \log_2 n$ ”).

Решение. Введем случайную величину X_k , равную количеству независимых множеств вершин размера k . Тогда из 39 и 40 задач видно, что

$$\mathbb{P}(X_k \geq 1) \leq \mathbb{M}X_k = C_n^k \left(\frac{1}{2}\right)^{\frac{k(k-1)}{2}} \leq \frac{n^k}{k!} \left(\frac{1}{2}\right)^{\frac{k(k-1)}{2}} \leq \frac{n^k e^k}{k^k} \left(\frac{1}{2}\right)^{\frac{k(k-1)}{2}} = \left(\frac{ne2^{\frac{k-1}{2}}}{k}\right)^k.$$

Несложно видеть, что при $k = 2 \log_2 n$ эта величина стремится к 0. Значит с вероятностью, стремящейся к 1, независимого множества вершин размера k в графе не существует.

Заметим, что на самом деле при $p = \frac{1}{2}$ почти наверное $\alpha(G) \geq (2 - \varepsilon) \log_2 n$ при сколь угодно малом наперед заданном $\varepsilon > 0$. Точнее, — и это нам понадобится позже, — справедлива

Теорема 1. Для любого $\varepsilon > 0$ при больших n выполнено неравенство

$$\mathbb{P}(\alpha(G) \geq (2 - \varepsilon) \log_2 n) > 1 - 2^{-n}.$$

Таким образом, при $p = \frac{1}{2}$ почти наверное число независимости — это примерно $2 \log_2 n$. Иными словами, что происходит? Мы берем полный граф на n вершинах и часть его рёбер удаляем с вероятностью $\frac{1}{2}$. У типичного графа, который остается в результате этой процедуры, примерно

$\frac{C_n^2}{2}$ рёбер — вдвое меньше, чем у полного графа. И у типичного же графа число независимости в логарифм раз больше числа независимости исходного полного графа (у него-то оно равно 1). Что ж, рёбер вдвое меньше, и число независимости выросло: вполне естественно! Оказывается, что для некоторых $G(n, r, s)$ при случайном удалении рёбер имеет место точно такой же “ожидаемый” результат (число независимости возрастает в примерно логарифм от числа вершин раз). Но чудо в том, что так получается не всегда! Для многих $G(n, r, s)$ число независимости вовсе не изменяется! Ниже мы вместе изучим примеры обеих ситуаций.

3.2 Случайные подграфы графа $G(n, 3, 0)$

Пусть $G_{1/2}(n, 3, 0)$ — случайный подграф графа $G(n, 3, 0)$, полученный взаимно независимым удалением рёбер из графа $G(n, 3, 0)$, каждого — с вероятностью $1/2$.

Задача 42. Если у Вас получилась задача 16, то вспомните просто, что $\alpha(G(n, 3, 0)) = C_{n-1}^2$. Иначе попробуйте решить этот частный случай той задачи.

Решение. Смотрите решение задачи 16.

В серии следующих ниже задач мы докажем, что почти наверное $\alpha(G_{1/2}(n, 3, 0)) \leq C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. Это и есть то самое удивительное явление: никакого роста в логарифм раз нет; если и есть рост, то лишь в такое количество раз, которое само стремится к 1 при $n \rightarrow \infty$! Можно доказать и гораздо более сильные факты, но это уже совсем трудно, а нам бы суть почувствовать!

В дальнейшем мы будем для краткости опускать целые части у величин, которые должны быть целыми. Например, запись $C_{\log_2 n}^k$ означает, смотря по контексту, что на самом деле речь идет о верхней или нижней целой части числа $\log_2 n$. Ни одна из выкладок от такого огрубления не пострадает.

Задача 43. Положим $k = C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. Считаем, что k целое (ср. замечание перед задачей). Пусть $A \subset V(n, 3)$ — произвольное множество вершин графа $G(n, 3, 0)$, имеющее мощность k . Обозначим через $r(A)$ количество рёбер графа $G(n, 3, 0)$, оба конца которых попадают в A . Поскольку $|A| = k > \alpha(G(n, 3, 0))$, ясно, что $r(A) > 0$. Пусть X_k — случайная величина, равная числу независимых множеств размера k в графе $G_{1/2}(n, 3, 0)$. Докажите, что

$$\mathbb{M}X_k = \sum_{A \subset V(n, 3): |A|=k} \left(\frac{1}{2}\right)^{r(A)}. \quad (2)$$

Решение. Пусть $t = C_{|V|}^k$. Давайте каждому подграфу на k вершинах поставим в соответствие случайную величину, равную 1, если соответствующий подграф на k вершинах стал независимым, и 0 в противном случае. Обозначим эти случайные величины Y_1, Y_2, \dots, Y_t . Тогда $X_k = Y_1 + Y_2 + \dots + Y_t$. Но математическое ожидание величины Y_i , очевидно, равно $\frac{1}{2}^{|Y_i|}$, где $|Y_i|$ — количество рёбер в соответствующем i -ой случайной величине подграфе. И теперь из линейности математического ожидания сразу следует, что

$$\mathbb{M}X_k = \sum_{A \subset V(n, 3): |A|=k} \left(\frac{1}{2}\right)^{r(A)}.$$

Задача 44. Докажите, что наша цель будет достигнута, едва мы докажем, что $\mathbb{M}X_k \rightarrow 0$ при $n \rightarrow \infty$.

Решение. Нам хочется доказать, что с большой вероятностью нет независимых множеств размера k , то есть $P(X_k = 0) \rightarrow 1$ при $n \rightarrow \infty$. Но понятно, что $P(X_k = 0) + P(X_k \geq 1) = 1$. Тогда нам нужно доказать, что $P(X_k \geq 1) \rightarrow 0$. Но из неравенства Маркова $P(X_k \geq 1) \leq \mathbb{M}X_k$. И осталось показать, что $\mathbb{M}X_k \rightarrow 0$ при $n \rightarrow \infty$.

Ясно, что надо научиться оценивать *снизу* величины $r(A)$. Для каждого A обозначим $B = B(A)$ любое (раз и навсегда избранное) подмножество множества A , которое является независимым в $G(n, 3, 0)$ и имеет максимальную мощность среди всех подобных подмножеств множества A .

Задача 45. Пусть $A \subset V(n, 3)$, $|A| = k$. Пусть $B = B(A)$. Заметим, что $k \approx \frac{n^2}{2}$. Предположим, что $|B|$ значительно меньше k : например, пусть $|B| < n^{1.9}$ (здесь странное число 1.9 взято почти с потолка, лишь бы строго меньше, чем 2). Докажите, что тогда при больших n заведомо выполнено неравенство $r(A) \geq \frac{k^2}{3|B|}$ (при правильном подходе тройку в знаменателе можно “почти” заменить на двойку, но да Бог с ним).

Решение.

Для данной задачи докажем вспомогательную Лемму.

Лемма. В любом подграфе $\tilde{\mathcal{G}}$ графа \mathcal{G} , содержащем mn вершин, и у которого $\alpha(G) \leq n$, содержится не менее $\frac{m^2n}{2} - \frac{mn}{2}$ рёбер ($m \in \mathbb{N}$).

Доказательство.

Давайте докажем это индукцией по m .

База. $m = 1$.

$\frac{m^2n}{2} - \frac{mn}{2} = 0$ и утверждение очевидно.

Переход. $m \rightarrow m + 1$.

Рассмотрим максимальное независимое множество в подграфе $\tilde{\mathcal{G}}$. Если их несколько, то возьмём любое из них. Очевидно, что число независимости подграфа не превосходит числа независимости исходного графа. Поэтому $\alpha(\tilde{\mathcal{G}}) \leq n$. Пусть максимальное независимое множество имеет размер k , $k \leq n$. Значит, из оставшихся $(m + 1)n - k$ вершин в это множество идёт хотя бы по 1 ребру, иначе мы могли бы увеличить независимое множество, а по предположению оно максимально. Тогда у нас есть минимум $(m + 1)n - k$ ребер. Ни одно из этих рёбер не лежит внутри подграфа на оставшихся $(m + 1)n - k$ вершинах. И $(m + 1)n - k \geq mn$, а значит, внутри подграфа на оставшихся $(m + 1)n - k$ вершинах по предположению индукции содержится не менее $\frac{m^2n}{2} - \frac{mn}{2}$ ребер. Тогда, всего рёбер не меньше, чем $\frac{m^2n}{2} - \frac{mn}{2} + (m + 1)n - k \geq \frac{m^2n}{2} - \frac{mn}{2} + mn = \frac{m^2n + 2mn + n}{2} - \frac{n}{2} - \frac{mn}{2} = \frac{(m+1)^2n}{2} - \frac{(m+1)n}{2}$. Переход доказан.

Тогда из леммы следует, что

$$r(A) \geq \frac{\left\lfloor \frac{|A|}{|B|} \right\rfloor^2 |B|}{2} - \frac{\left\lfloor \frac{|A|}{|B|} \right\rfloor |B|}{2} = \frac{\left\lfloor \frac{|A|}{|B|} \right\rfloor |B|}{2} \left(\left\lfloor \frac{|A|}{|B|} \right\rfloor - 1 \right) \geq \frac{k - |B|}{2} \left(\frac{k}{|B|} - 2 \right) = (1 + o(1)) \frac{k^2}{2|B|}.$$

Задача 46. Пусть $A \subset V(n, 3)$, $|A| = k$. Пусть $B = B(A)$. Пусть $|B| > 9n$, а еще лучше (в дополнение к предыдущей задаче), $|B| \geq n^{1.9}$. Докажите, что $r(A) \geq (|B| - 9n)(|A| - |B|)$.

Решение. Оценим число рёбер графа $G(n, 3, 0)$ в A . Поскольку B — *максимальное* независимое множество вершин графа $G(n, 3, 0)$, содержащееся в A , для любой вершины $\mathbf{x} \in A \setminus B$ есть такая вершина $\mathbf{y} \in B$, что $\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0)$. Покажем, что вершина \mathbf{y} далеко не единственная с этим свойством. Действительно, вершины \mathbf{x} и \mathbf{y} соединены ребром, а значит, как 3-элементные множества они не пересекаются. Оценим, сколько может быть вершин $\mathbf{z} \in B$, которые **не соединены** с \mathbf{x} . С одной стороны, они должны пересекаться с \mathbf{x} хотя бы по одному элементу. С другой стороны, так как B — независимое множество, они должны и с \mathbf{y} иметь непустое пересечение. Но \mathbf{x} и \mathbf{y} не пересекаются. Стало быть, таких вершин \mathbf{z} точно не больше, чем $9n$. В текущей ситуации $|B| > n^{1.9}$. Следовательно, количество вершин из B , с которыми соединена данная вершина $\mathbf{x} \in A \setminus B$, не меньше, чем $|B| - 9n$. Таким образом,

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0) : \mathbf{x}, \mathbf{y} \in A\}| \geq (|A| - |B|)(|B| - 9n) \geq \frac{C_{n-1}^2}{\ln n} n^{1.9} = (1 + o(1)) \frac{n^{3.9}}{2 \ln n},$$

(последние переходы возможны при условии, что $|B| \geq n^{1.9}$. А вот для неравенства $r(A) \geq (|B| - 9n)(|A| - |B|)$ нам достаточно $|B| > 9n$).

Задача 47. Разбейте сумму (2) на две части: в первой части будут лишь те A , для которых $|B| < n^{1.9}$; во второй — все остальные. К слагаемым в обеих частях примените оценки из соответствующих задач и убедитесь, что вся сумма (2) таки стремится к нулю, и все получилось! На что в выкладках можно было заменить порог $n^{1.9}$?

Решение. Достаточно проверить, что с вероятностью, стремящейся к нулю, в случайном графе $\mathcal{G}(G(n, 3, 0), 1/2)$ есть независимое множество вершин размера k . Эта вероятность заведомо не больше величины

$$\sum_{A \subset V(n, r), |A|=k} \mathbb{P}(A \text{ независимо в } \mathcal{G}(G(n, 3, 0), 1/2)) = \sum_{A \subset V(n, r), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0) : \mathbf{x}, \mathbf{y} \in A\}|}.$$

Покажем, что и последняя сумма стремится к нулю.

Возможны два варианта: либо для данного A выполнено $|B| \leq n^{1.9} = o(C_{n-1}^2)$ (множество A — *первого типа*), либо для данного A выполнено $|B| > n^{1.9}$ (множество A — *второго типа*).

В интересующей нас сумме выделим слагаемые, для которых A первого типа. Их сумма не превосходит величины

$$C_n^k 2^{-(1+o(1)) \frac{k^2}{2n^{1.9}}} < 3^k n^{3k} 2^{-(1+o(1)) \frac{k^2}{2n^{1.9}}} = 3^k 2^{(1+o(1)) 3 \frac{n^2}{2} \log_2 n} 2^{-(1+o(1)) \frac{n^4}{2(2)^2 n^{1.9}}} \rightarrow 0.$$

Здесь мы пользуемся тем, что

$$n^2 \log_2 n = o(n^{2.1}).$$

Пусть теперь A второго типа. По задаче 45

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0) : \mathbf{x}, \mathbf{y} \in A\}| \geq \frac{n^{3.9}}{2 \ln n},$$

т.е. сумма тех слагаемых, которые в интересующей нас сумме отвечают множествам A второго типа, не превосходит величины

$$C_n^k 2^{-(1+o(1)) \frac{n^{3.9}}{2 \ln n}} < 3^k n^{3k} 2^{-(1+o(1)) \frac{n^{3.9}}{2 \ln n}} = 3^k 2^{(1+o(1)) 3 \frac{n^2}{2} \log_2 n} 2^{-(1+o(1)) \frac{n^{3.9}}{2 \ln n}} \rightarrow 0.$$

И задача доказана.

3.3 Случайные подграфы графа $G(n, 3, 1)$

Пусть $G_{1/2}(n, 3, 1)$ — случайный подграф графа $G(n, 3, 1)$, полученный взаимно независимым удалением рёбер из графа $G(n, 3, 1)$, каждого — с вероятностью $1/2$. Казалось бы, все то же, что и с графами $G(n, 3, 0)$. Ан нет!

Вспомним, что $\alpha(G(n, 3, 1)) \approx n$ (см. задачу 12).

Задача 48*. Напишите аналог равенства (2) и докажите аналог оценки из задачи 45. Убедитесь в итоге, что существует $c > 0$, с которым почти наверное $\alpha(G_{1/2}(n, 3, 1)) \leq cn \log_2 n$.

Решение. Мы подробно вывели оценку в задаче 45, поэтому не будем делать этого повторно, а лишь скажем, что ввиду $\alpha(G(n, 3, 1)) \leq n$ мы знаем, что количество рёбер во множестве A размера k не меньше, чем $(1 + o(1))\frac{k^2}{2n}$. Пытливый читатель может убедиться в этом самостоятельно, повторив рассуждения из задачи 45.

Пусть $X_k = X_k(\mathcal{G}(G(n, 3, 1), 1/2))$ — это функция от случайного графа, равная количеству k -вершинных независимых множеств в нём (т.е. множеств, элементы которых попарно не соединены рёбрами). Оценим её математическое ожидание и применим неравенство Маркова:

$$\begin{aligned} \mathbb{M}X_k &= \sum_{A \subset V(n,3), |A|=k} \mathbb{P}(A \text{ является независимым множеством в } \mathcal{G}(G(n, 3, 1), 1/2)) = \\ &= \sum_{A \subset V(n,3), |A|=k} 2^{-|\{\mathbf{x}, \mathbf{y}\} \in E(n,3,1) : \mathbf{x}, \mathbf{y} \in A\}|}, \end{aligned}$$

т.е. в показателе экспоненты стоит число рёбер подграфа графа $G(n, 3, 1)$, порождённого конкретным множеством вершин A . Как мы уже упомянули,

$$|\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 1) : \mathbf{x}, \mathbf{y} \in A\}| > (1 + o(1)) \frac{k^2}{2\alpha(G(n, 3, 1))} = (1 + o(1)) \frac{k^2}{2n}.$$

Имея на руках такую оценку, получаем, что

$$\mathbb{M}X_k < \sum_{A \subset V(n,3), |A|=k} 2^{-(1+o(1))\frac{k^2}{2n}} = C_{C_3}^k 2^{-(1+o(1))\frac{k^2}{2n}}.$$

Хорошо известно, что $C_a^b \leq \left(\frac{ea}{b}\right)^b$, где e — основание натурального логарифма. Следовательно,

$$\mathbb{M}X_k < \left(\frac{n^3}{k}\right)^k 2^{-(1+o(1))\frac{k^2}{2n}} = 2^{3k \log_2 n - k \log_2 k - (1+o(1))\frac{k^2}{2n}}.$$

Видно, что существует функция $k = k(n)$, которая асимптотически ведет себя как $4n \log_2 n$ и с которой $\mathbb{E}X_k \rightarrow 0$ при $n \rightarrow \infty$. Отсюда с учетом неравенства Маркова вытекает утверждение теоремы:

$$\mathbb{P}(\alpha(\mathcal{G}(G(n, 3, 1), 1/2)) \leq 4(1 + o(1))n \log_2 n) = \mathbb{P}(X_k = 0) \geq 1 - \mathbb{E}X_k \rightarrow 1, \quad n \rightarrow \infty.$$

Это нам и требовалось доказать.

Задача 49. Докажите, что в графе $G(n, 3, 1)$ есть примерно $\frac{n}{2}$ полных подграфов, в каждом из которых примерно $\frac{n}{4}$ вершин и каждые два из которых не соединены рёбрами.

Решение. Для удобства сразу будем считать, что n делится на 4. Положим $m = \frac{n}{2}$. Разобьём \mathcal{R}_n на части $R_1 = \mathcal{R}_m$ и $R_2 = \mathcal{R}_n \setminus R_1$. Сперва опишем построение одной клики Q_1 . Для этого возьмем в R_1 непересекающиеся пары $\{1, 2\}, \{3, 4\}, \{5, 6\}, \dots, \{m-1, m\}$ (благо m четное). К каждой из этих пар добавим элемент $m+1 \in R_2$. Это и есть искомая клика. Число вершин в ней $\frac{m}{2} = \frac{n}{4}$. Аналогично построим еще $n-m-1$ клику Q_2, \dots, Q_{n-m} , добавляя к каждой из наших пар в R_1 элемент $m+2 \in R_2$, элемент $m+3 \in R_2$ и так далее. Очевидно, что для любых $i, j, i \neq j$, и для любых \mathbf{x} из Q_i , \mathbf{y} из Q_j ребра между \mathbf{x}, \mathbf{y} нет: эти тройки могут либо вовсе не пересекаться, либо пересекаться сразу по какой-то паре из R_1 .

Нам удалось построить $\frac{n}{2}$ клик размера $\frac{n}{4}$ каждая.

Задача 50. С помощью предыдущей задачи и теоремы 1 докажите, что для любого $\varepsilon > 0$ почти наверное $\alpha(G_{1/2}(n, 3, 1)) \geq (1 - \varepsilon)n \log_2 n$.

Решение. Как мы знаем, случайный граф $\mathcal{G}(G(n, 3, 1), 1/2)$ получается из графа $G(n, 3, 1)$ в результате взаимно независимого выбора рёбер из $E(n, 3, 1)$ с одной и той же вероятностью $\frac{1}{2}$. Поэтому на кликах Q_1, \dots, Q_{n-m} возникают независимые копии случайного графа Эрдеша–Реньи $G(m/2, 1/2)$. Отметим, что эти копии независимы и с точки зрения теории вероятностей (как случайные элементы), и с точки зрения теории графов (между ними нет ребер).

При $p = \frac{1}{2}$ теорема 1 говорит, что с асимптотической вероятностью 1 выполнено $\alpha(G(m/2, 1/2)) \sim 2 \log_2 m$ при $m \rightarrow \infty$, но m лишь в константу раз меньше n , откуда $\alpha(G(m/2, 1/2)) \sim 2 \log_2 n$ при $n \rightarrow \infty$. Более того, скорость стремления вероятности к единице очень высока. Заведомо при правильно подобранной бесконечно малой и больших n верна оценка

$$\mathbb{P}(\alpha(G(m/2, 1/2)) \geq 2(1 + o(1)) \log_2 n) \geq 1 - 2^{-n}.$$

А это значит, что

$$\mathbb{P}(\forall i = 1, \dots, n-m \quad \alpha(\mathcal{G}(Q_i, 1/2)) \geq 2(1 + o(1)) \log_2 n) \geq (1 - 2^{-n})^{n-m} \rightarrow 1, \quad n \rightarrow \infty.$$

Следовательно, с асимптотической вероятностью 1 в случайном графе $\mathcal{G}(G(n, 3, 1), 1/2)$ есть $n - m$ независимых множеств размера $2(1 + o(1)) \log_2 n$, между которыми точно нет ребер. Вместе они составляют, тем самым, одно независимое множество размера $2(n - m)(1 + o(1)) \log_2 n \sim n \log_2 n$, что и требовалось доказать.

Таким образом, для $G_{1/2}(n, 3, 1)$, как и для случайного графа Эрдеша–Реньи, имеем снова увеличение числа независимости в примерно логарифм от числа вершин раз. Такие вот удивительные эффекты!

Задача 51*. Попробуйте улучшить в константу раз результат задачи 50.

Решение. Для улучшения оценки достаточно полностью повторить рассуждения задач 49 и 50, лишь подставив вместо $m = \frac{n}{2}$ значение $m = 2 \left\lfloor \frac{n}{2 \log_2 n} \right\rfloor$, где $[x]$ — это обычная целая часть числа x . Тогда мы получим оценку ровно в два раза лучше, чем в задаче 50.

3.4 Случайные подграфы графа $G(n, 2, 1)$

Задача 52. Найдите $\alpha(G(n, 2, 1))$.

Решение. Очевидно, что это просто покрытие множества непересекающимися парами. А тогда $\alpha(G(n, 2, 1)) = \frac{n}{2}$, если n четно, и $\alpha(G(n, 2, 1)) = \frac{n-1}{2}$, если n нечетно.

Задача 53. Пусть $r(A)$ имеет тот же смысл, что и аналогичная величина в формуле (2). Докажите, что всегда $r(A) \geq \frac{2|A|^2}{n} - |A|$.

Решение. Множество A — это подмножество множества \mathcal{R}_n . Для каждого элемента $i \in \mathcal{R}_n$ определим k_i как число вершин графа $G(n, 2, 1)$ — “двоек”, — принадлежащих A и содержащих i . Понятно, что при фиксированном i любые две отвечающих ему двойки образуют ребро в $G(n, 2, 1)$. Поэтому

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}| \geq \sum_{i=1}^n C_{k_i}^2.$$

В то же время $k_1 + \dots + k_n = 2|A|$. Нетрудно показать, что минимум выражения $\sum_{i=1}^n C_{k_i}^2$ в этих ограничениях достигается при $k_i = \frac{2|A|}{n}$, $i = 1, \dots, n$, откуда и следует оценка

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}| \geq \sum_{i=1}^n C_{k_i}^2 \geq \frac{2|A|^2}{n} - |A|.$$

Задача 54. Выведите из предыдущей задачи неравенство $\alpha(G_{1/2}(n, 2, 1)) \leq (\frac{1}{2} + \varepsilon) n \log_2 n$, справедливое при каждом $\varepsilon > 0$ почти наверное.

Решение. С учетом оценки из задачи 53 имеем

$$\begin{aligned} \sum_{A \subset V(n, 2), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}|} &< C_n^k 2^{-(1+o(1))\frac{2k^2}{n}} < \left(\frac{eC_n^2}{k}\right)^k 2^{-(1+o(1))\frac{2k^2}{n}} < 2^k n^{2k} k^{-k} 2^{-(1+o(1))\frac{2k^2}{n}} = \\ &= 2^{2k \log_2 n - (1+o(1))k \log_2 k - (1+o(1))\frac{2k^2}{n}}. \end{aligned}$$

Следовательно, при подходящем $k \sim \frac{1}{2} n \log_2 n$ получаем

$$2 \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{2k}{n} < 0,$$

откуда

$$2k \log_2 n - (1 + o(1))k \log_2 k - (1 + o(1))\frac{2k^2}{n} = k \left(2 \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{2k}{n} \right) \rightarrow -\infty,$$

То есть мы получили, что $\mathbb{P}(X_k \geq 1) \leq \mathbb{M}X_k \rightarrow 0$, и оценка доказана.

Задача 55*. Докажите нижнюю оценку для $\alpha(G_{1/2}(n, 2, 1))$, имеющую порядок роста $cn \log_2 n$ с некоторым $c > 0$.

Решение. Доказательство данного факта мы не приводим, поскольку это займет достаточно много места. Однако любой желающий может найти его в статье [5].

Задача 56.** Найдите константу c в утверждении: для любого $\varepsilon > 0$ почти наверное

$$(c - \varepsilon)n \log_2 n \leq \alpha(G_{1/2}(n, 2, 1)) \leq (c + \varepsilon)n \log_2 n.$$

Решение. К сожалению, к началу конференции данная задача решена не была. И школьники это не изменили.

Список цитированной литературы

- [1] А.М. Райгородский, *Хроматические числа*, Москва, МЦНМО, 2003.
- [2] А.М. Райгородский, *Линейно-алгебраический метод в комбинаторике*, Москва, МЦНМО, 2007.
- [3] А.М. Райгородский, *Вероятность и алгебра в комбинаторике*, Москва, МЦНМО, 2010.
- [4] А.М. Райгородский, *Модели случайных графов*, Москва, МЦНМО, 2011.
- [5] Л.И. Боголюбский, А.С. Гусев, М.М. Пядеркин, А.М. Райгородский, *Числа независимости и хроматические числа случайных подграфов некоторых дистанционных графов*, Матем. сборник, 2014.
- [6] J. Balogh, A.V. Kostochka, A.M. Raigorodskii, *Coloring some finite sets in \mathbb{R}^n* , *Discussiones Mathematicae Graph Theory*, 33 (2013), N1, 25 - 31.

Combinatorial geometry and graph colorings: from algebra to probability

A.M. Raigorodskii, with the help of V. Bulankina and A. Gusev

1 Definitions and notation

One of the most famous and fascinating objects of combinatorial geometry is *the chromatic number of a space*. Before we introduce it, we remind that the space \mathbb{R}^n , which is called *the n -dimensional Euclidean space*, is just the set of all “points” \mathbf{x} , each of which is a sequence consisting of n real numbers: $\mathbf{x} = (x_1, \dots, x_n)$. Moreover, between any two points $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$, one can find the distance using the formula

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

In particular, for $n = 1$, we get the usual line, for $n = 2$ — the usual plane, for $n = 3$ — the usual space.

The chromatic number of \mathbb{R}^n is the quantity denoted by $\chi(\mathbb{R}^n)$ and equal to the minimum number of colors needed to color all the points of the space \mathbb{R}^n , so that the distance between any two points of the same color is not 1.

We will start from the simplest facts, which are widely known, and we will finally come to advanced results obtained just few months before the Summer Conference. Moreover, the methods, which we shall study, will be very different and nontrivial varying from linear algebra to probability theory and random graphs.

2 Problems before the intermediate finish

2.1 The simplest bounds for the chromatic number

Problem 1. Prove that $\chi(\mathbb{R}^1) = 2$.

Problem 2. Prove that $\chi(\mathbb{R}^2) \geq 4$.

Problem 3. Prove that $\chi(\mathbb{R}^2) \leq 7$.

Problem 4. Prove that $\chi(\mathbb{R}^3) \leq 27$.

Problem 5. Prove that $\chi(\mathbb{R}^3) \geq 5$.

Problem 6. Prove that $\chi(\mathbb{R}^n)$ is finite for every n .

Problem 7*. Prove that $\chi(\mathbb{R}^n) \leq (\lceil \sqrt{n} \rceil + 1)^n$.

Problem 8. Prove that in \mathbb{R}^n there is a set of $n + 1$ points, whose pairwise distances are equal to 1, and therefore, $\chi(\mathbb{R}^n) \geq n + 1$.

Problem 9*. Prove that $\chi(\mathbb{R}^n) \geq n + 2$.

2.2 Distance graphs of special type, their simplest properties, and the connection with the chromatic number of a space

Recall that the scalar product of vectors $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n)$ in \mathbb{R}^n is the expression

$$(\mathbf{x}, \mathbf{y}) = x_1y_1 + \dots + x_ny_n.$$

One can easily check that always

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}). \quad (1)$$

Let r, s be some natural numbers. For each $n \in \mathbb{N}$ denote by $G(n, r, s)$ the graph, whose set of vertices is

$$V(n, r) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = r\}$$

and whose set of edges is

$$E(n, r, s) = \{\{\mathbf{x}, \mathbf{y}\} : (\mathbf{x}, \mathbf{y}) = s\}.$$

In other words, vertices are all possible vectors consisting of 0s and 1s, such that in every such vector one has exactly r 1s and $n - r$ 0s. In turn, by edges those and only those vertices are joined whose scalar product equals s . Due to formula (1) one can say that edges are those and only those pairs of vertices whose distance equals $\sqrt{2r - 2s}$. This is why the graphs $G(n, r, s)$ are called *distance graphs*.

It is also convenient to have the following interpretation of a graph $G(n, r, s)$. Its vertices can be considered as all possible r -element subsets of the set $\mathcal{R}_n = \{1, 2, \dots, n\}$. Its edges can be considered as pairs of subsets whose intersections have cardinalities equal to s . Please make sure that you understand it!

Recall that an *independent set* of vertices of a graph is a set, in which every two vertices are not joined by an edge. The *independence number* $\alpha(G)$ of a graph G is the number of vertices in any maximal (by cardinality) independent set. The *chromatic number* $\chi(G)$ of a graph G is the minimum number of colors needed to color all the vertices of the graph in such a way that between any two vertices of the same color, there are no edges.

Problem 10. Prove that for any n, r, s , one has $\chi(\mathbb{R}^n) \geq \chi(G(n, r, s))$.

Problem 11. Prove that for every graph $G = (V, E)$, one has $\chi(G) \geq \frac{|V|}{\alpha(G)}$.

Problem 12. Find $\alpha(G(n, 3, 1))$. Derive from the obtained result a considerable improvement to the bound in the problem 9.

Problem 13*. Find $\chi(G(n, 3, 1))$ for $n = 2^k$. **Hint.** Use the problems 11 and 12 as well as the following lemma and induction by k .

Lemma 1. Let n be an even number and P_n be the set of all unordered pairs $\{a, b\}$ of natural numbers both of which do not exceed n . Then there exist such sets of pairs B_1, \dots, B_{n-1} that

$$P_n = B_1 \sqcup \dots \sqcup B_{n-1}.$$

Moreover, for any $i = 1, \dots, n - 1$, no two pairs from B_i contain a common element. For odd n , we have a partition

$$P_n = B_1 \sqcup \dots \sqcup B_n,$$

and, again for any $i = 1, \dots, n$, no two pairs from B_i contain a common element.

Problem 14.** Find sharpest possible bounds (ideally — a formula) for $\chi(G(n, 3, 1))$ for every n .

Problem 15. Prove that $\alpha(G(n, r, s)) \geq C_{n-s-1}^{r-s-1}$.

Problem 16*. Prove that $\alpha(G(n, r, 0)) = C_{n-1}^{r-1}$, if $2r \leq n$.

Problem 17. Prove that $\chi(G(n, r, 0)) \leq n - 2r + 2$, if $2r \leq n$.

Problem 18. Prove that $\chi(G(n, r, s)) \leq C_r^s C_{n-r}^{r-s} + 1$.

Problem 19. Prove that $\chi(G(n, r, s)) \leq C_n^{s+1}$.

Problem 20*. Let $k = \lceil \frac{r-1}{s} \rceil$. Prove that $\chi(G(n, r, s)) \leq k \cdot C_{\lfloor \frac{n}{k} \rfloor}^{s+1}$.

Problem 21*. Prove that $n - r + 1 \leq \chi(G(n, r, r - 1)) \leq n$ for $n = 2^k$. **Hint.** Use Lemma 1 and induction by r and k .

Problem 22.** Find $\chi(G(n, r, r - 1))$ or at least refine the bounds from the problem 21.

Please find out that none of the results that you have obtained does not allow you to improve the lower bounds of the value $\chi(\mathbb{R}^n)$ found in the problems 9, 12. In view of the problem 11, it be good to study upper bounds for the independence numbers of the graphs $G(n, r, s)$. It turns out that many of such bounds can be obtained with the help of the linear algebra method. Thus, in the next section, we will recall some basic notions of linear algebra.

2.3 Basics of linear algebra and its applications

We say that vectors $\mathbf{x}_1, \dots, \mathbf{x}_t$ in \mathbb{R}^n are *linearly independent*, if the equality $c_1\mathbf{x}_1 + \dots + c_t\mathbf{x}_t = 0$ is possible only in the case when $c_1 = \dots = c_t = 0$.

Problem 23. Prove that the maximum number of linearly independent vectors in \mathbb{R}^n equals n .

Problem 24. Prove that if $\mathbf{x}_1, \dots, \mathbf{x}_n$ form an arbitrary system of linearly independent vectors in \mathbb{R}^n , then any vector $\mathbf{x} \in \mathbb{R}^n$ can be represented as $\mathbf{x} = c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n$, where c_1, \dots, c_n are real numbers. (The system $\mathbf{x}_1, \dots, \mathbf{x}_n$ is called a *basis* of the space and the expression $c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n$ is called *linear combination* of the vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$ with *coefficients* c_1, \dots, c_n . In these terms, any vector $\mathbf{x} \in \mathbb{R}^n$ can be represented as a linear combination of the vectors of the basis.)

Let p be a prime number. Let \mathbb{Z}_p be the set of congruences modulo p . The space \mathbb{Z}_p^n , similarly to \mathbb{R}^n , is just the set of all the sequences of numbers from \mathbb{Z}_p . The operations of the sum of “vectors” $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^n$ and of their product with elements of \mathbb{Z}_p is done, as usual, coordinate by coordinate, but, this time, every coordinate is taken modulo p .

The notions of linear independence and of a basis for \mathbb{Z}_p^n are defined in the same way as for \mathbb{R}^n . However, here all the numbers c_i are elements of \mathbb{Z}_p — not \mathbb{R} , — and the equality to zero is understood as the equality to zero modulo p .

Problem 25. Prove that the maximum number of linearly independent vectors in \mathbb{Z}_p^n equals n and that any maximal system forms a basis.

Problem 26. Let $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ be an arbitrary independent set of vertices of the graph $G(n, 3, 1)$. Prove that the vectors $\mathbf{x}_1, \dots, \mathbf{x}_t$ are linearly independent in \mathbb{Z}_2^n and thus $\alpha(G(n, 3, 1)) \leq n$, which is only by an “epsilon” weaker than the result of the problem 12!

Let $F \in \{\mathbb{R}, \mathbb{Z}_p\}$. Let x_1, \dots, x_n be “variables”. By a *monomial* depending on these n variables we mean an expression of the form $x_1^{a_1} \dots x_n^{a_n}$, where a_1, \dots, a_n are some non-negative integers. A *polynomial* is an arbitrary linear combination of monomials. More precisely, a polynomial P belongs to $F[x_1, \dots, x_n]$, if its coefficients are from F . Polynomials are added and multiplied according to the usual rules. Also if $P \in F[x_1, \dots, x_n]$, then it can be multiplied by any element of F . In any case, the rules of summation and multiplication of the coefficients of polynomials are defined by the rules of summation and multiplication in the set F . The *degree* of a monomial is the sum of the degrees of its variables. The degree of a polynomial is the maximum of the degrees of its monomials. A polynomial $P \in F[x_1, \dots, x_n]$ *equals zero*, if all its coefficients are equal to zero in F . Polynomials $P_1 \in F[x_1, \dots, x_n], \dots, P_t \in F[x_1, \dots, x_n]$ are *linearly independent* over F , if $c_1 P_1 + \dots + c_t P_t = 0$ only in the case when all the numbers $c_1 \in F, \dots, c_t \in F$ are equal to zero in F . It is obvious that any polynomial is generated by the *basis* consisting of its monomials.

Problem 27. Prove that if some polynomials are linearly independent over their F , then their number does not exceed the number of monomials in a basis, which generates all these polynomials.

Problem 28. Let $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ be an arbitrary independent set of vertices of the graph $G(n, 5, 2)$. Let polynomials $P_1 \in \mathbb{Z}_3[y_1, \dots, y_n], P_2 \in \mathbb{Z}_3[y_1, \dots, y_n], \dots, P_t \in \mathbb{Z}_3[y_1, \dots, y_n]$ be given by formulae

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1), \quad i = 1, \dots, t.$$

For example, if $\mathbf{x}_1 = (1, 1, 1, 1, 1, 0, \dots, 0)$, $\mathbf{x}_2 = (0, \dots, 0, 1, 1, 1, 1, 1)$, then

$$P_1(y_1, \dots, y_n) = (y_1 + y_2 + y_3 + y_4 + y_5)(y_1 + y_2 + y_3 + y_4 + y_5 - 1) = y_1^2 + \dots + y_5^2 + 2y_1 y_2 + \dots + 2y_4 y_5 - y_1 - \dots - y_5,$$

$$\begin{aligned} P_2(y_1, \dots, y_n) &= (y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n)(y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n - 1) = \\ &= y_{n-4}^2 + \dots + y_n^2 + 2y_{n-4} y_{n-3} + \dots + 2y_{n-1} y_n - y_{n-4} - \dots - y_n. \end{aligned}$$

Prove that the polynomials P_1, \dots, P_t are linearly independent over \mathbb{Z}_3 and therefore $\alpha(G(n, 5, 2)) \leq C_n^2 + 2C_n^1$.

Problem 29. Assume that in the conditions of the previous problem the polynomials P_i are substituted by P'_i according to the following rule: every monomial of the form y_i^2 is changed by y_i , and after that monomials of the same form are added. Prove that the polynomials P'_1, \dots, P'_t corresponding to the vectors from an independent set of vertices W of the graph $G(n, 5, 2)$ are also linearly independent over \mathbb{Z}_3 , similarly to the initial polynomials P_1, \dots, P_t . Derive from this fact the bound $\alpha(G(n, 5, 2)) \leq C_n^2$ and compare it with the bound from the problem 15.

Problem 30. Derive from the result of the previous problem a lower bound for $\chi(\mathbb{R}^n)$, which considerably improves the bound from the problem 12. Ensure yourselves, however, that, in view of the problem 19, substantial further advances based on the graph $G(n, 5, 2)$ cannot be done.

Problem 31. Let $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ be an arbitrary independent set of vertices of the graph $G(n, 9, 4)$. Let polynomials $P_1 \in \mathbb{Z}_5[y_1, \dots, y_n]$, $P_2 \in \mathbb{Z}_5[y_1, \dots, y_n]$, \dots , $P_t \in \mathbb{Z}_5[y_1, \dots, y_n]$ be given by the formulae

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1)((\mathbf{x}_i, \mathbf{y}) - 2)((\mathbf{x}_i, \mathbf{y}) - 3), \quad i = 1, \dots, t.$$

Prove that the polynomials P_1, \dots, P_t are linearly independent over \mathbb{Z}_5 .

Problem 32. Which upper bound for $\alpha(G(n, 9, 4))$ follows from the previous problem?

Problem 33. Let in the conditions of the problem 31 the polynomials P_i be replaced by some P'_i according to the following rule: in them, every monomial, which appears after opening the brackets and summing similar monomials, has of course the form $y_1^{a_1} \cdot \dots \cdot y_n^{a_n}$; if among the numbers a_i , one has some numbers greater than or equal to 2, then we replace all of them by 1s and sum up similar monomials. For example, the monomial $y_1^2 y_2^2$ is transformed to $y_1 y_2$ and the same is true for the monomials $y_1^2 y_2, y_1 y_2^2$, etc. Prove that the polynomials P'_1, \dots, P'_t corresponding to the vectors from an independent set W of the graph $G(n, 9, 4)$ are also linearly independent over \mathbb{Z}_5 , just as it was with the initial polynomials P_1, \dots, P_t . Derive from this fact the bound $\alpha(G(n, 9, 4)) \leq C_n^4 + C_n^3 + C_n^2 + C_n^1 + C_n^0$ and compare it with the bound from the problem 15.

Problem 34. Derive from the result of the previous problem a lower bound for $\chi(\mathbb{R}^n)$, which considerably refines the bound from the problem 30. Ensure yourselves, however, that, in view of the problem 19, substantial further advances based on the graph $G(n, 9, 4)$ cannot be done.

Problem 35. Let r and s be such that $r - s = p$, where p is a prime number and $r - 2p < 0$. Prove that $\alpha(G(n, r, s)) \leq \sum_{k=0}^{p-1} C_n^k$. Compare this bound with the bound from the problem 15.

Problem 36*. Explore lower bounds for the quantity $\chi(\mathbb{R}^n)$, which follow from the results of the previous problem. How do these bounds correlate with the bounds from the problem 19?

3 Problems after the intermediate finish

Before the intermediate finish we have seen how important are the independence numbers of graphs for obtaining lower bounds on the chromatic number of a space. Moreover, we considered different sequences of distance graphs — the sequences $\{G(n, r, s)\}_{n=1}^{\infty}$ with given r and s . It is interesting to understand how will be changed the independence numbers, if, instead of the graphs $G(n, r, s)$, we take their spanning subgraphs, i.e., if we take the same sets of vertices and partially remove the edges. It seems to be evident that the independence numbers must become substantially larger, provided we remove many edges. However, surprisingly, sometimes this is true, but sometimes this is completely wrong! In order to obtain the corresponding results, let us learn some random graphs and some probability theory.

3.1 The random Erdős–Rényi graph and some of its probabilistic characteristics

Let $V_n = \{1, \dots, n\}$ be a set of vertices. In principle, one can construct on this set C_n^2 edges, if we do not allow multiple edges, loops and orientation. Let us each of these C_n^2 potential edges draw with *probability* $p \in [0, 1]$, which is the same for every edge. Different edges appear independently. Let $G = (V_n, E)$ be a graph which can appear as a result of the just-described probabilistic procedure. Denote the probability

of its appearance by $\mathbb{P}(G)$. Clearly it is equal to $p^{|E|}(1-p)^{C_n^2-|E|}$. If A is a property of a graph, then its probability — $\mathbb{P}(A)$ — is the sum over all the graphs G , which have property A , of the probabilities of these graphs.

Denote by Ω_n the set of all graphs on the vertices V_n . Any function X defined on Ω_n and taking real values is called *random variable*. For example, the number of triangles in a graph or its number of connected components, or its independence number are random variables. Here you must understand that the variables are random only due to the fact that a priori we do not know which graph will (randomly) come to us. When a graph is already born the value of X is determined uniquely!

Any random variable has some “mean value” — the so-called (*mathematical*) *expectation*. The expectation of a variable X is the number $\mathbb{M}X$ defined by the formula $\mathbb{M}X = \sum_{G \in \Omega_n} X(G)\mathbb{P}(G)$. We just sum up the values of the function X on all the graphs multiplied by the probabilities of these graphs. Of course this is some weighted average (weights are probabilities) — a kind of the mass centre). Let us learn to calculate expectations and apply the obtained results to the study of the properties of random graphs.

Problem 37. Prove that if a random variable is just a constant c , then $\mathbb{M}c = c$.

Problem 38. Let X_1, X_2 be random variables and c_1, c_2 be some fixed numbers. Certainly $c_1X_1 + c_2X_2$ is also a random variable. Prove that its expectation equals $c_1\mathbb{M}X_1 + c_2\mathbb{M}X_2$. This property is called *linearity of expectation*.

Problem 39. Using linearity of expectation find expectations of a) the number of triangles in the random graph; b) the number of connected components of the random graph, each of which is a cycle on k vertices (k is a fixed given number); c) the number of independent sets in the random graph, each of which has cardinality k (k is a fixed given number).

Problem 40. Prove *Markov’s inequality*: if X is a random variable taking non-negative values and a is a positive number, then $\mathbb{P}(X \geq a) \leq \frac{\mathbb{M}X}{a}$.

Problem 41. Using Markov’s inequality prove that if $p = \frac{1}{2}$, then $\mathbb{P}(\alpha(G) \leq 2 \log_2 n) \rightarrow 1$ as $n \rightarrow \infty$ (it is used to say that “almost surely $\alpha(G) \leq 2 \log_2 n$ ”).

Note that actually for $p = \frac{1}{2}$ almost surely $\alpha(G) \geq (2 - \varepsilon) \log_2 n$ for any given arbitrarily small $\varepsilon > 0$. More precisely, — and we shall use it later, — the following theorem holds.

Theorem 1. For any $\varepsilon > 0$ and large enough n the inequality

$$\mathbb{P}(\alpha(G) \geq (2 - \varepsilon) \log_2 n) > 1 - 2^{-n}$$

holds.

Thus, for $p = \frac{1}{2}$, almost surely the independence number is approximately $2 \log_2 n$. In other words, what’s happening? We take the complete graph on n vertices and we delete some of its edges, each with probability $\frac{1}{2}$. A typical graph, which appears as a result of this procedure, has about $\frac{C_n^2}{2}$ edges — two times less than the complete graph has. And the independence number of a typical graph is in a logarithm times greater than the independence number of the initial graph (the independence number of the complete graph is of course 1). OK, the number of edges is two times smaller and the independence number increases: quite natural. It turns out that for some $G(n, r, s)$ when deleting their edges randomly, we get the same “expected” result (the independence number becomes approximately \log times bigger). But the miracle is that this happens not everytime! For many $G(n, r, s)$ the independence number does not change at all! Below, we will study together examples of both situations.

3.2 Random subgraphs of the graph $G(n, 3, 0)$

Let $G_{1/2}(n, 3, 0)$ be a random subgraph of the graph $G(n, 3, 0)$ obtained by deleting mutually independently some edges of the graph $G(n, 3, 0)$, each with probability $1/2$.

Problem 42. If you solved the problem 16, then just derive from it that $\alpha(G(n, 3, 0)) = C_{n-1}^2$. Otherwise, try to solve this particular case of that problem.

In a series of problems below, we will prove that almost surely $\alpha(G_{1/2}(n, 3, 0)) \leq C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. This is exactly what we mentioned above speaking about a surprising phenomenon: there is no growth in log times; if there is some growth, then it is only in such a number of times that itself tends to 1 as $n \rightarrow \infty$! One can prove even stronger facts, but this is very difficult, and we do not want to do it here: we just want to see the essence!

In what follows, we will for conciseness omit integer parts around quantities which must be integer. For example, writing $C_{\log_2 n}^k$ means, depending on context, that actually we take an upper or a lower integer part of the number $\log_2 n$. None of the computations will become false after this roughening.

Problem 43. Put $k = C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. Assume that k is integer (cf. a remark before the problem). Let $A \subset V(n, 3)$ be an arbitrary set of vertices of the graph $G(n, 3, 0)$ having cardinality k . Denote by $r(A)$ the number of edges of the graph $G(n, 3, 0)$, whose both ends are in A . Since $|A| = k > \alpha(G(n, 3, 0))$, it is clear that $r(A) > 0$. Let X_k be the random variable equal to the number of independent sets of size k in a graph $G_{1/2}(n, 3, 0)$. Prove that

$$\mathbb{M}X_k = \sum_{A \subset V(n, 3): |A|=k} \left(\frac{1}{2}\right)^{r(A)}. \quad (2)$$

Problem 44. Prove that our aim will be attained, if we will prove that $\mathbb{M}X_k \rightarrow 0$ as $n \rightarrow \infty$.

Clearly we have to learn bounding *from below* the quantity $r(A)$. For each A , denote by $B = B(A)$ any (chosen for everytime) subset of A , which is independent in $G(n, 3, 0)$ and has the maximum cardinality among all analogous subsets of the set A .

Problem 45. Let $A \subset V(n, 3)$, $|A| = k$. Let $B = B(A)$. Note that $k \approx \frac{n^2}{2}$. Assume that $|B|$ is substantially smaller than k : for example, let $|B| < n^{1.9}$ (here the strange number 1.9 is taken almost arbitrarily; important is that it is strictly smaller than 2). Prove that for large enough n the inequality $r(A) \geq \frac{k^2}{3|B|}$ holds (being more careful one can replace 3 in the denominator by “almost” 2, but does not matter).

Problem 46. Let $A \subset V(n, 3)$, $|A| = k$. Let $B = B(A)$. Let $|B| > 9n$ or, even better (in addition to the previous problem), $|B| \geq n^{1.9}$. Prove that $r(A) \geq (|B| - 9n)(|A| - |B|)$.

Problem 47. Decompose sum (2) into two parts: in the first part, only those A will be taken, for which $|B| < n^{1.9}$; in the second part, all the other sets A will be considered. To the summands in both parts apply the bounds from the corresponding problems and make it sure that the whole sum (2) does really tend to zero, which means that we are done!

How can we change the threshold $n^{1.9}$ in order to still get the same result?

3.3 Random subgraphs of the graph $G(n, 3, 1)$

Let $G_{1/2}(n, 3, 1)$ be a random subgraph of the graph $G(n, 3, 1)$ obtained by deleting mutually independently some edges of the graph $G(n, 3, 1)$, each with probability $1/2$. It seems that everything is the same as with the graphs $G(n, 3, 0)$. This is completely wrong!

Recall that $\alpha(G(n, 3, 1)) \approx n$ (see the problem 12).

Problem 48*. Write down an analog of inequality (2) and prove an analog of the bound from the problem 45. Ensure yourselves eventually that there exists a $c > 0$, with which almost asurely $\alpha(G_{1/2}(n, 3, 1)) \leq cn \log_2 n$.

Problem 49. Prove that in the graph $G(n, 3, 1)$, there exist approximately $\frac{n}{2}$ complete subgraphs, each having about $\frac{n}{4}$ vertices, such that every two of them are not connected by an edge.

Problem 50. With the help of the previous problem and Theorem 1 prove that for every $\varepsilon > 0$, almost surely $\alpha(G_{1/2}(n, 3, 1)) \geq (1 - \varepsilon)n \log_2 n$.

Thus, for $G_{1/2}(n, 3, 1)$, just as it was for the Erdős–Rényi random graph, we again have the growth of the independence number in approximately logarithm of the number of vertices times!

Problem 51*. Try to improve into a constant number of times the bound in the problem 50.

3.4 Random subgraphs of the graph $G(n, 2, 1)$

Problem 52. Find $\alpha(G(n, 2, 1))$.

Problem 53. Let $r(A)$ be the same as in formula (2). Prove that always $r(A) \geq \frac{2|A|^2}{n} - |A|$.

Problem 54. Derive from the previous problem the inequality $\alpha(G_{1/2}(n, 2, 1)) \leq (\frac{1}{2} + \varepsilon)n \log_2 n$, which is true for every $\varepsilon > 0$ almost surely.

Problem 55*. Prove a lower bound for $\alpha(G_{1/2}(n, 2, 1))$ which has order of magnitude $cn \log_2 n$ with some $c > 0$.

Problem 56.** Find a constant c in the assertion: for any $\varepsilon > 0$, almost surely

$$(c - \varepsilon)n \log_2 n \leq \alpha(G_{1/2}(n, 2, 1)) \leq (c + \varepsilon)n \log_2 n.$$

References

- [1] A.M. Raigorodskii, *The chromatic numbers*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2003 (in Russian).
- [2] A.M. Raigorodskii, *The linear algebra method in combinatorics*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2007 (in Russian).
- [3] A.M. Raigorodskii, *Probability and algebra in combinatorics*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2008 (in Russian).

- [4] A.M. Raigorodskii, *Models of random graphs*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2011 (in Russian).

Combinatorial geometry and graph colorings: from algebra to probability

A.M. Raigorodskii, with the help of V. Bulankina and A. Gusev

1 Definitions and notation

One of the most famous and fascinating objects of combinatorial geometry is *the chromatic number of a space*. Before we introduce it, we remind that the space \mathbb{R}^n , which is called *the n -dimensional Euclidean space*, is just the set of all “points” \mathbf{x} , each of which is a sequence consisting of n real numbers: $\mathbf{x} = (x_1, \dots, x_n)$. Moreover, between any two points $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$, one can find the distance using the formula

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

In particular, for $n = 1$, we get the usual line, for $n = 2$ — the usual plane, for $n = 3$ — the usual space.

The chromatic number of \mathbb{R}^n is the quantity denoted by $\chi(\mathbb{R}^n)$ and equal to the minimum number of colors needed to color all the points of the space \mathbb{R}^n , so that the distance between any two points of the same color is not 1.

We will start from the simplest facts, which are widely known, and we will finally come to advanced results obtained just few months before the Summer Conference. Moreover, the methods, which we shall study, will be very different and nontrivial varying from linear algebra to probability theory and random graphs.

2 Problems before the intermediate finish

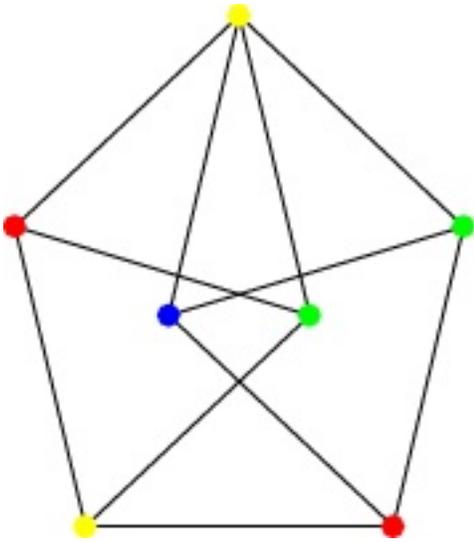
2.1 The simplest bounds for the chromatic number

Problem 1. Prove that $\chi(\mathbb{R}^1) = 2$.

Solution. Clearly, one color is not enough since points 1 and 2 should be of different colors. Two colors suffice. Indeed, let us split the line into semi-open intervals $[a; a + 1)$, $a \in \mathbb{Z}$, and color them in turn into black and white.

Problem 2. Prove that $\chi(\mathbb{R}^2) \geq 4$.

Solution. Clearly, the figure below cannot be colored properly into three colors.



Problem 3. Prove that $\chi(\mathbb{R}^2) \leq 7$.

Solution. One can see that the following coloring is proper:



Problem 4. Prove that $\chi(\mathbb{R}^3) \leq 27$.

Solution. It is the particular case of Problem 7.

Problem 5. Prove that $\chi(\mathbb{R}^3) \geq 5$.

Solution. It is the particular case of Problem 9.

Problem 6. Prove that $\chi(\mathbb{R}^n)$ is finite for every n .

Solution. Problem 6 will follow from Problem 7.

Problem 7*. Prove that $\chi(\mathbb{R}^n) \leq (\lceil \sqrt{n} \rceil + 1)^n$.

Solution. Let us take some $k \in \mathbb{Z}$ and $p \in \mathbb{R}$, tile \mathbb{R}^n with cubes of edge kp , split each edge of some cube into k parts, it will give a splitting of a cube into k^n small cubes of edge p , then color each small cube into its color and then shift this coloring to color the whole space. For the coloring to be proper, the following two inequalities should hold: $p\sqrt{n} \leq 1$, $(k-1)p \geq 1$. But for $k = \lceil \sqrt{n} \rceil + 1$ and $p = \frac{1}{\sqrt{n}}$ both inequalities are held.

Problem 8. Prove that in \mathbb{R}^n there is a set of $n+1$ points, whose pairwise distances are equal to 1, and therefore, $\chi(\mathbb{R}^n) \geq n+1$.

Solution. Let us construct such a set of points explicitly. Let

$$\begin{aligned} A_1 &= \left(\frac{\sqrt{2}}{2}; 0; 0; \dots; 0; 0 \right), \\ A_2 &= \left(0; \frac{\sqrt{2}}{2}; 0; \dots; 0; 0 \right), \\ &\quad \dots, \\ A_n &= \left(0; 0; 0; \dots; 0; \frac{\sqrt{2}}{2} \right). \end{aligned}$$

Pairwise distances between these n points are all equal to 1. Now find the $(n+1)$ th point of the form $S = (a; a; a; \dots; a; a)$. For this we need

$$\begin{aligned} SA_i &= \sqrt{(n-1)a^2 + \left(a - \frac{\sqrt{2}}{2}\right)^2} = 1, \\ na^2 - \sqrt{2}a - \frac{1}{2} &= 0. \end{aligned}$$

This system gives us a quadratic equation with positive discriminant. Thus, we will find two points S_1 and S_2 , such that for each of them and for every $j = 1, 2, \dots, n$, the distance between S_i and A_j equals 1.

Problem 9*. Prove that $\chi(\mathbb{R}^n) \geq n+2$.

Solution. Let us take two equal figures as in Problem 8, namely, $S_1S_2A_1 \dots A_n$ and $T_1T_2B_1 \dots B_n$. We can place them in \mathbb{R}^n in such a way that S_1 coincides with T_1 , and the distance S_2T_2 equals 1. Now, if we color \mathbb{R}^n into $n+1$ color, then the points S_1 and S_2 will be of one color, and the points T_1 and T_2 will be of one color. Then S_2 and T_2 will be of one color, which is impossible.

2.2 Distance graphs of special type, their simplest properties, and the connection with the chromatic number of a space

Recall that the scalar product of vectors $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{y} = (y_1, \dots, y_n)$ in \mathbb{R}^n is the expression

$$(\mathbf{x}, \mathbf{y}) = x_1y_1 + \dots + x_ny_n.$$

One can easily check that always

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}). \quad (1)$$

Let r, s be some natural numbers. For each $n \in \mathbb{N}$ denote by $G(n, r, s)$ the graph, whose set of vertices is

$$V(n, r) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = r\}$$

and whose set of edges is

$$E(n, r, s) = \{\{\mathbf{x}, \mathbf{y}\} : (\mathbf{x}, \mathbf{y}) = s\}.$$

In other words, vertices are all possible vectors consisting of 0s and 1s, such that in every such vector one has exactly r 1s and $n - r$ 0s. In turn, those and only those vertices are joined by edges whose scalar product equals s . Due to formula (1) one can say that edges are those and only those pairs of vertices whose distance equals $\sqrt{2r - 2s}$. This is why the graphs $G(n, r, s)$ are called *distance graphs*.

It is also convenient to have the following interpretation of a graph $G(n, r, s)$. Its vertices can be considered as all possible r -element subsets of the set $\mathcal{R}_n = \{1, 2, \dots, n\}$. Its edges can be considered as pairs of subsets whose intersections have cardinalities equal to s . Please make sure that you understand it!

Recall that an *independent set* of vertices of a graph is a set, in which every two vertices are not joined by an edge. The *independence number* $\alpha(G)$ of a graph G is the number of vertices in any maximal (by cardinality) independent set. The *chromatic number* $\chi(G)$ of a graph G is the minimum number of colors needed to color all the vertices of the graph in such a way that between any two vertices of the same color, there are no edges.

Problem 10. Prove that for any n, r, s , one has $\chi(\mathbb{R}^n) \geq \chi(G(n, r, s))$.

Solution. The graph $G(n, r, s)$ can be embedded into \mathbb{R}^n : first, we map every vector consisting of 0s and 1s to the corresponding point, then the distances between all points are equal to $\sqrt{2r - 2s}$, and second, we make a homothety with coefficient $\frac{1}{\sqrt{2r - 2s}}$, thus making all pairwise distances equal to 1. Hence, if we can properly color the space into k colors, then we can also properly color the vertices of the graph $G(n, r, s)$.

Problem 11. Prove that for every graph $G = (V, E)$, one has $\chi(G) \geq \frac{|V|}{\alpha(G)}$.

Solution. Every color should be an independent set, hence, its cardinality will not exceed $\alpha(G)$. Let us increase the quantity of vertices of every color and make it equal to $\alpha(G)$, then the total number of vertices will increase and become equal to $\chi(G) \cdot \alpha(G) \geq |V|$. It implies the desired inequality.

Problem 12. Find $\alpha(G(n, 3, 1))$. Derive from the obtained result a considerable improvement to the bound in Problem 9.

Solution. The answer depends on the residue of n modulo 4. We will prove by induction that

$$\begin{aligned} n \equiv 0 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n, \\ n \equiv 1 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n - 1, \\ n \equiv 2 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n - 2, \\ n \equiv 3 \pmod{4} &\Rightarrow \alpha(G(n, 3, 1)) = n - 2, \end{aligned}$$

Every vector consists of zeroes and ones. Fix any independent set. It follows from the condition that every two distinct vectors in it either do not intersect, or intersect by 2 elements. First we give examples which show that $\alpha(G(n, 3, 1))$ is at least the required number. For $n = 4$

$$\begin{aligned} & (0, 1, 1, 1), \\ & (1, 0, 1, 1), \\ & (1, 1, 0, 1), \\ & (1, 1, 1, 0). \end{aligned} \tag{1}$$

For n divisible by 4 we split the coordinates into groups of 4 and in every group perform the same construction as above.

For $n \equiv 1 \pmod{4}$ we forget one coordinate and repeat the same construction as above.

For other values of n , we give another construction:

$$\begin{aligned} & (1, 1, 1, 0, \dots, 0), \\ & (1, 1, 0, 1, 0, \dots, 0), \\ & (1, 1, 0, 0, 1, 0, \dots, 0), \\ & \dots, \\ & (1, 1, 0, 0, \dots, 0, 1, 0), \\ & (1, 1, 0, 0, \dots, 0, 0, 1), \end{aligned} \tag{2}$$

Here two first coordinates are always equal to 1, hence, every two vectors intersect in exactly two coordinates. This example contains $n - 2$ vectors.

Now we prove that it is the maximal possible value. Take two intersecting vectors, without loss of generality they are

$$(1, 1, 1, 0, \dots, 1) \text{ and } (1, 1, 0, 1, 0, \dots, 0).$$

Now take any other vector. Either it has a nonzero coordinate on the position n , or it is as in (1). In the first case the vector is of form $(1, 1, 0, 0, \dots, 0, 1, 0, \dots)$, and the vectors of the second type are no more possible, in the second case we have no more than 4 vectors which have nonzero coordinates on the first 4 positions, and we can apply the induction step. In the first case we have no more than $n - 2$ vectors, as in (2). It is not more than in the answer, and we are done.

We get the following bound for the chromatic number:

$$\chi(\mathbb{R}^n) \geq \chi(G(n, 3, 1)) \geq \frac{C_n^3}{\alpha(G(n, 3, 1))} \geq \frac{(n-1)(n-2)}{6}.$$

Problem 13*. Find $\chi(G(n, 3, 1))$ for $n = 2^k$. **Hint.** Use Problems 11 and 12 as well as the following lemma and induction by k .

Solution. The proof of this theorem can be found in [6].

Lemma 1. Let n be an even number and P_n be the set of all unordered pairs $\{a, b\}$ of natural numbers both of which do not exceed n . Then there exist such sets of pairs B_1, \dots, B_{n-1} that

$$P_n = B_1 \sqcup \dots \sqcup B_{n-1}.$$

Moreover, for any $i = 1, \dots, n-1$, no two pairs from B_i contain a common element. For odd n , we have a partition

$$P_n = B_1 \sqcup \dots \sqcup B_n,$$

and, again for any $i = 1, \dots, n$, no two pairs from B_i contain a common element.

Problem 14.** Find sharpest possible bounds (ideally — a formula) for $\chi(G(n, 3, 1))$ for every n .

Solution. This problem has two stars, hence, if you have solved it, you could obtain a new result.

Problem 15. Prove that $\alpha(G(n, r, s)) \geq C_{n-s-1}^{r-s-1}$.

Solution. Consider only those vertices which have ones at the first $s + 1$ positions. There are C_{n-s-1}^{r-s-1} such vertices. The scalar product of any two of them is at least $s + 1$, hence, no two of them are joined by an edge.

Problem 16*. Prove that $\alpha(G(n, r, 0)) = C_{n-1}^{r-1}$, if $2r \leq n$.

Solution. Let us denote by B any (fixed throughout the proof) subset in the set of vertices $V(n, r)$, which is independent in $G(n, r, 0)$ and has cardinality $\alpha(G(n, r, 0))$.

Lemma. For every $s, 1 \leq s \leq n$, let us consider the set $A_s = \{s, s + 1, \dots, s + r - 1\}$, where the sum is modulo n . Then B cannot contain more than r subsets of form A_s .

Proof. Fix any A_s from $\alpha(G(n, r, 0))$. Take all the other sets A_k intersecting A_s and form $r - 1$ pairs $\{A_{s-i}, A_{s+r-i}\}$. Now the statement of Lemma follows from the fact that B contains at most one element from each pair.

Let us deduce the Problem statement from the Lemma. Take an arbitrary permutation σ of elements $\{1, 2, \dots, n\}$ and fix $i \in \{1, 2, \dots, n\}$. Let $A = \{\sigma(i), \sigma(i + 1), \dots, \sigma(i + r - 1)\}$, where the sum is taken modulo n , as above. Since σ was an arbitrary permutation, it follows from Lemma that $P(A \in B) \leq \frac{r}{n}$. But A is taken equiprobably from all the r -element subsets. Hence,

$$\frac{r}{n} \geq P(A \in B) = \frac{|B|}{C_n^r}$$

and

$$|B| \leq \frac{r}{n} C_n^r = C_{n-1}^{r-1}.$$

Problem 17. Prove that $\chi(G(n, r, 0)) \leq n - 2r + 2$, if $2r \leq n$.

Solution. Let us color all the vertices having 1st coordinate equal to one into the first color. Then let us color all the yet uncolored vertices, which have second coordinate equal to 1, into the second color, and so on till the $(n - 2r + 1)$ th color. Clearly, there will be no edges between the vertices of one color. It remains to color some vertices, and we have one more color. But what vertices are yet uncolored? Only those who have only ones on the last $2r - 1$ coordinates. Clearly, there are no edges between these vertices, hence, we can color them all in the remaining color.

Problem 18. Prove that $\chi(G(n, r, s)) \leq C_r^s C_{n-r}^{r-s} + 1$.

Solution. What is $C_r^s C_{n-r}^{r-s}$? It is the degree of every vertex of the graph $G(n, r, s)$. It is easy to see that if the degree of every vertex of the graph does not exceed d , then the graph can be properly colored into $d + 1$ colors. Indeed, let us color the vertices one by one. For every yet uncolored vertex, there exists at least one color such that our vertex is not connected with vertices of this color. Hence, we can color it in this color.

Problem 19. Prove that $\chi(G(n, r, s)) \leq C_n^{s+1}$.

Solution. Let us enumerate all the $(s + 1)$ -element subsets of \mathcal{R}_n with numbers $1, \dots, C_n^{s+1}$. Now let us color all the vertices containing the first subset into the first color, all the yet uncolored vertices containing the second subset into the second color, and so on. Finally, all the vertices will be colored, and there will be no edges between the vertices of one color.

Problem 20*. Let $k = \lceil \frac{r-1}{s} \rceil$. Prove that $\chi(G(n, r, s)) \leq k \cdot C_{\lfloor \frac{n}{k} \rfloor}^{s+1}$.

Solution. The proof of this fact can be found in [6].

Problem 21*. Prove that $n - r + 1 \leq \chi(G(n, r, r - 1)) \leq n$ for $n = 2^k$. **Hint.** Use Lemma 1 (see above) and induction by r and k .

Solution. To prove the lower bound, we show that the graph contains a clique of size $n - r + 1$. Indeed, let us take the vertices corresponding to the vectors having ones on the first $r - 1$ coordinates. There are exactly $n - r + 1$ such vertices, and they are all mutually joined by edges.

Consider the particular case $r = 2$. Let us show that Lemma 1 implies the inequality $\chi(G(n, 2, 1)) \leq n$. Indeed, let us identify the vertices of $G(n, 2, 1)$ with the set of pairs of integers $1, \dots, n$, and two vertices are joined by an edge if and only if the corresponding pairs have a common element. Hence, if we take colors $\chi_i = B_i$ from Lemma 1, then the graph will be colored into $n - 1$ colors for $n = 2m$ and into n colors for $n = 2m + 1$.

Now take arbitrary r and prove the upper bound by induction on r . Its base $r = 2$ is proved above. Suppose that the upper bound is true for all $r < k$. Let us prove the step, for this we need to color the graph $G(n, k, k - 1)$.

Let $n = 2^l$. To color the graph $G(n, k, k - 1)$, we use induction on l . The base will be for the maximal l_0 such that $2^{l_0} < k$. For this l_0 we have $\chi(G(2^{l_0}, k, k - 1)) = 0$, and the upper bound is satisfied. Now we prove the induction step. We assume that $\chi(G(2^{l-1}, k, k - 1)) \leq 2^{l-1}$. Let us split the set of elements into two parts:

$$\begin{aligned} A_1 &= \{1, \dots, n/2\}, \\ A_2 &= \{n/2 + 1, \dots, n\}. \end{aligned}$$

Split the vertices of our graph into $k + 1$ pairwise disjoint sets

$$V_j = \{v \in V(G(n, k, k - 1)) : |v \cap A_1| = j\}, \quad j = 0, \dots, k.$$

We note that for $l = l_0 + 1$ some V_j s are empty. It will only improve the bound, hence, below we assume that all V_j are nonempty.

Consider the graph $G(n/2, j, j - 1)$ for $j = 1, \dots, k - 1$. By the induction assumption, $\chi(G(n/2, j, j - 1)) \leq n/2$, and all the j -element subsets of the set A_1 can be colored into $n/2$ colors $\varphi_1, \dots, \varphi_{n/2}$ in such a way that every two such subsets of one color intersect by a number of elements not equal to $j - 1$. Let us denote by $W_{j,1}^\nu$ the set of all such subsets which are colored with color φ_ν . We also introduce the graph $G(n/2, k - j, k - j - 1)$ constructed on the set of elements of A_2 . Then all the $(k - j)$ -element subsets of the set A_2 can be colored with colors $\psi_1, \dots, \psi_{n/2}$ in such a way that subsets, colored with one color, intersect by a number of elements not equal to $k - j - 1$. We denote by $W_{k-j,2}^\mu$ the set of all $(k - j)$ -element subsets of A_2 , colored with the color ψ_μ .

For $\nu \in \{1, \dots, n\}$, let $U_j^{1,\nu} = \{w_1 \sqcup w_2 : w_1 \in W_{j,1}^\nu, w_2 \in W_{j,2}^\nu\}$, and let $U_j^1 = \bigsqcup_{\nu=1}^{n/2} U_j^{1,\nu}$. It is clear that

every two sets from the collection U_j^1 intersect by a number of elements not equal to $k - 1$. Indeed, if this is not true, then there exist vertices $v, w \in U_j^1$ such that $|v \cap w| = k - 1$. Then either $v \cap A_1 = w \cap A_1$, or $v \cap A_2 = w \cap A_2$, hence, the non-coinciding “halves” of these vertices are colored with the same color. Without loss of generality, we assume that $v \cap A_1 = w \cap A_1$, then $v \cap A_2$ and $w \cap A_2$ have at most $k - j - 2$ common elements. Hence, the vertices v and w cannot intersect by $k - 1$ elements, and we get a contradiction. The case $v \cap A_2 = w \cap A_2$ can be treated analogously.

In the same way we can obtain the collection U_j^2 , taking the unions of sets from $W_{j,1}^1$ with sets from $W_{k-j,2}^2$, of sets from $W_{j,1}^2$ with sets from $W_{k-j,2}^3$, \dots , of sets from $W_{1,j}^{n/2}$ with sets from $W_{k-j,2}^1$. Analogously, taking cyclical shifts, we define $U_j^3, \dots, U_j^{n/2}$. Here $j = 1, \dots, k - 1$. By the assumption of the induction on n , there exist collections $U_0^i \cup U_k^i$, which contain subsets of A_2 and A_1 , respectively, and intersecting by a number of elements not equal to $k - 1$ for every $i = 1, \dots, n/2$.

Now we finally define the color χ_i for $i = 1, \dots, n/2$ as the union of collections with even indices:

$$\chi_i = U_0^i \cup U_2^i \cup U_4^i \cup \dots$$

For $i = n/2 + 1, \dots, n$ we take the union of collections with odd indices:

$$\chi_i = U_1^{i-n/2} \cup U_3^{i-n/2} \cup U_5^{i-n/2} \dots$$

Clearly, we colored our graph with not more than n colors, which ends the induction on the parameter n , and, hence, it ends also the induction on r . The upper bound is proved.

Problem 22.** Find $\chi(G(n, r, r - 1))$ or at least refine the bounds from Problem 21.

Solution. This problem has two stars, hence, if you have solved it, you could obtain a new result.

Please find out that none of the results that you have obtained allows you to improve the lower bounds of the value $\chi(\mathbb{R}^n)$ found in Problems 9 and 12. In view of Problem 11, it will be good to study upper bounds for the independence numbers of the graphs $G(n, r, s)$. It turns out that many of such bounds can be obtained with the help of the linear algebra method. Thus, in the next section, we will recall some basic notions of linear algebra.

2.3 Basics of linear algebra and its applications

We say that vectors $\mathbf{x}_1, \dots, \mathbf{x}_t$ in \mathbb{R}^n are *linearly independent*, if the equality $c_1\mathbf{x}_1 + \dots + c_t\mathbf{x}_t = 0$ is possible only in the case when $c_1 = \dots = c_t = 0$.

Problem 23. Prove that the maximum number of linearly independent vectors in \mathbb{R}^n equals n .

Solution. The basis vectors $\mathbf{e}_i = (0, 0, \dots, 0, 1, 0, \dots, 0)$, where one is at the i th position, $i = 1, 2, \dots, n$, are linearly independent, since $c_1\mathbf{e}_1 + c_2\mathbf{e}_2 + \dots + c_n\mathbf{e}_n = (c_1, c_2, \dots, c_n)$. Now we prove by induction on n that every $n + 1$ vectors in \mathbb{R}^n are linearly dependent.

Base $n = 1$ is obvious.

Step from n to $n + 1$. If the $(n + 1)$ th coordinate of all the $n + 2$ vectors is zero, then we can forget it, and, using the induction assumption, find a nontrivial linear combination of the given $n + 2$ vectors

such that the resulting vector is zero. It will remain zero when we add back the last coordinate. Let a_k be the $(n + 1)$ th coordinate of the vector \mathbf{x}_k . Now, if the $(n + 1)$ th coordinate of some vector \mathbf{x}_i is nonzero, then replace our set of vectors with $\mathbf{x}'_1, \mathbf{x}'_2, \dots, \mathbf{x}'_{n+1}, \mathbf{x}'_{n+2}$, where $\mathbf{x}'_j = \mathbf{x}_j - (a_j/a_i)\mathbf{x}_i$, $\mathbf{x}'_i = 0$. Then by the induction assumption for the vectors $\mathbf{x}'_1, \dots, \mathbf{x}'_{i-1}, \mathbf{x}'_{i+1}, \dots, \mathbf{x}'_{n+2}$, we can find coefficients c_1, \dots, c_{n+1} not all vanishing such that

$$\begin{aligned} 0 &= c_1\mathbf{x}'_1 + \dots + c_{i-1}\mathbf{x}'_{i-1} + c_i\mathbf{x}'_{i+1} + \dots + c_{n+1}\mathbf{x}'_{n+2} = c_1(\mathbf{x}_1 - (a_1/a_i)\mathbf{x}_i) + \dots + c_{n+1}(\mathbf{x}_{n+2} - (a_{n+2}/a_i)\mathbf{x}_i) = \\ &= c_1\mathbf{x}_1 + \dots + c_{i-1}\mathbf{x}_{i-1} + (-c_1(a_1/a_i) - c_2(a_2/a_i) - \dots - c_{i-1}(a_{i-1}/a_i) - c_i(a_{i+1}/a_i) - \dots - c_{n+1}(a_{n+2}/a_i))\mathbf{x}_i + \\ &\quad + c_i\mathbf{x}_{i+1} + \dots + c_{n+1}\mathbf{x}_{n+2}. \end{aligned}$$

Hence, we presented a nontrivial linear combination of the initial vectors resulting into a zero vector. We get a contradiction.

Problem 24. Prove that if $\mathbf{x}_1, \dots, \mathbf{x}_n$ form an arbitrary system of linearly independent vectors in \mathbb{R}^n , then any vector $\mathbf{x} \in \mathbb{R}^n$ can be represented as $\mathbf{x} = c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n$, where c_1, \dots, c_n are real numbers. (The system $\mathbf{x}_1, \dots, \mathbf{x}_n$ is called a *basis* of the space and the expression $c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n$ is called *linear combination* of the vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$ with *coefficients* c_1, \dots, c_n . In these terms, any vector $\mathbf{x} \in \mathbb{R}^n$ can be represented as a linear combination of the vectors of the basis.)

Solution. On the contrary, suppose that there exists a vector \mathbf{x} which cannot be represented as a linear combination of vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$. Then the system of vectors $\{\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{x}\}$ will be linearly independent: indeed, let $c_1\mathbf{x}_1 + \dots + c_n\mathbf{x}_n + c\mathbf{x} = 0$, then either $c = 0$ and all c_i vanish since \mathbf{x}_i , $i = 1, 2, \dots, n$, are linearly independent, or $c \neq 0$, but then $\mathbf{x} = (c_1/c)\mathbf{x}_1 + \dots + (c_n/c)\mathbf{x}_n$, which contradicts our assumption. But the set $\{\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{x}\}$ contains $n + 1$ vectors, and we get a contradiction with the previous problem.

Let p be a prime number. Let \mathbb{Z}_p be the set of congruences modulo p . The space \mathbb{Z}_p^n , similarly to \mathbb{R}^n , is just the set of all the sequences of numbers from \mathbb{Z}_p . The operations of the sum of “vectors” $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^n$ and of their product with elements of \mathbb{Z}_p is done, as usual, coordinate by coordinate, but, this time, every coordinate is taken modulo p .

The notions of linear independence and of a basis for \mathbb{Z}_p^n are defined in the same way as for \mathbb{R}^n . However, here all the numbers c_i are elements of \mathbb{Z}_p — not \mathbb{R} , — and the equality to zero is understood as the equality to zero modulo p .

Problem 25. Prove that the maximum number of linearly independent vectors in \mathbb{Z}_p^n equals n and that any maximal system forms a basis.

Solution. The proof is the same as the proof of two previous problems. Indeed, every element can be seen as a sequence of residues modulo p , the coefficients are not real numbers but residues modulo p , and the only difference is that by $1/a$ we now mean the inverse element modulo p .

Problem 26. Let $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ be an arbitrary independent set of vertices of the graph $G(n, 3, 1)$. Prove that the vectors $\mathbf{x}_1, \dots, \mathbf{x}_t$ are linearly independent in \mathbb{Z}_2^n and thus $\alpha(G(n, 3, 1)) \leq n$, which is only by an “epsilon” weaker than the result of Problem 12!

Solution. On the contrary, suppose that there exist coefficients $c_1, \dots, c_t \in \mathbb{Z}_2$, not all vanishing, such that

$$c_1 \mathbf{x}_1 + \dots + c_t \mathbf{x}_t = 0.$$

Without loss of generality we may assume that $c_1 \neq 0$. Let us take the scalar product of the both hands of this equality by \mathbf{x}_1 . Note that if we take the scalar product of two vectors, each has three nonzero coordinates equal to 1, then it equals 3, if the vectors are equal, and 0, 1, or 2 in the other cases. Since we take vectors from an independent subset of the graph $G(n, 3, 1)$, the scalar product cannot equal 1. If we take the obtained equality modulo two, then the first summand of the left hand side will be equal to 1 (since $3 \equiv 1 \pmod{2}$), and all the others will be equal to 0, but on the right hand side we have 0. We get a contradiction.

Let $F \in \{\mathbb{R}, \mathbb{Z}_p\}$. Let x_1, \dots, x_n be “variables”. By a *monomial* depending on these n variables we mean an expression of the form $x_1^{a_1} \dots x_n^{a_n}$, where a_1, \dots, a_n are some non-negative integers. A *polynomial* is an arbitrary linear combination of monomials. More precisely, a polynomial P belongs to $F[x_1, \dots, x_n]$, if its coefficients are from F . Polynomials are added and multiplied according to the usual rules. Also if $P \in F[x_1, \dots, x_n]$, then it can be multiplied by any element of F . In any case, the rules of summation and multiplication of the coefficients of polynomials are defined by the rules of summation and multiplication in the set F . The *degree* of a monomial is the sum of the degrees of its variables. The degree of a polynomial is the maximum of the degrees of its monomials. A polynomial $P \in F[x_1, \dots, x_n]$ *equals zero*, if all its coefficients are equal to zero in F . Polynomials $P_1 \in F[x_1, \dots, x_n], \dots, P_t \in F[x_1, \dots, x_n]$ are *linearly independent* over F , if $c_1 P_1 + \dots + c_t P_t = 0$ only in the case when all the numbers $c_1 \in F, \dots, c_t \in F$ are equal to zero in F . It is obvious that any polynomial is generated by the *basis* consisting of its monomials.

Problem 27. Prove that if some polynomials are linearly independent over their F , then their number does not exceed the number of monomials in a basis, which generates all these polynomials.

Solution. Every polynomial is a linear combination of basis monomials, and suppose that there exist n basis monomials. Then every polynomial corresponds to a unique sequence of n coefficients from F . In other words, any polynomial can be viewed as a vector in F^n . Then by Problems 24 and 25, the maximal possible number of linearly independent vectors in this space is n , which gives the required bound.

Problem 28. Let $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ be an arbitrary independent set of vertices of the graph $G(n, 5, 2)$. Let polynomials $P_1 \in \mathbb{Z}_3[y_1, \dots, y_n], P_2 \in \mathbb{Z}_3[y_1, \dots, y_n], \dots, P_t \in \mathbb{Z}_3[y_1, \dots, y_n]$ be given by formulae

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1), \quad i = 1, \dots, t.$$

For example, if $\mathbf{x}_1 = (1, 1, 1, 1, 1, 0, \dots, 0)$, $\mathbf{x}_2 = (0, \dots, 0, 1, 1, 1, 1, 1)$, then

$$P_1(y_1, \dots, y_n) = (y_1 + y_2 + y_3 + y_4 + y_5)(y_1 + y_2 + y_3 + y_4 + y_5 - 1) = y_1^2 + \dots + y_5^2 + 2y_1 y_2 + \dots + 2y_4 y_5 - y_1 - \dots - y_5,$$

$$\begin{aligned} P_2(y_1, \dots, y_n) &= (y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n)(y_{n-4} + y_{n-3} + y_{n-2} + y_{n-1} + y_n - 1) = \\ &= y_{n-4}^2 + \dots + y_n^2 + 2y_{n-4} y_{n-3} + \dots + 2y_{n-1} y_n - y_{n-4} - \dots - y_n. \end{aligned}$$

Prove that the polynomials P_1, \dots, P_t are linearly independent over \mathbb{Z}_3 and therefore $\alpha(G(n, 5, 2)) \leq C_n^2 + 2C_n^1$.

Solution. As we did in Problem 26, assume the contrary: suppose that there exists a linear dependency, which has a nonzero coefficient at some P_i . Let us substitute \mathbf{y} by \mathbf{x}_i . Then the right hand side will remain zero, and all P_j , $j \neq i$, will vanish in the left hand side. Indeed, the scalar product $(\mathbf{x}_i, \mathbf{y})$ can equal 0, 1, 3, or 4, and then the polynomial vanishes modulo 3. The scalar product cannot be equal to two since we started from an independent subset of $G(n, 5, 2)$. It can equal 5 in the only case when two vectors coincides, which gives us the only nonzero summand, and we get a contradiction.

Now let us count the number of possible monomials. We have products of form $y_i y_j$, squares y_i^2 , and linear terms y_i . This gives us $C_n^2 + 2C_n^1$ monomials, which implies the required bound for $\alpha(G(n, 5, 2))$.

Problem 29. Assume that in the conditions of the previous problem the polynomials P_i are substituted by P'_i according to the following rule: every monomial of the form y_i^2 is changed by y_i , and after that monomials of the same form are added. Prove that the polynomials P'_1, \dots, P'_t corresponding to the vectors from an independent set of vertices W of the graph $G(n, 5, 2)$ are also linearly independent over \mathbb{Z}_3 , similarly to the initial polynomials P_1, \dots, P_t . Derive from this fact the bound $\alpha(G(n, 5, 2)) \leq C_n^2$ and compare it with the bound from the problem 15.

Solution. Note that in the previous solution, when we used linear dependencies, we used only the values of the polynomials at the points having coordinates equal either to 0 or to 1. Clearly, the values of the new polynomials will coincide with the values of the old polynomials in these points, hence, the same proof can be applied.

Now note that, if we open the brackets and perform the required substitutions, every polynomial will contain only pairwise products of variables, hence, the basis of the corresponding space contains at most C_n^2 monomials, which gives the required bound.

Now let us compare the bound with the bound of Problem 15. We get that $\alpha(G(n, 5, 2)) \sim \frac{1}{2}n^2$.

Problem 30. Derive from the result of the previous problem a lower bound for $\chi(\mathbb{R}^n)$, which considerably improves the bound from Problem 12. Ensure yourselves, however, that, in view of Problem 19, substantial further advances based on the graph $G(n, 5, 2)$ cannot be done.

Solution. Let us apply the homothety with the coefficient $1/\sqrt{6}$ to the graph $G(n, 5, 2)$ and then apply Problem 11. We obtain that

$$\chi(\mathbb{R}^n) \geq \frac{|V|}{\alpha(G(n, 5, 2))} \geq C_n^5 / C_n^2 = 60n^3 + O(n^2).$$

On the other hand, using this graph, we cannot bound the chromatic number of order greater than C_n^3 .

Problem 31. Let $W = \{\mathbf{x}_1, \dots, \mathbf{x}_t\}$ be an arbitrary independent set of vertices of the graph $G(n, 9, 4)$. Let polynomials $P_1 \in \mathbb{Z}_5[y_1, \dots, y_n]$, $P_2 \in \mathbb{Z}_5[y_1, \dots, y_n]$, \dots , $P_t \in \mathbb{Z}_5[y_1, \dots, y_n]$ be given by the formulae

$$P_i(\mathbf{y}) = P_i(y_1, \dots, y_n) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1)((\mathbf{x}_i, \mathbf{y}) - 2)((\mathbf{x}_i, \mathbf{y}) - 3), \quad i = 1, \dots, t.$$

Prove that the polynomials P_1, \dots, P_t are linearly independent over \mathbb{Z}_5 .

Solution. As we did in Problem 28, we take a nontrivial linear combination resulting into zero vector. Then we find a nonzero term in this linear combination, substitute the corresponding vector x_i instead of y into the whole linear combination and obtain that on one hand we have identically zero, while on the other hand we have exactly one nonzero term corresponding to x_i . We get a contradiction.

Problem 32. Which upper bound for $\alpha(G(n, 9, 4))$ follows from the previous problem?

Solution. We need to count the number of monomials necessary to generate all the vectors P_1, P_2, \dots, P_t . It suffices to take all the monomials of the form

$$y_i y_j y_k y_l, y_i^2 y_j y_k, y_i y_j y_k, y_i^3 y_j, y_i^2 y_j^2, y_i^2 y_j, y_i y_j, y_i^4, y_i^3, y_i^2, y_i, \text{const.}$$

The number of such monomials equals $C_n^4 + 4C_n^3 + 6C_n^2 + 4C_n^1 + 1$, hence, $\alpha(G(n, 9, 4))$ is bounded by the same value.

Problem 33. Let in the conditions of Problem 31 the polynomials P_i be replaced by some P'_i according to the following rule: in them, every monomial, which appears after opening the brackets and summing similar monomials, has of course the form $y_1^{a_1} \cdot \dots \cdot y_n^{a_n}$; if among the numbers a_i , one has some numbers greater than or equal to 2, then we replace all of them by 1s and sum up similar monomials. For example, the monomial $y_1^2 y_2^2$ is transformed to $y_1 y_2$ and the same is true for the monomials $y_1^2 y_2, y_1 y_2^2$, etc. Prove that the polynomials P'_1, \dots, P'_t corresponding to the vectors from an independent set W of the graph $G(n, 9, 4)$ are also linearly independent over \mathbb{Z}_5 , just as it was with the initial polynomials P_1, \dots, P_t . Derive from this fact the bound $\alpha(G(n, 9, 4)) \leq C_n^4 + C_n^3 + C_n^2 + C_n^1 + C_n^0$ and compare it with the bound from Problem 15.

Solution. To prove linear independency in Problem 31, we substituted 0 and 1 instead of y_i into some inequalities. In the both cases, the value of the polynomial will not change during this operation. Hence, the proof remains valid, and we get a new estimate on the number of such polynomials: it is bounded by the number of generating monomials, which is equal to $C_n^4 + C_n^3 + C_n^2 + C_n^1 + C_n^0$. Asymptotically this coincides with the bound from Problem 15.

Problem 34. Derive from the result of the previous problem a lower bound for $\chi(\mathbb{R}^n)$, which considerably refines the bound from Problem 30. Ensure yourselves, however, that, in view of Problem 19, substantial further advances based on the graph $G(n, 9, 4)$ cannot be done.

Solution. In the same way as we did in Problem 30, we get $\chi(\mathbb{R}^n) \geq C_n^9 / C_n^4 = \frac{4!}{9!} n^5 + O(n^4)$. On the other hand, if we apply Problem 19, we get a bound not better than C_n^5 , which asymptotically gives the same order of magnitude.

Problem 35. Let r and s be such that $r - s = p$, where p is a prime number and $r - 2p < 0$. Prove that $\alpha(G(n, r, s)) \leq \sum_{k=0}^{p-1} C_n^k$. Compare this bound with the bound from Problem 15.

Solution. Fix any independent subset $W = \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ and consider polynomials $P_i \in \mathbb{Z}_p[y_1, \dots, y_n]$ given by formulae

$$P_i(\mathbf{y}) = (\mathbf{x}_i, \mathbf{y})((\mathbf{x}_i, \mathbf{y}) - 1) \dots ((\mathbf{x}_i, \mathbf{y}) - (p - 1)).$$

As we did above, we prove that they are linearly independent and that their number is bounded from above by the required value. On the other hand, in Problem 15 the same value was bounded from below, which gives asymptotically the same order of magnitude: $\alpha(G(n, r, s)) \sim \frac{1}{(p-1)!} n^{p-1}$.

Problem 36*. Explore lower bounds for the quantity $\chi(\mathbb{R}^n)$, which follow from the results of the previous problem. How do these bounds correlate with the bounds from Problem 19?

Solution. We use the same notation as in the previous problem. We have

$$\chi(\mathbb{R}^n) \geq \chi(G(n, r, s)) \geq \frac{|V(n, r)|}{\alpha(G(n, r, s))} \geq \frac{C_n^r}{\sum_{k=0}^{p-1} C_n^k} = (1 + o(1)) \left(\frac{C_n^r}{C_n^{r-s-1}} \right),$$

i.e., there exists a constant c_1 such that $\chi(G(n, r, s)) \geq c_1 n^{s+1}$, but, on the other hand, we know by Problem 19 that $\chi(G(n, r, s)) \leq c_2 n^{s+1}$ for some other constant c_2 . This means that we know the order of growth of the chromatic number for the graphs $G(n, r, s)$ with $r - s = p$, p prime, $r - 2p < 0$.

3 Problems after the intermediate finish

Before the intermediate finish we have seen how important are the independence numbers of graphs for obtaining lower bounds on the chromatic number of a space. Moreover, we considered different sequences of distance graphs — the sequences $\{G(n, r, s)\}_{n=1}^{\infty}$ with given r and s . It is interesting to understand how will be changed the independence numbers, if, instead of the graphs $G(n, r, s)$, we take their spanning subgraphs, i.e., if we take the same sets of vertices and partially remove the edges. It seems to be evident that the independence numbers must become substantially larger, provided we remove many edges. However, surprisingly, sometimes this is true, but sometimes this is completely wrong! In order to obtain the corresponding results, let us learn some random graphs and some probability theory.

3.1 The random Erdős–Rényi graph and some of its probabilistic characteristics

Let $V_n = \{1, \dots, n\}$ be a set of vertices. In principle, one can construct on this set C_n^2 edges, if we do not allow multiple edges, loops and orientation. Let us each of these C_n^2 potential edges draw with *probability* $p \in [0, 1]$, which is the same for every edge. Different edges appear independently. Let $G = (V_n, E)$ be a graph which can appear as a result of the just-described probabilistic procedure. Denote the probability of its appearance by $\mathbb{P}(G)$. Clearly it is equal to $p^{|E|}(1-p)^{C_n^2-|E|}$. If A is a property of a graph, then its probability — $\mathbb{P}(A)$ — is the sum over all the graphs G , which have property A , of the probabilities of these graphs.

Denote by Ω_n the set of all graphs on the vertices V_n . Any function X defined on Ω_n and taking real values is called *random variable*. For example, the number of triangles in a graph or its number of connected components, or its independence number are random variables. Here you must understand that the variables are random only due to the fact that a priori we do not know which graph will (randomly) come to us. When a graph is already born the value of X is determined uniquely!

Any random variable has some “mean value” — the so-called (*mathematical*) *expectation*. The expectation of a variable X is the number $\mathbb{M}X$ defined by the formula $\mathbb{M}X = \sum_{G \in \Omega_n} X(G)\mathbb{P}(G)$. We just sum up the values of the function X on all the graphs multiplied by the probabilities of these graphs. Of course this is some weighted average (weights are probabilities) — a kind of the mass centre). Let us learn to calculate expectations and apply the obtained results to the study of the properties of random graphs.

Problem 37. Prove that if a random variable is just a constant c , then $\mathbb{M}c = c$.

Solution. What is the average value of the constant? Obviously, it is constant itself.

Problem 38. Let X_1, X_2 be random variables and c_1, c_2 be some fixed numbers. Certainly $c_1X_1 + c_2X_2$ is also a random variable. Prove that its expectation equals $c_1\mathbb{M}X_1 + c_2\mathbb{M}X_2$. This property is called *linearity of expectation*.

Solution.

$$\begin{aligned}\mathbb{M}(c_1X_1 + c_2X_2) &= \sum_G (c_1X_1(G)P(G) + c_2X_2(G)P(G)) = c_1 \sum_G X_1(G)P(G) + c_2 \sum_G X_2(G)P(G) = \\ &= c_1\mathbb{M}X_1 + c_2\mathbb{M}X_2.\end{aligned}$$

Problem 39. Using linearity of expectation find expectations of a) the number of triangles in the random graph; b) the number of connected components of the random graph, each of which is a cycle on k vertices (k is a fixed given number); c) the number of independent sets in the random graph, each of which has cardinality k (k is a fixed given number).

Solution. a) There are C_n^3 choices of three vertices, and each of them will give a triangle with probability p^3 . From linearity of expectation, it follows that $\mathbb{M}X = C_n^3 p^3$, where X is the required random variable.

b) There are C_n^k choices of k vertices in the given graph, and each of them can form $(k-1)!/2$ cycles (here we count the order of the vertices in the cycle). The probability of such an ordered set to become a connected component being a cycle equals $p^k(1-p)^{(C_k^2-k)+k(n-k)}$, since there should be exactly k edges between the vertices of this cycle and since there should be no edges between this subgraph and the other vertices of the graph. It follows from linearity that

$$\mathbb{M}X = C_n^k (k-1)! p^k (1-p)^{(C_k^2-k)+k(n-k)},$$

where X is the required random variable.

c) There are C_n^k choices of k vertices, and each of them is independent with probability $(1-p)^{C_k^2}$. Hence, $\mathbb{M}X = C_n^k (1-p)^{C_k^2}$, where X is the required random variable.

Problem 40. Prove *Markov's inequality*: if X is a random variable taking non-negative values and a is a positive number, then $\mathbb{P}(X \geq a) \leq \frac{\mathbb{M}X}{a}$.

Solution.

$$\mathbb{M}X = \sum_z zP(X=z) = \sum_{z \geq a} zP(X=z) + \sum_{z < a} zP(X=z) \geq \sum_{z \geq a} aP(X=z) = aP(X \geq a).$$

This is equivalent to Markov's inequality.

Problem 41. Using Markov's inequality prove that if $p = \frac{1}{2}$, then $\mathbb{P}(\alpha(G) \leq 2 \log_2 n) \rightarrow 1$ as $n \rightarrow \infty$ (it is used to say that "almost surely $\alpha(G) \leq 2 \log_2 n$ ").

Solution. Introduce the random variable X_k which is equal to the number of independent sets of vertices of size k . Then from problems 39 and 40 can be seen that

$$P(X_k \geq 1) \leq \mathbb{M}X_k = C_n^k \left(\frac{1}{2}\right)^{\frac{k(k-1)}{2}} \leq \frac{n^k}{k!} \left(\frac{1}{2}\right)^{\frac{k(k-1)}{2}} \leq \frac{n^k e^k}{k^k} \left(\frac{1}{2}\right)^{\frac{k(k-1)}{2}} = \left(\frac{ne2^{\frac{k-1}{2}}}{k}\right)^k$$

It is easy to see that for $k = 2\log_2 n$ this value tends to 0. So, with probability tending to 1, an independent set of vertices of size k in the graph does not exist.

Note that actually for $p = \frac{1}{2}$ almost surely $\alpha(G) \geq (2 - \varepsilon)\log_2 n$ for any given arbitrarily small $\varepsilon > 0$. More precisely, — and we shall use it later, — the following theorem holds.

Theorem 1. *For any $\varepsilon > 0$ and large enough n the inequality*

$$\mathbb{P}(\alpha(G) \geq (2 - \varepsilon)\log_2 n) > 1 - 2^{-n}$$

holds.

Thus, for $p = \frac{1}{2}$, almost surely the independence number is approximately $2\log_2 n$. In other words, what's happening? We take the complete graph on n vertices and we delete some of its edges, each with probability $\frac{1}{2}$. A typical graph, which appears as a result of this procedure, has about $\frac{C_n^2}{2}$ edges — two times less than the complete graph has. And the independence number of a typical graph is in a logarithm times greater than the independence number of the initial graph (the independence number of the complete graph is of course 1). OK, the number of edges is two times smaller and the independence number increases: quite natural. It turns out that for some $G(n, r, s)$ when deleting their edges randomly, we get the same “expected” result (the independence number becomes approximately log times bigger). But the miracle is that this happens not everytime! For many $G(n, r, s)$ the independence number does not change at all! Below, we will study together examples of both situations.

3.2 Random subgraphs of the graph $G(n, 3, 0)$

Let $G_{1/2}(n, 3, 0)$ be a random subgraph of the graph $G(n, 3, 0)$ obtained by deleting mutually independently some edges of the graph $G(n, 3, 0)$, each with probability $1/2$.

Problem 42. If you solved Problem 16, then just derive from it that $\alpha(G(n, 3, 0)) = C_{n-1}^2$. Otherwise, try to solve this particular case of that problem.

Solution. See the solution of Problem 16.

In a series of problems below, we will prove that almost surely $\alpha(G_{1/2}(n, 3, 0)) \leq C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. This is exactly what we mentioned above speaking about a surprising phenomenon: there is no growth in log times; if there is some growth, then it is only in such a number of times that itself tends to 1 as $n \rightarrow \infty$! One can prove even stronger facts, but this is very difficult, and we do not want to do it here: we just want to see the essence!

In what follows, we will for conciseness omit integer parts around quantities which must be integer. For example, writing $C_{\log_2 n}^k$ means, depending on context, that actually we take an upper or a lower integer part of the number $\log_2 n$. None of the computations will become false after this roughening.

Problem 43. Put $k = C_{n-1}^2 \left(1 + \frac{1}{\ln n}\right)$. Assume that k is integer (cf. a remark before the problem). Let $A \subset V(n, 3)$ be an arbitrary set of vertices of the graph $G(n, 3, 0)$ having cardinality k . Denote by $r(A)$ the number of edges of the graph $G(n, 3, 0)$, whose both ends are in A . Since $|A| = k > \alpha(G(n, 3, 0))$, it is clear that $r(A) > 0$. Let X_k be the random variable equal to the number of independent sets of size k in a graph $G_{1/2}(n, 3, 0)$. Prove that

$$\mathbb{M}X_k = \sum_{A \subset V(n,3): |A|=k} \left(\frac{1}{2}\right)^{r(A)}. \quad (2)$$

Solution. Let $t = C_{|V|}^k$. Let each subgraph on k vertices correspond to the random variable equal to 1 if the corresponding subgraph on k vertices became independent, and 0 otherwise. Let these random variables be Y_1, Y_2, \dots, Y_t . Then $X_k = Y_1 + Y_2 + \dots + Y_t$. But the expectation of Y_i is obviously equal to $\frac{1}{2^{|Y_i|}}$, where $|Y_i|$ is the number of edges in corresponding to the i -th random variable subgraph. It immediately follows from the linearity of the expectation that

$$\mathbb{M}X_k = \sum_{A \subset V(n,3): |A|=k} \left(\frac{1}{2}\right)^{r(A)}.$$

Problem 44. Prove that our aim will be attained, if we will prove that $\mathbb{M}X_k \rightarrow 0$ as $n \rightarrow \infty$.

Solution. We want to prove that with high probability there are no independent sets of size k , i.e., $P(X_k = 0) \rightarrow 1$ as $n \rightarrow \infty$. But it is clear that $P(X_k = 0) + P(X_k \geq 1) = 1$. Then we need to prove that $P(X_k \geq 1) \rightarrow 0$. But Markov's inequality implies that $P(X_k \geq 1) \leq \mathbb{M}X_k$. It remains to show that $\mathbb{M}X_k \rightarrow 0$ as $n \rightarrow \infty$.

Clearly we have to learn bounding *from below* the quantity $r(A)$. For each A , denote by $B = B(A)$ any (chosen for everytime) subset of A , which is independent in $G(n, 3, 0)$ and has the maximum cardinality among all analogous subsets of the set A .

Problem 45. Let $A \subset V(n, 3)$, $|A| = k$. Let $B = B(A)$. Note that $k \approx \frac{n^2}{2}$. Assume that $|B|$ is substantially smaller than k : for example, let $|B| < n^{1.9}$ (here the strange number 1.9 is taken almost arbitrarily; important is that it is strictly smaller than 2). Prove that for large enough n the inequality $r(A) \geq \frac{k^2}{3|B|}$ holds (being more careful one can replace 3 in the denominator by "almost" 2, but this does not matter).

Solution. First, let us prove the following lemma:

Lemma. Any subgraph $\tilde{\mathcal{G}}$ of graph \mathcal{G} , with mn vertices, and with $\alpha(\mathcal{G}) \leq n$, contains not less than $\frac{m^2n}{2} - \frac{mn}{2}$ edges ($m \in N$).

Proof.

Let us prove this by induction on m .

Base. $m = 1$.

$\frac{m^2n}{2} - \frac{mn}{2} = 0$. It is obvious.

The induction step. $m \rightarrow m + 1$.

Consider a maximal independent set in the subgraph $\tilde{\mathcal{G}}$. If there is more than one such set, consider any of them. It is obvious that the independence number of the subgraph does not exceed the independence number of the initial graph. Therefore, $\alpha(\tilde{\mathcal{G}}) \leq n$. So, there is at least 1 edge from each of the remaining $(m+1)nk$ vertices to this set, otherwise we could increase the independent set, but by the assumption it is maximum. So, we have not less than $(m+1)n-k$ edges. And no one from this edges is lying in the subgraph on remaining $(m+1)n-k$ vertices. But $(m+1)n-k \geq mn$, and so in the subgraph on remaining $(m+1)n-k$ vertices there are not less than $\frac{m^2n}{2} - \frac{mn}{2}$ edges (by the induction hypothesis). Then, there are not less than

$$\frac{m^2n}{2} - \frac{mn}{2} + (m+1)n - k \geq \frac{m^2n}{2} - \frac{mn}{2} + mn = \frac{m^2n + 2mn + n}{2} - \frac{n}{2} - \frac{mn}{2} = \frac{(m+1)^2n}{2} - \frac{(m+1)n}{2}$$

edges. The induction step is proved.

So it follows from lemma that

$$r(A) \geq \frac{\left[\frac{|A|}{|B|}\right]^2 |B|}{2} - \frac{\left[\frac{|A|}{|B|}\right] |B|}{2} = \frac{\left[\frac{|A|}{|B|}\right] |B|}{2} \left(\left[\frac{|A|}{|B|}\right] - 1 \right) \geq \frac{k - |B|}{2} \left(\frac{k}{|B|} - 2 \right) = (1 + o(1)) \frac{k^2}{2|B|}.$$

Problem 46. Let $A \subset V(n, 3)$, $|A| = k$. Let $B = B(A)$. Let $|B| > 9n$ or, even better (in addition to the previous problem), $|B| \geq n^{1.9}$. Prove that $r(A) \geq (|B| - 9n)(|A| - |B|)$.

Solution. Let us estimate the number of edges of the graph $G(n, 3, 0)$ in A . Recall that B is the *maximum* independent set of vertices of graph $G(n, 3, 0)$ in A . Because of this, for any vertex $\mathbf{x} \in A \setminus B$ there is a vertex $\mathbf{y} \in B$ such that $\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0)$. Let us show that the vertex \mathbf{y} is not unique with this property. Indeed, the vertices \mathbf{x} and \mathbf{y} are connected by an edge, and so they do not intersect as 3-element sets. Let us estimate how many vertices $\mathbf{z} \in B$ which **aren't connected** with \mathbf{x} can exist. On the one hand, they must intersect with \mathbf{x} by at least one element. On the other hand, they must intersect with \mathbf{y} too, cause B is an independent set. But \mathbf{x} and \mathbf{y} haven't any intersection. So, there are not more than $3^2 n^{3-2} = 3n$ such vertices \mathbf{z} in the current situation $|B| > n^{3-1.1}$. Consequently, the number of vertices of B , which is connected to the given vertex $\mathbf{x} \in A \setminus B$, is not less than $|B| - 9n$. Thus,

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0) : \mathbf{x}, \mathbf{y} \in A\}| \geq (|A| - |B|)(|B| - 9n) \geq \frac{C_{n-1}^2}{\ln n} n^{1.9} = (1 + o(1)) \frac{n^{3.9}}{2 \ln n},$$

(last transitions are possible, provided that $|B| \geq n^{1.9}$. But for inequality $r(A) \geq (|B| - 9n)(|A| - |B|)$ it suffices that $|B| > 9n$).

Problem 47. Decompose sum (2) into two parts: in the first part, only those A will be taken, for which $|B| < n^{1.9}$; in the second part, all the other sets A will be considered. To the summands in both parts apply the bounds from the corresponding problems and make it sure that the whole sum (2) does really tend to zero, which means that we are done!

How can we change the threshold $n^{1.9}$ in order to still get the same result?

Solution. It is sufficient to verify that in the random graph $\mathcal{G}(G(n, 3, 0), 1/2)$ there is an independent set of vertices of size k with probability tending to zero. It is known that this probability is not greater than

$$\sum_{ACV(n,r), |A|=k} \mathbb{P}(A \text{ is independent in } \mathcal{G}(G(n, 3, 0), 1/2)) = \sum_{ACV(n,r), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0) : \mathbf{x}, \mathbf{y} \in A\}|}.$$

Let us show that the last sum tends to zero too.

There are two options: either for the A holds $|B| \leq n^{1.9} = o(C_{n-1}^2)$ (A is set of the first type), or for the A holds $|B| > n^{1.9}$ (A is set of the second type).

Let us select terms corresponding to the sets A of the first type in the sum above. This sum does not exceed

$$C_{C_n^3}^k 2^{-(1+o(1))\frac{k^2}{2n^{1.9}}} < 3^k n^{3k} 2^{-(1+o(1))\frac{k^2}{2n^{1.9}}} = 3^k 2^{(1+o(1))3\frac{n^2}{2} \log_2 n} 2^{-(1+o(1))\frac{n^4}{2(2)^2 n^{1.9}}} \rightarrow 0.$$

Here we use the fact that r is constant and

$$n^2 \log_2 n = o(n^{2.1}).$$

Now let A be a set of the second type. Using Problem 45,

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 0) : \mathbf{x}, \mathbf{y} \in A\}| \geq \frac{n^{3.9}}{2 \ln n},$$

So, the sum of terms corresponding to the sets A of the second type (in the sum above) does not exceed

$$C_{C_n^3}^k 2^{-(1+o(1))\frac{n^{3.9}}{2 \ln n}} < 3^k n^{3k} 2^{-(1+o(1))\frac{n^{3.9}}{2 \ln n}} = 3^k 2^{(1+o(1))3\frac{n^2}{2} \log_2 n} 2^{-(1+o(1))\frac{n^{3.9}}{2 \ln n}} \rightarrow 0.$$

The result follows.

3.3 Random subgraphs of the graph $G(n, 3, 1)$

Let $G_{1/2}(n, 3, 1)$ be a random subgraph of the graph $G(n, 3, 1)$ obtained by deleting mutually independently some edges of the graph $G(n, 3, 1)$, each with probability $1/2$. It seems that everything is the same as with the graphs $G(n, 3, 0)$. This is completely wrong!

Recall that $\alpha(G(n, 3, 1)) \approx n$ (see Problem 12).

Problem 48*. Write down an analog of inequality (2) and prove an analog of the bound from Problem 45. Ensure yourselves eventually that there exists a $c > 0$, with which almost asurely $\alpha(G_{1/2}(n, 3, 1)) \leq cn \log_2 n$.

Solution. We explained in detail how to prove the bound in Problem 45, so we will not re-do it. We assume that the quantity of edges in the set A of cardinality k is not less than $(1 + o(1))\frac{k^2}{2n}$. If somebody does not believe this, he should repeat inference from Problem 45 by himself.

Let $X_k = X_k(\mathcal{G}(G(n, 3, 1), 1/2))$ be a function of random graph which is equal to quantity of independent sets with k vertices in the graph (i. e., of sets such that their elements are not mutually connected by edges). Let us estimate its expectation and use Markov's inequality:

$$\begin{aligned} \mathbb{E}X_k &= \sum_{A \subset V(n, 3), |A|=k} \mathbb{P}(A \text{ is an independent set in } \mathcal{G}(G(n, 3, 1), 1/2)) = \\ &= \sum_{A \subset V(n, 3), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 1) : \mathbf{x}, \mathbf{y} \in A\}|}, \end{aligned}$$

so in exponential factor there is a quantity of edges of subgraph of graph $G(n, 3, 1)$, which is induced by the concrete set of vertices A . As we remember

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 1) : \mathbf{x}, \mathbf{y} \in A\}| > (1 + o(1))\frac{k^2}{2\alpha(G(n, 3, 1))} = (1 + o(1))\frac{k^2}{2n}.$$

So, cause of this bound, we obtain that

$$\mathbb{E}X_k < \sum_{A \subset V(n,3), |A|=k} 2^{-(1+o(1))\frac{k^2}{2n}} = C_{C_3^n}^k 2^{-(1+o(1))\frac{k^2}{2n}}.$$

It is well known that $C_a^b \leq \left(\frac{ea}{b}\right)^b$, where e is a base of the natural logarithm. So,

$$\mathbb{E}X_k < \left(\frac{n^3}{k}\right)^k 2^{-(1+o(1))\frac{k^2}{2n}} = 2^{3k \log_2 n - k \log_2 k - (1+o(1))\frac{k^2}{2n}}.$$

I.e., there exists a function $k = k(n)$, which is asymptotically equal to $4n \log_2 n$ and such that for this subsequence, $\mathbb{E}X_k \rightarrow 0$ where $n \rightarrow \infty$. The theorem follows from this statement and Markov's inequality:

$$\mathbb{P}(\alpha(\mathcal{G}(G(n, 3, 1), 1/2)) \leq 4(1 + o(1))n \log_2 n) = \mathbb{P}(X_k = 0) \geq 1 - \mathbb{E}X_k \rightarrow 1, \quad n \rightarrow \infty.$$

QED.

Problem 49. Prove that in the graph $G(n, 3, 1)$, there exist approximately $\frac{n}{2}$ complete subgraphs, each having about $\frac{n}{4}$ vertices, such that every two of them are not connected by an edge.

Solution. For convenience let us assume that n is divisible by 4. Let $m = \frac{n}{2}$. We divide \mathcal{R}_n into parts $R_1 = \mathcal{R}_m$ and $R_2 = \mathcal{R}_n \setminus R_1$. First, we describe the construction of one clique (independent subset) Q_1 . For this, we take disjoint pairs $\{1, 2\}, \{3, 4\}, \{5, 6\}, \dots, \{m-1, m\}$ (cause of m is even) in R_1 . We add element $m+1 \in R_2$ to each of these pairs. This is the desired clique. It contains $\frac{m}{2} = \frac{n}{4}$ vertices. We similarly construct $n-m-1$ cliques Q_2, \dots, Q_{n-m} by adding to all the pairs in R_1 element $m+2 \in R_2$, element $m+3 \in R_2$, etc. Obviously, there are no edges between \mathbf{x}, \mathbf{y} for any $i, j, i \neq j, \mathbf{x}$ from Q_i, \mathbf{y} from Q_j : these triples either do not intersect at all or intersect by some pair of R_1 .

Hence, we have constructed $\frac{n}{2}$ cliques, each containing $\frac{n}{4}$ elements.

Problem 50. With the help of the previous problem and Theorem 1 prove that for every $\varepsilon > 0$, almost surely $\alpha(G_{1/2}(n, 3, 1)) \geq (1 - \varepsilon)n \log_2 n$.

Solution. As we know, a random graph $\mathcal{G}(G(n, 3, 1), 1/2)$ is obtained from the graph $G(n, 3, 1)$ as a result of mutually independent choice of edges from $E(n, 3, 1)$ with the same probability $\frac{1}{2}$. Therefore, there are independent copies of a random graph of Erdős–Rényi $G(m/2, 1/2)$ on cliques Q_1, \dots, Q_{n-m} . Let us note that these copies are independent from the point of view of probability theory (as random elements), and from the point of view of the theory of graphs (there are no edges between them).

When $p = \frac{1}{2}$, Theorem 1 says that with the asymptotic probability 1, we have $\alpha(G(m/2, 1/2)) \sim 2 \log_2 m$ when $m \rightarrow \infty$, but m is only by a constant factor less than n , so $\alpha(G(m/2, 1/2)) \sim 2 \log_2 n$ when $n \rightarrow \infty$. Moreover, the rate of tending of probability to one is very high. For an appropriate choice of the infinitesimal parameter and large n , we get the estimate

$$\mathbb{P}(\alpha(G(m/2, 1/2)) \geq 2(1 + o(1)) \log_2 n) \geq 1 - 2^{-n}.$$

This means that

$$\mathbb{P}(\forall i = 1, \dots, n-m \quad \alpha(\mathcal{G}(Q_i, 1/2)) \geq 2(1 + o(1)) \log_2 n) \geq (1 - 2^{-n})^{n-m} \rightarrow 1, \quad n \rightarrow \infty.$$

Therefore, with the asymptotic probability 1 there are $n - m$ independent sets of size $2(1 + o(1)) \log_2 n$ in a random graph $\mathcal{G}(G(n, 3, 1), 1/2)$, and there are no edges between them. Together they make up one independent set of size $2(n - m)(1 + o(1)) \log_2 n \sim n \log_2 n$, QED.

Thus, for $G_{1/2}(n, 3, 1)$, just as it was for the Erdős–Rényi random graph, we again have the growth of the independence number in approximately logarithm of the number of vertices times!

Problem 51*. Try to improve into a constant number of times the bound in the problem 50.

Solution. To improve the bound, it suffices to repeat the proofs of Problems 49 and 50, replacing $m = \frac{n}{2}$ by $m = 2 \left\lceil \frac{n}{2 \log_2 n} \right\rceil$, here $[x]$ is the usual integer part of x . Then we obtain an estimate of exactly two times better than in Problem 50.

3.4 Random subgraphs of the graph $G(n, 2, 1)$

Problem 52. Find $\alpha(G(n, 2, 1))$.

Solution. Obviously, this is just a cover of our set by disjoint pairs. Hence, $\alpha(G(n, 2, 1)) = \frac{n}{2}$ for even n , and $\alpha(G(n, 2, 1)) = \frac{n-1}{2}$ for odd n .

Problem 53. Let $r(A)$ be the same as in formula (2). Prove that always $r(A) \geq \frac{2|A|^2}{n} - |A|$.

Solution. The set A is a subset of \mathcal{R}_n . For every $i \in \mathcal{R}_n$, let k_i be the number of vertices of the graph $G(n, 2, 1)$ (“twos”) which belong to A and contain i . It is clear that for fixed i , any two “twos” corresponding to this i form an edge in $G(n, 2, 1)$. Therefore,

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}| \geq \sum_{i=1}^n C_{k_i}^2.$$

At the same time $k_1 + \dots + k_n = 2|A|$. It is easy to show that, under these constraints, the minimum of $\sum_{i=1}^n C_{k_i}^2$ is achieved at $k_i = \frac{2|A|}{n}$, $i = 1, \dots, n$, which implies the bound

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}| \geq \sum_{i=1}^n C_{k_i}^2 \geq \frac{2|A|^2}{n} - |A|.$$

Problem 54. Derive from the previous problem the inequality $\alpha(G_{1/2}(n, 2, 1)) \leq \left(\frac{1}{2} + \varepsilon\right) n \log_2 n$, which is true for every $\varepsilon > 0$ almost surely.

Solution. We know the estimate from Problem 53, so we have

$$\begin{aligned} \sum_{A \subset V(n, 2), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}|} &< C_n^k 2^{-(1+o(1))\frac{2k^2}{n}} < \left(\frac{eC_n^2}{k}\right)^k 2^{-(1+o(1))\frac{2k^2}{n}} < 2^k n^{2k} k^{-k} 2^{-(1+o(1))\frac{2k^2}{n}} = \\ &= 2^{2k \log_2 n - (1+o(1))k \log_2 k - (1+o(1))\frac{2k^2}{n}}. \end{aligned}$$

Therefore, for a suitable $k \sim \frac{1}{2}n \log_2 n$ we obtain

$$2 \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{2k}{n} < 0,$$

then

$$2k \log_2 n - (1 + o(1))k \log_2 k - (1 + o(1)) \frac{2k^2}{n} = k \left(2 \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{2k}{n} \right) \rightarrow -\infty.$$

That is, we have shown that $P(X_k \geq 1) \leq MX_k \rightarrow 0$ and the estimate is proved.

Problem 55*. Prove a lower bound for $\alpha(G_{1/2}(n, 2, 1))$ which has order of magnitude $cn \log_2 n$ with some $c > 0$.

Solution. The proof of this fact is quite long. If you want you can find it in [5].

Problem 56.** Find a constant c in the assertion: for any $\varepsilon > 0$, almost surely

$$(c - \varepsilon)n \log_2 n \leq \alpha(G_{1/2}(n, 2, 1)) \leq (c + \varepsilon)n \log_2 n.$$

Solution. Unfortunately, by the beginning of the conference, this problem has not been solved. And the students did not change this fact.

References

- [1] A.M. Raigorodskii, *The chromatic numbers*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2003 (in Russian).
- [2] A.M. Raigorodskii, *The linear algebra method in combinatorics*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2007 (in Russian).
- [3] A.M. Raigorodskii, *Probability and algebra in combinatorics*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2008 (in Russian).
- [4] A.M. Raigorodskii, *Models of random graphs*, Moscow Centre for Continuous Mathematical Education (MCCME), Moscow, Russia, 2011 (in Russian).
- [5] L. I. Bogolyubskiy, A. S. Gusev, M. M. Pyaderkin, and A. M. Raigorodskii, The independence numbers and the chromatic numbers of random subgraphs of some distance graphs, *Sbornik:Math*, 2014, to appear (current Russian version will be on the disc, English journal version will be available at http://www.mathnet.ru/php/person.phtml?&personid=8601&option_lang=eng)
- [6] J. Balogh, A.V. Kostochka, A.M. Raigorodskii, *Coloring some finite sets in \mathbb{R}^n* , *Discussiones Mathematicae Graph Theory*, 33 (2013), N1, 25 - 31.

Числа независимости и хроматические числа случайных подграфов некоторых дистанционных графов*

Л.И. Боголюбский[†], А.С. Гусев[‡], М.М. Пядёркин[§], А.М. Райгородский[¶]

1 Введение

1.1 Мотивировка из комбинаторной геометрии

Отправной точкой для нашего исследования служит граф $G(n, 3, 1) = (V(n, 3), E(n, 3, 1))$, у которого

$$V(n, 3) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = 3\}, \quad E(n, 3, 1) = \{\{\mathbf{x}, \mathbf{y}\} : (\mathbf{x}, \mathbf{y}) = 1\},$$

где (\mathbf{x}, \mathbf{y}) — скалярное произведение векторов в евклидовом пространстве. Иными словами, вершины графа $G(n, 3, 1)$ — $(0,1)$ -векторы с ровно тремя единицами, а ребра — пары вершин, имеющих в точности одну общую единицу (или, что то же самое, пары вершин, отстоящих друг от друга на евклидово расстояние 2). Ввиду последнего обстоятельства граф $G(n, 3, 1)$ является *дистанционным*, т.е. его вершины — точки пространства, а ребра — отрезки фиксированной длины (см. [1]).

Граф $G(n, 3, 1)$ впервые появился в работе Ж. Нады 1972 года (см. [2]), где он был использован для отыскания конструктивных оценок числа Рамсея (см. [3], [4]). Другое важное применение этот граф нашел в статье [5] Д. Лармана и К.А. Роджерса, которая вышла в том же 1972 году и посвящена классическому объекту комбинаторной геометрии — *хроматическому числу* $\chi(\mathbb{R}^n)$ евклидова пространства \mathbb{R}^n :

$$\chi(\mathbb{R}^n) = \min\{\chi : \mathbb{R}^n = V_1 \sqcup \dots \sqcup V_\chi, \forall i \forall \mathbf{x}, \mathbf{y} \in V_i \mid \mathbf{x} - \mathbf{y} \neq 1\},$$

где $|\mathbf{x} - \mathbf{y}|$ — евклидово расстояние. Иначе говоря, хроматическое число пространства — это минимальное количество цветов, в которые можно так покрасить все точки \mathbb{R}^n , чтобы между одноцветными точками не было расстояния 1.

Суть наблюдения Лармана и Роджерса состояла в том, что, очевидно, $\chi(\mathbb{R}^n) \geq \chi(G(n, 3, 1))$, где $\chi(G)$ — обычное хроматическое число графа G , равное наименьшему количеству цветов, в которые можно так покрасить все вершины графа, чтобы вершины одного цвета не были соединены ребром. Таким образом, задача отыскания нижней оценки хроматического числа пространства была сведена к оценке хроматического числа конечного графа.

Одна из наиболее стандартных нижних оценок хроматического числа абстрактного графа $G = (V, E)$ имеет вид $\chi(G) \geq \frac{|V|}{\alpha(G)}$. Здесь $\alpha(G)$ — *число независимости* графа G , равное максимальному числу вершин графа, которые попарно не соединены ребрами:

$$\alpha(G) = \max\{|W| : \forall \mathbf{x}, \mathbf{y} \in W \ \{\mathbf{x}, \mathbf{y}\} \notin E\}.$$

*Настоящая работа выполнена при финансовой поддержке гранта РФФИ N 12-01-00683, гранта Президента РФ МД-6277.2013.1 и гранта НШ-2519.2012.1 поддержки ведущих научных школ.

[†]МГУ им. М.В. Ломоносова, механико-математический факультет, кафедра теории вероятностей.

[‡]МГУ им. М.В. Ломоносова, механико-математический факультет, кафедра теории вероятностей.

[§]МГУ им. М.В. Ломоносова, механико-математический факультет, кафедра теории вероятностей.

[¶]МГУ им. М.В. Ломоносова, механико-математический факультет, кафедра математической статистики и случайных процессов; Московский физико-технический институт (государственный университет), факультет инноваций и высоких технологий, кафедра дискретной математики.

Ж. Надь доказал следующую теорему.

Теорема 1. *Справедлива формула*

$$\alpha(G(n, 3, 1)) = \begin{cases} n, & \text{если } n \equiv 0 \pmod{4}, \\ n - 1, & \text{если } n \equiv 1 \pmod{4}, \\ n - 2, & \text{если } n \equiv 2, 3 \pmod{4}. \end{cases}$$

Из этой теоремы сразу вытекала рекордная на тот момент оценка

$$\chi(\mathbb{R}^n) \geq \chi(G(n, 3, 1)) \geq \frac{C_n^3}{\alpha(G(n, 3, 1))} \sim \frac{n^2}{6}.$$

В принципе могло стать, что оценка, найденная с помощью числа независимости, подлежит улучшению. Однако совсем недавно в совместной работе Й. Балоба, А.В. Косточки и А.М. Райгородского (см. [6]) была доказана

Теорема 2. *Если $n = 2^k$, то $\chi(G(n, 3, 1)) = \frac{(n-1)(n-2)}{6}$. В любом случае $\chi(G(n, 3, 1)) = \frac{n^2}{6} + O(n)$.*

Таким образом, для графа $G(n, 3, 1)$ известно и число независимости, и хроматическое число.

В следующем параграфе мы напомним несколько объектов и фактов из теории случайных графов. В последнем параграфе мы поставим одну из основных задач статьи и опишем дальнейшую структуру работы. В завершение текущего параграфа дадим несколько ссылок на книги и обзоры, в которых можно найти много дополнительной информации о дистанционных графах, их хроматических числах и числах независимости, а также о их месте и роли в современной комбинаторной геометрии: [1], [7]–[13].

1.2 Мотивировка из теории случайных графов

В 1959 году П. Эрдеши и А. Реньи предложили модель случайного графа, которая к настоящему времени очень глубоко изучена (см. [14]–[20]). Случайный граф $G(n, p)$ в этой модели — это случайный элемент со значениями во множестве всех графов на n вершинах $V_n = \{1, \dots, n\}$ без петель, кратных ребер и ориентации, имеющий биномиальное распределение, т.е.

$$\mathbb{P}(G(n, p) = (V_n, E)) = p^{|E|}(1-p)^{C_n^2 - |E|}.$$

Отметим, что p — вероятность ребра — это, вообще говоря, функция от n .

Одной из важнейших задач о случайных графах Эрдеши–Реньи является задача об отыскании их чисел независимости и хроматических чисел. Дабы сформулировать ниже классическую теорему об асимптотическом поведении этих чисел, договоримся о некоторой терминологии. Во-первых, если \mathcal{A} — это какое-то свойство графа (например, свойство связности), то мы будем писать $\mathbb{P}(G(n, p) \in \mathcal{A})$ или, при отсутствии разночтений, просто $\mathbb{P}(\mathcal{A})$, имея в виду вероятность, с которой случайный граф $G(n, p)$ обладает этим свойством. Заметим, что в принципе само свойство может зависеть от n : граф обладает свойством \mathcal{A}_n , коль скоро, скажем, его хроматическое число больше $\frac{n}{2}$. Во-вторых, мы будем говорить, что свойство \mathcal{A} (или, точнее, последовательность свойств \mathcal{A}_n) реализуется с *асимптотической вероятностью 1*, если $\mathbb{P}(G(n, p) \in \mathcal{A}_n) \rightarrow 1$ при $n \rightarrow \infty$. Наконец, пусть f — некоторая функция натурального аргумента n , а g — некоторая функция, определенная на множестве всех графов. Мы скажем, что с асимптотической вероятностью 1 выполнено свойство $g(G(n, p)) \sim f(n)$, если существует еще одна функция φ аргумента n , которая бесконечно мала по отношению к f при $n \rightarrow \infty$ и с которой

$$\mathbb{P}(|g(G(n, p)) - f(n)| < \varphi(n)) \rightarrow 1, \quad n \rightarrow \infty.$$

Теорема 3. *Пусть p — это либо константа, либо произвольная функция, которая стремится к нулю при $n \rightarrow \infty$, но при этом ограничена снизу величиной $\frac{c}{n}$, где $c > 1$. Положим $d = \frac{1}{1-p}$. Тогда с асимптотической вероятностью 1 выполнены соотношения*

$$\alpha(G(n, p)) \sim 2 \log_d(np), \quad \chi(G(n, p)) \sim \frac{n}{2 \log_d(np)}.$$

В случае постоянного p теорема была доказана в работе Б. Боллобаша 1988 года (см. [21]), а в случае меньших вероятностей ребра утверждение теоремы принадлежит Т. Лучаку, который установил его в 1991 году (см. [22]). Многочисленные результаты, уточняющие теорему 3, можно найти в книгах [18], [20].

Естественное обобщение модели Эрдеша–Реньи устроено следующим образом. Пусть дана некоторая последовательность графов $H_n = (V_n, E_n)$, в которой $|V_n| \rightarrow \infty$ при $n \rightarrow \infty$. Заметим, что здесь n не обязано быть числом вершин. Например, вполне годится $H_n = G(n, 3, 1)$, в которой $|V(n, 3)| = C_n^3$. Определим случайный граф $\mathcal{G}(H_n, p)$ как случайный элемент со значениями во множестве всех остовных подграфов $G = (V_n, E)$ графа H_n и с биномиальным распределением, т.е.

$$\mathbb{P}(\mathcal{G}(H_n, p) = (V_n, E)) = p^{|E|}(1-p)^{|E_n|-|E|}.$$

Понятно, что $G(n, p) = \mathcal{G}(K_n, p)$, где K_n — полный граф на n вершинах.

С одной стороны, очень хорошо изучен случай $H_n = Q^n$, где Q^n — это n -мерный куб, т.е. граф, вершины которого суть все $(0, 1)$ -векторы, а ребра — это пары вершин, различающихся ровно в одной координате (образующих ребро куба). В частности, число независимости случайного подграфа куба исследовалось в работе [23], где доказано, что если p — любая функция от n , с которой $pn \rightarrow \infty$ при $n \rightarrow \infty$, то с асимптотической вероятностью 1 выполнено $\alpha(\mathcal{G}(Q^n, p)) \sim 2^{n-1}$. Отметим, что граф Q^n , подобно графу $G(n, 3, 1)$, является дистанционным.

С другой стороны, в последние 10 лет бурно развивается наука о свойствах случайных подграфов регулярных графов (см., например, [24]). Глубоко изучены пороговые вероятности для планарности, для возникновения гигантской компоненты и пр. Однако задачи о раскрасках в такой общности не имеют смысла. Отметим, тем не менее, что $G(n, 3, 1)$ — регулярный граф: степень каждой его вершины равна $3C_{n-3}^2$.

1.3 Постановка задачи и структура статьи

Из первых двух параграфов ясно, что одним из основных вопросов настоящей работы является вопрос об асимптотическом поведении числа независимости и хроматического числа случайного графа $\mathcal{G}(G(n, 3, 1), p)$. Вместе с тем в статье будут изучены и многие другие близкие задачи.

Опишем дальнейшую структуру нашего текста. В разделе 2 мы сформулируем и докажем оценки величины $\alpha(\mathcal{G}(G(n, 3, 1), 1/2))$. Раздел 3 мы посвятим величине $\chi(\mathcal{G}(G(n, 3, 1), 1/2))$. В разделе 4 мы введем графы $G(n, r, s)$, которые естественным образом обобщают графы $G(n, 3, 1)$ и которые еще более важны для комбинаторной геометрии: мы начали с $G(n, 3, 1)$ для большей ясности дальнейшего изложения. В том же разделе 4 мы получим результаты для числа независимости случайного графа $\mathcal{G}(G(n, r, s), 1/2)$. В разделе 5 мы изучим хроматическое число этого графа. Разобравшись, тем самым, со случаем $p = \frac{1}{2}$, мы скажем несколько слов про общий случай в разделе 6. Наконец, в разделе 7 мы поговорим об одной задаче теории Рамсея, которая решается с помощью разработанной нами техники.

2 Число независимости случайного графа $\mathcal{G}(G(n, 3, 1), 1/2)$

2.1 Формулировки результатов

Мы уже использовали выше терминологию “асимптотическое равенство выполнено с асимптотической вероятностью 1”. В аналогичном смысле мы будем понимать и асимптотические неравенства, т.е. утверждение типа “выполнено $g(\mathcal{G}(G(n, 3, 1), 1/2)) \leq (1 + o(1))f(n)$ с асимптотической вероятностью 1” (здесь всякий раз будет $f(n) \rightarrow \infty$ при $n \rightarrow \infty$) означает существование такой функции φ аргумента n , что $\varphi = o(1)$ при $n \rightarrow \infty$ и

$$\mathbb{P}(g(\mathcal{G}(G(n, 3, 1), 1/2)) \leq (1 + \varphi(n))f(n)) \rightarrow 1, \quad n \rightarrow \infty.$$

Теорема 4. *С асимптотической вероятностью 1 справедливо неравенство*

$$\alpha(\mathcal{G}(G(n, 3, 1), 1/2)) \leq 4(1 + o(1))n \log_2 n.$$

Теорема 5. *С асимптотической вероятностью 1 справедливо неравенство*

$$\alpha(\mathcal{G}(G(n, 3, 1), 1/2)) \geq 2(1 + o(1))n \log_2 n.$$

Таким образом, мы имеем практически неулучшаемые оценки: константы в них отличаются лишь в примерно два раза. Отметим, что оценки из теорем 4 и 5 можно записать в виде

$$\alpha(\mathcal{G}(G(n, 3, 1), 1/2)) = \Theta(\alpha(G(n, 3, 1)) \log_2(|V(n, 3)|)),$$

где символ Θ означает, что равенство выполнено с точностью до положительных констант в верхней и нижней оценке. Этот результат хорошо согласуется с классической теоремой 3, поскольку там $\alpha(K_n) = 1$, а $\log_2(|V_n|) = \log_2 n$.

В следующем параграфе мы докажем теорему 4. В параграфе 2.3 мы приведем доказательство теоремы 5. А в параграфе 2.4 мы дадим некоторые комментарии.

2.2 Доказательство теоремы 4

Это доказательство стандартно, но мы его приводим подробно, т.к. в дальнейшем мы будем иметь дело с уточненными вариантами аналогичных доказательств.

Пусть $X_k = X_k(\mathcal{G}(G(n, 3, 1), 1/2))$ — это функция от случайного графа, равная количеству k -вершинных независимых множеств в нем (т.е. множеств, элементы которых попарно не соединены ребрами). Оценим ее математическое ожидание и применим неравенство Маркова:

$$\begin{aligned} \mathbb{E}X_k &= \sum_{ACV(n,3), |A|=k} \mathbb{P}(A \text{ является независимым множеством в } \mathcal{G}(G(n, 3, 1), 1/2)) = \\ &= \sum_{ACV(n,3), |A|=k} 2^{-|\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 1) : \mathbf{x}, \mathbf{y} \in A\}|}, \end{aligned}$$

т.е. в показателе экспоненты стоит число ребер подграфа графа $G(n, 3, 1)$, порожденного конкретным множеством вершин A . Из классической теоремы Турана (см. [25]) следует, что если $k > \alpha(G(n, 3, 1))$, то мы не только можем гарантировать наличие ребер в таком подграфе, но и можем эффективно оценить снизу число этих ребер. Дабы записать оценку, напомним, что $\alpha(G(n, 3, 1)) \sim n$ при $n \rightarrow \infty$, а значит, $k \rightarrow \infty$ при $n \rightarrow \infty$. Поэтому в известном смысле корректна запись

$$|\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 1) : \mathbf{x}, \mathbf{y} \in A\}| > (1 + o(1)) \frac{k^2}{2\alpha(G(n, 3, 1))} = (1 + o(1)) \frac{k^2}{2n}.$$

Имея на руках такую оценку, получаем, что

$$\mathbb{E}X_k < \sum_{ACV(n,3), |A|=k} 2^{-(1+o(1))\frac{k^2}{2n}} = C_{C_n^3}^k 2^{-(1+o(1))\frac{k^2}{2n}}.$$

Хорошо известно, что $C_a^b \leq \left(\frac{ea}{b}\right)^b$, где e — основание натурального логарифма. Следовательно,

$$\mathbb{E}X_k < \left(\frac{n^3}{k}\right)^k 2^{-(1+o(1))\frac{k^2}{2n}} = 2^{3k \log_2 n - k \log_2 k - (1+o(1))\frac{k^2}{2n}}.$$

Видно, что существует функция $k = k(n)$, которая асимптотически ведет себя как $4n \log_2 n$ и с которой $\mathbb{E}X_k \rightarrow 0$ при $n \rightarrow \infty$. Отсюда с учетом неравенства Маркова вытекает утверждение теоремы:

$$\mathbb{P}(\alpha(\mathcal{G}(G(n, 3, 1), 1/2)) \leq 4(1 + o(1))n \log_2 n) = \mathbb{P}(X_k = 0) \geq 1 - \mathbb{E}X_k \rightarrow 1, \quad n \rightarrow \infty.$$

Теорема доказана.

2.3 Доказательство теоремы 5

Если рассуждение из предыдущего параграфа было вполне стандартным и никак не использовало специфику графа $G(n, 3, 1)$ (за исключением величины его числа независимости), то здесь мы в большей мере будем опираться на структуру нашего графа. Прежде всего введем ряд обозначений и терминов.

Пусть $\mathcal{R}_n = \{1, \dots, n\}$. Каждой вершине $\mathbf{x} \in V(n, 3)$ можно поставить в естественное соответствие тройку элементов из \mathcal{R}_n : это просто номера координат, на которых у вектора \mathbf{x} находятся единицы. Тогда ребро в графе $G(n, 3)$ — это пара троек, пересекающихся ровно по одному элементу.

Клик в графе называется любой полный подграф, т.е. подграф, в котором проведены все возможные ребра. Размер максимальной клики в абстрактном графе G называется *кликковым числом* и обозначается $\omega(G)$. Это обозначение хорошо согласуется с обозначением числа независимости $\alpha(G)$, которое в понятном смысле двойственно ему.

Для графа $G(n, 3, 1)$ любая клика — это набор троек в \mathcal{R}_n , попарные пересечения которых имеют мощность 1. Ясно, что $\omega(G(n, 3, 1)) \sim \frac{n}{2}$ при $n \rightarrow \infty$ (фиксируется один элемент \mathcal{R}_n , а оставшаяся часть множества \mathcal{R}_n разбивается на непересекающиеся пары).

Дальнейшая идея состоит в том, что, оказывается, в графе $G(n, 3, 1)$ можно выбрать “почти” n “почти” максимальных клик, между которыми, однако, нет ни одного ребра.

Итак, положим $m = 2 \left\lfloor \frac{n}{2 \log_2 n} \right\rfloor$, где $[x]$ — это обычная целая часть числа x . Разобьем \mathcal{R}_n на части $R_1 = \mathcal{R}_m$ и $R_2 = \mathcal{R}_n \setminus R_1$. Сперва опишем построение одной клики Q_1 . Для этого возьмем в R_1 непересекающиеся пары $\{1, 2\}, \{3, 4\}, \{5, 6\}, \dots, \{m-1, m\}$ (благо m четное). К каждой из этих пар добавим элемент $m+1 \in R_2$. Это и есть искомая клика (см. рис. 1). Число вершин в ней $\frac{m}{2} \sim \frac{n}{2 \log_2 n}$, $n \rightarrow \infty$, т.е. оно отличается от максимально возможного лишь в примерно логарифм раз. Аналогично построим еще $n-m-1$ клику Q_2, \dots, Q_{n-m} , добавляя к каждой из наших пар в R_1 элемент $m+2 \in R_2$, элемент $m+3 \in R_2$ и так далее. Очевидно, что для любых i, j , $i \neq j$, и для любых \mathbf{x} из Q_i , \mathbf{y} из Q_j ребра между \mathbf{x}, \mathbf{y} нет: эти тройки могут либо вовсе не пересекаться, либо пересекаться сразу по какой-то паре из R_1 .

Как мы знаем, случайный граф $\mathcal{G}(G(n, 3, 1), 1/2)$ получается из графа $G(n, 3, 1)$ в результате взаимно независимого выбора ребер из $E(n, 3, 1)$ с одной и той же вероятностью $\frac{1}{2}$. Поэтому на кликах Q_1, \dots, Q_{n-m} возникают независимые копии случайного графа Эрдеша–Реньи $G(m/2, 1/2)$. Отметим, что эти копии независимы и с точки зрения теории вероятностей (как случайные элементы), и с точки зрения теории графов (между ними нет ребер).

При $p = \frac{1}{2}$ теорема 3 говорит, что с асимптотической вероятностью 1 выполнено $\alpha(G(m/2, 1/2)) \sim 2 \log_2 m$ при $m \rightarrow \infty$, но m лишь в логарифм раз меньше n , откуда $\alpha(G(m/2, 1/2)) \sim 2 \log_2 n$ при $n \rightarrow \infty$. Более того, скорость стремления вероятности к единице очень высока (см. [17], [18], [26]). Заведомо при правильно подобранной бесконечно малой и больших n верна оценка

$$\mathbb{P}(\alpha(G(m/2, 1/2)) \geq 2(1 + o(1)) \log_2 n) \geq 1 - e^{-n}.$$

А это значит, что

$$\mathbb{P}(\forall i = 1, \dots, n-m \quad \alpha(\mathcal{G}(Q_i, 1/2)) \geq 2(1 + o(1)) \log_2 n) \geq (1 - e^{-n})^{n-m} \rightarrow 1, \quad n \rightarrow \infty.$$

Следовательно, с асимптотической вероятностью 1 в случайном графе $\mathcal{G}(G(n, 3, 1), 1/2)$ есть $n-m$ независимых множеств размера $2(1 + o(1)) \log_2 n$, между которыми точно нет ребер. Вместе они составляют, тем самым, одно независимое множество размера $2(n-m)(1 + o(1)) \log_2 n \sim 2n \log_2 n$, что и требовалось доказать.

2.4 Комментарии

Утверждение и доказательство теоремы 4 можно вложить в существенно более общий контекст. Справедлива

Теорема 6. Пусть дана некоторая последовательность графов $H_n = (V_n, E_n)$, в которой $|V_n| \rightarrow \infty$ при $n \rightarrow \infty$. Рассмотрим случайный граф $\mathcal{G}(H_n, p)$ с произвольной вероятностью ребра $p = p(n)$.

Пусть $k = k(n)$ — произвольная функция, с которой выполнено

$$\sum_{A \subset V_n, |A|=k} (1-p)^{|\{\{\mathbf{x}, \mathbf{y}\} \in E_n : \mathbf{x}, \mathbf{y} \in A\}|} \rightarrow 0, \quad n \rightarrow \infty.$$

Тогда с асимптотической вероятностью 1 имеет место неравенство $\alpha(\mathcal{G}(H_n, p)) < k$.

Доказательство теоремы 6 мы, разумеется, не приводим.

В параграфе 2.2 мы воспользовались оценкой Турана для величины $|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 1) : \mathbf{x}, \mathbf{y} \in A\}|$. Конечно, могло бы стать, что эта оценка не точна. Однако оценка достигается, причем именно на конструкции из клик, которая сработала в параграфе 2.3. Действительно, пусть Q_1, \dots, Q_{n-m} — те самые клики. Пусть $k = k(n)$ — произвольная функция, асимптотически ведущая себя как $4n \log_2 n$. Оценка Турана имела в этом случае вид

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 3, 1) : \mathbf{x}, \mathbf{y} \in A\}| > 8(1 + o(1))n \log_2^2 n.$$

Рассмотрим любое множество A мощности k , у которого мощности пересечения с множествами вершин наших клик примерно одинаковы. Тогда эти мощности асимптотически равны $4 \log_2 n$. Значит, число ребер в подграфе графа $G(n, 3, 1)$, порожденном таким множеством A , асимптотически равно $8n \log_2^2 n$. Ясно, что описанных множеств A очень много, и, если стремиться к улучшению именно верхней оценки числа независимости, то нужно как-то аккуратно классифицировать различные $A \subset V(n, 3)$ по количеству ребер графа $G(n, 3, 1)$, которые в них проведены. По-видимому, даже для графа $G(n, 3, 1)$ — это трудная задача.

В завершение параграфа назовем конструкцию из клик, попарно не соединенных ребрами, *блоком*. Подобные конструкции понадобятся нам и в дальнейшем.

3 Хроматическое число случайного графа $\mathcal{G}(G(n, 3, 1), 1/2)$

3.1 Формулировки результатов

Следующая теорема является тривиальным следствием теоремы 4 и оценки $\chi(G) \geq \frac{|V|}{\alpha(G)}$. Естественно, ее мы не доказываем.

Теорема 7. *С асимптотической вероятностью 1 справедливо неравенство*

$$\chi(\mathcal{G}(G(n, 3, 1), 1/2)) \geq \frac{1}{24}(1 + o(1)) \frac{n^2}{\log_2 n}.$$

Гораздо более тонким является тот факт, что оценку из теоремы 7 принципиально улучшить нельзя.

Теорема 8. *С асимптотической вероятностью 1 справедливо неравенство*

$$\chi(\mathcal{G}(G(n, 3, 1), 1/2)) \leq \frac{1}{6}(1 + o(1)) \frac{n^2}{\log_2 n}.$$

Теорему 8 мы докажем в следующем параграфе. Отметим, что в рамках нашего подхода для хроматического числа получается вдвое больший зазор, нежели для числа независимости.

3.2 Доказательство теоремы 8

Нам понадобится вспомогательная конструкция: а именно, мы разобьем множество вершин графа $G(n, 3, 1)$ — множество “троек” — на своего рода слои. После этого мы будем вести раскраску вершин случайного графа отдельно по слоям.

Итак, начнем с построения первого слоя, который мы обозначим \mathcal{S}_1 . Для этого разделим n на 4 с остатком: $n = 4s_1 + t_1$, $t_1 \leq 3$. Положим $L_1 = \mathcal{R}_{2s_1}$, $R_1 = \{2s_1 + 1, \dots, 4s_1\}$, $T_1 = \{4s_1 + 1, \dots, n\}$, так что $\mathcal{R}_n = L_1 \sqcup R_1 \sqcup T_1$. По понятным причинам назовем L_1 *левой половинкой*, R_1 *правой половинкой*, а T_1 *довеском*.

Далее, *совершенным паросочетанием* в любой из половинок называется разбиение этой половинки на двухэлементные множества — *пары*. Например, совокупность пар $\{1, 2\}, \{3, 4\}, \dots, \{2s_1 - 1, 2s_1\}$ образует совершенное паросочетание в левой половинке. Хорошо известно (см. [25]), что множество всех пар в L_1 разбивается на непересекающиеся совершенные паросочетания. Поскольку всего пар $C_{2s_1}^2$, а в каждом паросочетании их s_1 , выходит, что общее число паросочетаний в разбиении равно $2s_1 - 1$. Обозначим эти паросочетания M_1, \dots, M_{2s_1-1} . Аналогичные паросочетания в R_1 обозначим N_1, \dots, N_{2s_1-1} .

Зафиксируем паросочетание M_i . К каждой паре в нем добавим элемент $j \in R_1$. Образуется клика из троек в графе $G(n, 3, 1)$. Совокупность всех $2s_1$ таких клик — это блок (см. §2.4). В общей сложности имеем $2s_1 - 1$ блоков по $2s_1$ клик в каждом. Аналогично строим $2s_1 - 1$ блоков по паросочетаниям из правой половинки. Обозначим наши блоки A_1, \dots, A_{2s_1-1} и B_1, \dots, B_{2s_1-1} соответственно.

Множество троек, которые имеют общие элементы с довеском T_1 , обозначим C_1 . В итоге в слой \mathcal{S}_1 мы отправим все тройки из блоков A_1, \dots, A_{2s_1-1} и B_1, \dots, B_{2s_1-1} .

Какие тройки не попали ни в первый слой, ни в C_1 ? Разумеется, только те, которые либо целиком лежат в L_1 , либо целиком лежат в R_1 . Как в графе $G(n, 3, 1)$, так, тем более, и в его случайном подграфе тройки из разных половинок попарно несмежны. Поэтому про правую половинку можно забыть и красить лишь содержимое левой (см., впрочем, замечание 1 в конце доказательства). С левой же половинкой поступаем ровно так же, как, строя слой \mathcal{S}_1 , мы поступили со всем \mathcal{R}_n . Иными словами, полагаем $2s_1 = 4s_2 + t_2$, $t_2 \leq 3$, $L_2 = \mathcal{R}_{2s_2}$, $R_2 = \{2s_2 + 1, \dots, 4s_2\}$, $T_2 = \{4s_2 + 1, \dots, 2s_1\}$, так что $L_1 = L_2 \sqcup R_2 \sqcup T_2$. Строим $4s_2 - 2$ блоков и множество троек C_2 , имеющих непустые пересечения с T_2 . В слой \mathcal{S}_2 кладем все тройки из блоков.

И так далее. На выходе имеем последовательность слоев \mathcal{S}_k и дополнительных множеств C_k . В слое \mathcal{S}_k находится $4s_k - 2$ блоков, в каждом таком блоке $2s_k$ клик, и у каждой из этих клик s_k вершин. При этом слой \mathcal{S}_k локализован в множестве $\{1, \dots, \frac{n}{2^{k-1}}\}$.

Теперь перейдем к случайному графу $\mathcal{G}(G(n, 3, 1), 1/2)$ и его раскраске. Прежде всего раскрасим его вершины, расположенные в множествах C_k . Здесь случайность роли не играет, и мы осуществим покраску с запасом, т.е. сделаем ее в исходном графе $G(n, 3, 1)$. Очевидно, что в этом случае на вершины из C_k уйдет не больше $3(4s_k + 3)$ цветов. В сумме имеем

$$\sum_k 3(4s_k + 3) \leq 3 \left((n + 3) + \left(\frac{n}{2} + 3\right) + \left(\frac{n}{4} + 3\right) + \dots \right) = \Theta(n).$$

Как видно из утверждения теоремы, в котором обещается порядка $\frac{n^2}{\log_2 n}$ цветов, это количество не внесет значительного вклада в результат.

Рассмотрим слои. Сперва выберем из них те, чьи номера больше величины $\log_2 \log_2 n + 1$. Все эти слои локализованы в множестве $\left\{1, \dots, \left\lceil \frac{n}{\log_2 n} \right\rceil\right\}$. Снова забудем про случайность и воспользуемся с запасом раскраской графа $G\left(\left\lceil \frac{n}{\log_2 n} \right\rceil, 3, 1\right)$. В работе [6] показано, что на эту раскраску уйдет порядка $\frac{n^2}{\log_2^2 n}$ цветов, и это, опять-таки, в растущее число раз меньше величины, обещанной в теореме, которую мы доказываем.

Остаются слои с номерами $k \leq \log_2 \log_2 n + 1$. Заметим, что в этих слоях $s_k \rightarrow \infty$ при $n \rightarrow \infty$ и, более того, $\log_2 s_k \sim \log_2 n$. Пусть дан какой-то из этих слоев. Рассмотрим один из блоков в нем. Каждая клика в этом блоке имеет s_k вершин, и в случайном графе $\mathcal{G}(G(n, 3, 1), 1/2)$ на ней образуется случайный граф Эрдеша–Реньи $G(s_k, 1/2)$. По теореме 3 этой граф с высокой вероятностью красится в $(1 + o(1)) \frac{s_k}{2 \log_2 s_k}$ цветов. При правильно подобранной бесконечно малой и больших n “высокая вероятность” — это $1 - e^{-s_k} \geq 1 - e^{-n/\log_2 n}$ (см. [17], [18], [26]). Последняя величина, даже возведенная в степень, равную числу всех клик во всех блоках всех наших слоев, стремится к единице. Поэтому с асимптотической вероятностью 1 мы можем каждый блок покрасить в $(1 + o(1)) \frac{s_k}{2 \log_2 s_k}$ цветов.

Следовательно, на слой уйдет

$$4s_k(1 + o(1)) \frac{s_k}{2 \log_2 s_k} = (1 + o(1)) \frac{2s_k^2}{\log_2 s_k} = (1 + o(1)) \frac{n^2}{2^{2k+1} \log_2 n}$$

красок. Суммарно имеем

$$\sum_{k=1}^{\log_2 \log_2 n + 1} (1 + o(1)) \frac{n^2}{2^{2k+1} \log_2 n} \leq (1 + o(1)) \frac{1/8}{1 - 1/4} \cdot \frac{n^2}{\log_2 n} = \frac{1}{6} (1 + o(1)) \frac{n^2}{\log_2 n},$$

и теорема доказана.

Замечание 1. В процессе доказательства мы пренебрегали некоторыми половинками. Естественно, мы предполагали, что на их покраску уйдет столько же цветов, сколько ушло на покраску половинок, задействованных в слоях (*тех же самых* цветов). На самом деле в итоговой оценке вероятности следовало учитывать все клики из таким образом “потерянных” блоков. Однако и их не так много, чтобы заставить величину $1 - e^{-n/\log_2 n}$ путем возведения ее в соответствующую степень перестать стремиться к единице.

4 Графы $G(n, r, s)$, их случайные подграфы и числа независимости

4.1 Определения и формулировки результатов

Определения графов $G(n, r, s)$ полностью аналогичны определению графа $G(n, 3, 1)$ и подсказываются соответствием параметров:

$$V(n, r) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = r\}, \quad E(n, r, s) = \{\{\mathbf{x}, \mathbf{y}\} : (\mathbf{x}, \mathbf{y}) = s\}.$$

Графы $G(n, r, s)$ и их внутренняя структура играют значительную роль в различных областях дискретной математики. Прежде всего это, конечно, комбинаторная геометрия. Так, граф $G(n, 5, 2)$ возник в работе [27] Д. Лармана 1978 года, где с помощью оценки числа независимости этого графа было получено улучшение оценки Лармана–Роджерса из параграфа 1.1: $\chi(\mathbb{R}^n) \geq cn^3$, $c > 0$. А в 1981 году П. Франкл и Р.М. Уилсон опубликовали замечательную статью [28], в которой доказали, что $\chi(\mathbb{R}^n) \geq (1.207\dots + o(1))^n$, и для этого им понадобились графы с параметрами $r \sim \frac{2-\sqrt{2}}{2}n$, $s \sim \frac{r}{2}$, $n \rightarrow \infty$. Иными словами, важны графы $G(n, r, s)$ не только с постоянными, но и с растущими r и s .

В той же работе [28] Франкла и Уилсона эти графы были применены к отысканию конструктивных оценок числа Рамсея, ради которых они и были впервые придуманы Надем (см. параграф 1.1). А в 1993 году именно они дали первый контрпример к гипотезе Борсука о разбиении множеств на части меньшего диаметра (см. [7]–[9], [29]–[31]).

Впоследствии числам независимости и хроматическим числам графов $G(n, r, s)$ было посвящено множество работ, среди которых [32]–[38]. Однако, как мы увидим ниже, известно далеко не все. Отметим, что графы $G(n, r, s)$ глубоко связаны и с теорией кодирования. Например, клика в графе $G(n, n/2, n/4)$ при n , делящемся на 4, — это по сути матрица Адамара (см. [39], [40]).

В этом разделе мы изучим числа независимости случайных графов $\mathcal{G}(G(n, r, s), 1/2)$, причем r и s мы будем считать постоянными при $n \rightarrow \infty$. Даже величины $\alpha(G(n, r, s))$ найдены далеко не при всех r и s . Перечислим известные результаты.

Прежде всего очевидно, что запретить $(0, 1)$ -векторам иметь скалярное произведение s можно, заставив их иметь одно и то же множество из $s + 1$ единиц. Это значит, что

$$\alpha(G(n, r, s)) \geq C_{n-s-1}^{r-s-1} = \Theta(n^{r-s-1}).$$

С другой стороны, можно, наоборот, потребовать, чтобы попарные скалярные произведения не превосходили $s - 1$, как это обычно делают в теории кодов, исправляющих ошибки (см. [40]). При таком

подходе работает теорема Рёдля (см. [26] и [41]), из которой следует, что

$$\alpha(G(n, r, s)) \geq (1 + o(1)) \frac{C_n^s}{C_r^s} = \Theta(n^s).$$

Понятно, что при $r = 2s + 1$ оценки имеют одинаковый порядок, при $r > 2s + 1$ сильнее первая оценка, а при $r < 2s + 1$ сильнее вторая оценка.

Верхние оценки получаются с помощью линейно-алгебраического метода (см. [9]), и для них существенно, чтобы разность $r - s$ была степенью простого числа. Например, графы $G(n, 3, 1)$ и $G(n, 5, 2)$ удовлетворяют этому условию. Если оно выполнено, то теорема Франкла–Уилсона (см. [28]) говорит, что

$$\begin{aligned} \alpha(G(n, r, s)) &\leq (1 + o(1)) C_n^{r-s-1} = \Theta(n^{r-s-1}), \quad r \geq 2s + 1, \\ \alpha(G(n, r, s)) &\leq (1 + o(1)) \frac{C_n^{2s-r+1} C_n^{r-s-1}}{C_r^{2s-r+1}} = \Theta(n^s), \quad r < 2s + 1. \end{aligned}$$

Таким образом, при всех r и s , разность которых — степень простого, мы знаем порядок роста числа независимости, а при $r \geq 2s + 1$ и том же ограничении на разность мы даже знаем его асимптотику. Еще раз подчеркнем, что это специфика постоянных r, s . При этом без условия на разность $r - s$ оценки, как правило, гораздо хуже, и мы не будем на них останавливаться.

Перейдем к случайным графам. Имеет место универсальная верхняя оценка.

Теорема 9. *С асимптотической вероятностью 1 справедливо неравенство*

$$\alpha(\mathcal{G}(G(n, r, s), 1/2)) \leq (1 + o(1)) 2r \alpha(G(n, r, s)) \log_2 n.$$

Если, сверх того, известно, что $\alpha(G(n, r, s)) = \Theta(n^\beta)$, $\beta > 0$, то с асимптотической вероятностью 1 справедливо неравенство

$$\alpha(\mathcal{G}(G(n, r, s), 1/2)) \leq (1 + o(1)) 2(r - \beta) \alpha(G(n, r, s)) \log_2 n.$$

В частности,

$$\begin{aligned} \alpha(\mathcal{G}(G(n, r, s), 1/2)) &\leq (1 + o(1)) 2(s + 1) \alpha(G(n, r, s)) \log_2 n, \quad r \geq 2s + 1, \quad r - s - \text{степень простого,} \\ \alpha(\mathcal{G}(G(n, r, s), 1/2)) &\leq (1 + o(1)) 2(r - s) \alpha(G(n, r, s)) \log_2 n, \quad r < 2s + 1, \quad r - s - \text{степень простого.} \end{aligned}$$

Теорему 9 мы докажем в следующем параграфе. Нижние оценки обеспечивает

Теорема 10. *С асимптотической вероятностью 1 справедливо неравенство*

$$\alpha(\mathcal{G}(G(n, r, s), 1/2)) \geq (1 + o(1)) \frac{C_n^r (r - s)}{C_r^s C_{n-r}^{r-s}} \log_2 n.$$

Эту теорему мы докажем в разделе 5, где речь пойдет о хроматических числах: она будет следствием одного из общих утверждений о раскраске. А сейчас посмотрим на соотношения между теоремами 9 и 10. Очевидно, что при любых r, s оценка в теореме 10 имеет порядок $n^s \log_2 n$, т.е. при условиях $r \leq 2s + 1$ и $r - s = a^l$, где a — простое число, мы имеем лишь константный зазор между верхней и нижней оценками. Однако при $r > 2s + 1$ зазор растет полиномиально по n , и даже тривиальная оценка $\alpha(\mathcal{G}(G(n, r, s), 1/2)) \geq \alpha(G(n, r, s))$ становится сильнее оценки из теоремы 10, хотя и она в логарифм раз, конечно, меньше оценки из теоремы 9.

Имеет место

Теорема 11. *Пусть $r \geq 2s + 1$. Тогда с асимптотической вероятностью 1 справедливо неравенство*

$$\alpha(\mathcal{G}(G(n, r, s), 1/2)) \geq (1 + o(1)) 2C_n^s \log_2 n.$$

К сожалению, оценка в теореме 11 только в постоянное число раз больше оценки из теоремы 10. Она замечательна тем, что при $r = 2s + 1$ она согласуется с теоремой 5. Ее обобщением она и служит. Ее доказательство мы приведем в параграфе 4.3. Заметим, что при тех же $r = 3, s = 1$ теорема 10 дает лишь оценку величиной $\frac{2}{9}n \log_2 n$, тогда как оценка из теоремы 5 (теоремы 11) имеет величину $2n \log_2 n$. В этом ценность теоремы 11.

Ни при каких r, s теоремы 9, 10, 11 не дают асимптотику числа независимости. Это не удивительно, ведь даже для графа $G(n, 3, 1)$ имел место двухкратный зазор. Впрочем, есть граф, устроенный потенциально проще: это граф $G(n, 2, 1)$. Для него, очевидно, $\alpha(G(n, 2, 1)) = \lfloor \frac{n}{2} \rfloor$. Тогда теорема 9 дает оценку $(1 + o(1))n \log_2 n$, а теорема 10 — оценку $(1 + o(1))\frac{1}{4}n \log_2 n$. Теорема 11 здесь не работает. Имеет место

Теорема 12. *С асимптотической вероятностью 1 справедливо неравенство*

$$\alpha(\mathcal{G}(G(n, 2, 1), 1/2)) \leq (1 + o(1))\frac{1}{2}n \log_2 n.$$

Пафос в том, что, хотя и тут асимптотика не найдена, теорема 12 — это первое утверждение, в котором нам удастся усилить общую теорему 9. Более того, при $r \leq 2s + 1$ у нас оно одно такое. Мы докажем теорему 12 в параграфе 4.4.

И все-таки про один важный класс графов мы не сказали ни слова. Это класс, в котором находятся графы $G(n, r, 0)$. Такие графы называются *кнезеровскими* по имени математика, который в 50-е годы XX века высказал гипотезу о том, что $\chi(G(n, r, 0)) = n - 2r + 2$. Гипотезу доказал Л. Ловас только в конце 70-х годов с помощью им же разработанного топологического метода (см. [42]). Однако с числом независимости все несколько проще. Здесь независимое множество вершин — это набор попарно пересекающихся r -элементных подмножеств n -элементного множества, и при постоянном r его максимальная мощность найдена в классической теореме Эрдеша–Ко–Радо 1961 года (см. [4], [9], [43], [44]): она равна C_{n-1}^{r-1} . Конечно, мы и выше писали о том, что при $r \geq 2s + 1$ (оно сейчас как раз так) известна асимптотика величины $\alpha(G(n, r, s))$. Но в текущей ситуации и того больше: $\alpha(G(n, r, s)) = C_{n-1}^{r-1}$. Да и не нужно требовать, чтобы $r - s = r$ было степенью простого числа. Совсем несложной является

Теорема 13. *Пусть $r > 1^1$. С асимптотической вероятностью 1 справедлива асимптотика*

$$\alpha(\mathcal{G}(G(n, r, 0), 1/2)) \sim C_{n-1}^{r-1}.$$

Теорему 13 мы докажем в последнем параграфе настоящего раздела. Несмотря на свою простоту, эта теорема исключительно значима. Оказывается, иногда теорема 9 допускает улучшение в $\Theta(\log_2 n)$ раз, в результате чего число независимости случайного графа вовсе не меняется по отношению к числу независимости исходного графа (ср. похожий результат про куб в работе [23]). Есть шанс, что не только при $s = 0$, но и при всех $r > 2s + 1$ имеет место то же самое свойство. Этого мы пока не можем ни доказать, ни опровергнуть.

Подытожим параграф:

- при $r \leq 2s + 1$ и $r - s = a^l$, где a — простое число, найден порядок роста величины $\alpha(\mathcal{G}(G(n, r, s), 1/2))$ (теоремы 9 и 10);
- при $r = 2s + 1$ найдены лучшие нижние оценки величины $\alpha(\mathcal{G}(G(n, r, s), 1/2))$, нежели оценки при $r < 2s + 1$ (теорема 11);
- для параметров $r = 2, s = 1$, которые также удовлетворяют соотношению $r \leq 2s + 1$, улучшена верхняя оценка из теоремы 9 (теорема 12); других аналогичных пар с условием $r \leq 2s + 1$ не найдено;

¹Граф $G(n, 1, 0)$ — это просто полный граф, с ним все ясно.

- при произвольных $r > 2s + 1$ точные по порядку оценки не известны; зато в случае, когда $s = 0$, число независимости асимптотически почти наверное вовсе не изменяется (теорема 13), и есть основания предполагать, что это верно при всех $r > 2s + 1$;
- случаи, в которых $r - s$ не является, вообще говоря, степенью простого и которые отличны от двух предыдущих, с точки зрения конкретизации верхних оценок не рассматривались.

4.2 Доказательство теоремы 9

Теорема 9 является следствием общей теоремы 6. Величина $\alpha = \alpha(G(n, r, s))$ всегда растет с ростом n . Поэтому можно корректно говорить об асимптотиках. В силу теоремы Турана для любого множества $A \subset V(n, r)$, имеющего мощность $k > \alpha$, выполнено неравенство

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, r, s) : \mathbf{x}, \mathbf{y} \in A\}| > (1 + o(1)) \frac{k^2}{2\alpha}.$$

Значит,

$$\begin{aligned} \sum_{A \subset V(n, r), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, r, s) : \mathbf{x}, \mathbf{y} \in A\}|} &< C_{C_n^r}^k 2^{-(1+o(1)) \frac{k^2}{2\alpha}} < \left(\frac{eC_n^r}{k} \right)^k 2^{-(1+o(1)) \frac{k^2}{2\alpha}} < 3^k n^{rk} k^{-k} 2^{-(1+o(1)) \frac{k^2}{2\alpha}} = \\ &= 2^{rk \log_2 n - (1+o(1))k \log_2 k - (1+o(1)) \frac{k^2}{2\alpha}}. \end{aligned}$$

Последнее выражение стремится к нулю, коль скоро $r \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{k}{2\alpha}$ стремится к минус бесконечности. Очевидно, что, беря $k \sim 2r\alpha \log_2 n$, мы и добиваемся нужного результата. При этом мы даже не пользуемся вычитаемым $\log_2 k$. Если же мы знаем, что $\alpha = \Theta(n^\beta)$, $\beta > 0$, то при $k \sim 2(r - \beta)\alpha \log_2 n$ имеем $\log_2 k \sim \beta \log_2 n$, и этого хватает, чтобы все выражение $r \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{k}{2\alpha}$ стремилось к $-\infty$.

Теорема 9 доказана.

4.3 Доказательство теоремы 11

Идея доказательства в точности та же, что и в случае теоремы 5. Положим $m = (r - s) \left\lceil \frac{n}{(r - s) \log_2 n} \right\rceil$. Разобьем $\mathcal{R}_n = \{1, \dots, n\}$ на части $R_1 = \mathcal{R}_m$ и $R_2 = \mathcal{R}_n \setminus R_1$. Далее разобьем R_1 на последовательные куски мощности $r - s$: $\{1, 2, \dots, r - s\}$, $\{r - s + 1, \dots, 2(r - s)\}$, \dots , $\{m - (r - s) + 1, \dots, m\}$. Зафиксируем произвольное s -элементное подмножество множества R_2 . Добавим его к каждому из “кусков”. Получится клика в графе $G(n, r, s)$. Всего таких клик C_{n-m}^s . Между ними ребер нет, поскольку вершины из разных клик, будучи r -элементными множествами, либо пересекаются хотя бы по $r - s \geq 2s + 1 - s = s + 1$ элементам в R_1 , либо пересекаются по не более $s - 1$ элементам в целом. Совокупность клик, как и прежде, называется блоком.

Число вершин в каждой клике из блока равно $m' = \left\lceil \frac{n}{(r - s) \log_2 n} \right\rceil$. При рассмотрении случайного графа на данной клике образуется случайный граф $G(m', 1/2)$, у которого

$$\mathbb{P}(\alpha(G(m', 1/2)) \geq 2(1 + o(1)) \log_2 m') \geq 1 - e^{-m'}.$$

Значит,

$$\mathbb{P}(\alpha(\mathcal{G}(G(n, r, s), 1/2)) \geq 2C_{n-m}^s (1 + o(1)) \log_2 m') \geq (1 - e^{-m'})^{C_{n-m}^s}.$$

Поскольку s — константа, $C_{n-m}^s \sim C_n^s \sim \frac{n^s}{s!}$ при $n \rightarrow \infty$. В то же время $\log_2 m' \sim \log_2 n$. В итоге имеем

$$\mathbb{P}(\alpha(\mathcal{G}(G(n, r, s), 1/2)) \geq 2C_n^s (1 + o(1)) \log_2 n) \rightarrow 1, \quad n \rightarrow \infty,$$

и теорема 11 доказана.

4.4 Доказательство теоремы 12

Теорема 12, как и общая теорема 9, является следствием теоремы 6. Улучшение достигается за счет того, что здесь удастся уточнить турановскую оценку числа ребер в том или ином множестве вершин A , имеющем данную мощность $k > \alpha = \alpha(G(n, 2, 1)) = \lfloor \frac{n}{2} \rfloor$. Турановская оценка — это оценка величиной

$$(1 + o(1)) \frac{k^2}{2\alpha} \sim \frac{k^2}{n}.$$

Покажем, что имеет место оценка величиной $\frac{2k^2}{n} - k$.

Множество A — это подмножество множества \mathcal{R}_n . Для каждого элемента $i \in \mathcal{R}_n$ определим k_i как число вершин графа $G(n, 2, 1)$ — “двоек”, — принадлежащих A и содержащих i . Понятно, что при фиксированном i любые две отвечающих ему двойки образуют ребро в $G(n, 2, 1)$. Поэтому

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}| \geq \sum_{i=1}^n C_{k_i}^2.$$

В то же время $k_1 + \dots + k_n = 2k$. Нетрудно показать, что минимум выражения $\sum_{i=1}^n C_{k_i}^2$ в этих ограничениях достигается при $k_i = \frac{2k}{n}$, $i = 1, \dots, n$, откуда и следует оценка

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}| \geq \sum_{i=1}^n C_{k_i}^2 \geq \frac{2k^2}{n} - k.$$

С учетом этой оценки имеем

$$\begin{aligned} \sum_{A \subset V(n, 2), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, 2, 1) : \mathbf{x}, \mathbf{y} \in A\}|} &< C_{C_n^2}^k 2^{-(1+o(1))\frac{2k^2}{n}} < \left(\frac{eC_n^2}{k}\right)^k 2^{-(1+o(1))\frac{2k^2}{n}} < 2^k n^{2k} k^{-k} 2^{-(1+o(1))\frac{2k^2}{n}} = \\ &= 2^{2k \log_2 n - (1+o(1))k \log_2 k - (1+o(1))\frac{2k^2}{n}}. \end{aligned}$$

Следовательно, при подходящем $k \sim \frac{1}{2}n \log_2 n$ получаем

$$2 \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{2k}{n} < 0,$$

откуда

$$2k \log_2 n - (1 + o(1))k \log_2 k - (1 + o(1))\frac{2k^2}{n} = k \left(2 \log_2 n - (1 + o(1)) \log_2 k - (1 + o(1)) \frac{2k}{n} \right) \rightarrow -\infty,$$

и теорема 12 доказана.

4.5 Доказательство теоремы 13

Положим

$$k = \left\lceil C_{n-1}^{r-1} \left(1 + \frac{1}{\ln n} \right) \right\rceil.$$

Достаточно проверить, что с вероятностью, стремящейся к нулю, в случайном графе $\mathcal{G}(G(n, r, 0), 1/2)$ есть независимое множество вершин размера k . Эта вероятность заведомо не больше величины

$$\sum_{A \subset V(n, r), |A|=k} \mathbb{P}(A \text{ независимо в } \mathcal{G}(G(n, r, 0), 1/2)) = \sum_{A \subset V(n, r), |A|=k} 2^{-|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, r, 0) : \mathbf{x}, \mathbf{y} \in A\}|}.$$

Покажем, что и последняя сумма стремится к нулю.

Поскольку $k > C_{n-1}^{r-1}$, любое множество $A \subset V(n, r)$, $|A| = k$, не является независимым в $G(n, r, 0)$. Каждому такому множеству A сопоставим максимальное по мощности множество $B \subset A$, которое

независимо в $G(n, r, 0)$. Если максимальных множеств несколько, сопоставляем любое из них. Разумеется, $|B| \leq C_{n-1}^{r-1}$.

Возможны два варианта: либо для данного A выполнено $|B| \leq n^{r-1.1} = o(C_{n-1}^{r-1})$ (множество A — *первого типа*), либо для данного A выполнено $|B| > n^{r-1.1}$ (множество A — *второго типа*). Если A первого типа, то мы оценим величину

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, r, 0) : \mathbf{x}, \mathbf{y} \in A\}|$$

с помощью теоремы Турана:

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, r, 0) : \mathbf{x}, \mathbf{y} \in A\}| \geq (1 + o(1)) \frac{k^2}{2n^{r-1.1}}.$$

В интересующей нас сумме выделим слагаемые, для которых A первого типа. Их сумма не превосходит величины

$$C_{C_n}^k 2^{-(1+o(1))\frac{k^2}{2n^{r-1.1}}} < 3^k n^{rk} 2^{-(1+o(1))\frac{k^2}{2n^{r-1.1}}} = 3^k 2^{(1+o(1))r\frac{n^{r-1}}{(r-1)!} \log_2 n} 2^{-(1+o(1))\frac{n^{2r-2}}{2((r-1)!)^2 n^{r-1.1}}} \rightarrow 0.$$

Здесь мы пользуемся тем, что r — константа, а

$$n^{r-1} \log_2 n = o(n^{r-0.9}).$$

Пусть теперь A второго типа. Оценим число ребер графа $G(n, r, 0)$ в A . Поскольку B — *максимальное* независимое множество вершин графа $G(n, r, 0)$, содержащееся в A , для любой вершины $\mathbf{x} \in A \setminus B$ есть такая вершина $\mathbf{y} \in B$, что $\{\mathbf{x}, \mathbf{y}\} \in E(n, r, 0)$. Покажем, что вершина \mathbf{y} далеко не единственная с этим свойством. Действительно, вершины \mathbf{x} и \mathbf{y} соединены ребром, а значит, как r -элементные множества они не пересекаются. Оценим, сколько может быть вершин $\mathbf{z} \in B$, которые **не соединены** с \mathbf{x} . С одной стороны, они должны пересекаться с \mathbf{x} хотя бы по одному элементу. С другой стороны, так как B — независимое множество, они должны и с \mathbf{y} иметь непустое пересечение. Но \mathbf{x} и \mathbf{y} не пересекаются. Стало быть, таких вершин \mathbf{z} точно не больше, чем $r^2 n^{r-2}$. В текущей ситуации $|B| > n^{r-1.1}$. Следовательно, количество вершин из B , с которыми соединена данная вершина $\mathbf{x} \in A \setminus B$, не меньше, чем

$$|B| - r^2 n^{r-2} > n^{r-1.1} - r^2 n^{r-2} = (1 + o(1)) n^{r-1.1}.$$

Таким образом,

$$|\{\{\mathbf{x}, \mathbf{y}\} \in E(n, r, 0) : \mathbf{x}, \mathbf{y} \in A\}| \geq (|A| - |B|)(1 + o(1)) n^{r-1.1} \geq \frac{C_{n-1}^{r-1}}{\ln n} (1 + o(1)) n^{r-1.1} \sim \frac{n^{2r-2.1}}{(r-1)! \ln n},$$

т.е. сумма тех слагаемых, которые в интересующей нас сумме отвечают множествам A второго типа, не превосходит величины

$$C_{C_n}^k 2^{-(1+o(1))\frac{n^{2r-2.1}}{(r-1)! \ln n}} < 3^k n^{rk} 2^{-(1+o(1))\frac{n^{2r-2.1}}{(r-1)! \ln n}} = 3^k 2^{(1+o(1))r\frac{n^{r-1}}{(r-1)!} \log_2 n} 2^{-(1+o(1))\frac{n^{2r-2.1}}{(r-1)! \ln n}} \rightarrow 0.$$

Здесь мы пользуемся тем, что при $r > 1$ (т.е. $r \geq 2$) выполнено $2r - 2.1 > r - 1$.

Теорема 13 доказана.

Отметим, что выбор остаточного члена $C_{n-1}^{r-1}/\ln n$ совершенно произволен и отнюдь не оптимален.

5 Хроматическое число случайного графа $\mathcal{G}(G(n, r, s), 1/2)$

5.1 Формулировки результатов

Как и в параграфе 4.1, стоит сперва сказать о том, что известно относительно величины $\chi(G(n, r, s))$. Нижние оценки являются следствием верхних оценок числа независимости. Иными словами, при $r - s = a^l$, a — простое число, выполнены неравенства

$$\chi(G(n, r, s)) \geq \frac{C_n^r}{\alpha(G(n, r, s))} = \Omega(n^{s+1}), \quad r \geq 2s + 1,$$

$$\chi(G(n, r, s)) \geq \frac{C_n^r}{\alpha(G(n, r, s))} = \Omega(n^{r-s}), \quad r < 2s + 1.$$

Для получения верхних оценок известны два подхода. Во-первых, есть теорема Брукса (см. [25]), которая говорит, что $\chi(G) \leq \Delta + 1$, где Δ — максимальная степень вершины графа G . В нашем случае графы регулярны, т.е. все степени вершин в них одинаковы и равны $C_r^s C_{n-r}^{r-s} = \Theta(n^{r-s})$. Таким образом, $\chi(G(n, r, s)) = O(n^{r-s})$. Во-вторых, мы можем покрыть множество $V(n, r)$ независимыми множествами — цветами, — каждый из которых состоит из всех вершин, содержащих данное $(s+1)$ -элементное подмножество множества \mathcal{R}_n . Тогда, конечно, $\chi(G(n, r, s)) = O(n^{s+1})$. В итоге имеем во всех случаях, когда разность $r - s$ — это степень простого, порядок роста хроматического числа.

Случай $s = 0$ особый, поскольку здесь известно, что $\chi(G(n, r, 0)) = n - 2r + 2$, причем даже простоту числа $r = r - s$ требовать не нужно (см. [42]).

Для случайного графа нижние оценки хроматического числа — это исключительно следствия верхних оценок числа независимости, т.е. теоремы 9 и ее уточнений. С верхними оценками все интереснее. С одной стороны, есть совершенно общее утверждение, которое мы приводим в теореме 14.

Теорема 14. Пусть дана последовательность графов $G_n = (V_n, E_n)$, у которых $N := |V_n| \rightarrow \infty$, $n \rightarrow \infty$, и степень каждой вершины не превосходит величины $d = d(N)$, где функция d такова, что любая ее положительная степень растет быстрее величины $\ln N$. Тогда для любого $\varepsilon > 0$ с асимптотической вероятностью 1 имеем

$$\chi(\mathcal{G}(G_n, 1/2)) \leq (1 + \varepsilon) \frac{d}{\log_2 d}.$$

Теорема 14 — это своего рода теорема Брукса для случайных графов. Ее мы докажем в следующем параграфе. Для графов $G(n, r, s)$ она вполне годится, ведь $N = |V(n, r)| = C_n^r$, откуда $\ln N = \Theta(\ln n)$, тогда как $d = \Theta(n^{r-s})$, а стало быть, $\ln N = o(d^\beta)$, сколь бы близкой к нулю ни была константа $\beta > 0$. В итоге получаем

$$\chi(\mathcal{G}(G(n, r, s), 1/2)) \leq (1 + \varepsilon) \frac{C_r^s C_{n-r}^{r-s}}{(r-s) \log_2 n}.$$

Следствием из этого является теорема 10, которую мы в свое время не стали доказывать. Кроме того, теорема 14 означает, что при $r \leq 2s + 1$ и $r - s = a^l$, где a — простое число, найден порядок роста хроматического числа случайного графа. Ввиду результатов раздела 4 можно предположить, что при $r > 2s + 1$ картина будет иной. Например, можно, по-видимому, доказать, что $\chi(\mathcal{G}(G(n, r, 0), 1/2)) \sim n$ при $r > 1$ и $n \rightarrow \infty$. Однако пока в случае $r > 2s + 1$ мы имеем растущий зазор между верхними и нижними оценками хроматического числа случайного графа.

С другой стороны, как и в случае с теоремами 10 и 11, теорема 14 допускает уточнение при $r = 2s + 1$. К сожалению, с ростом s процедура получения этого уточнения становится крайне громоздкой. Суть процедуры будет ясна из доказательства следующей теоремы. Формулировать общий результат мы не станем.

Теорема 15. С асимптотической вероятностью 1 справедливо неравенство

$$\chi(\mathcal{G}(G(n, 5, 2), 1/2)) \leq \frac{8}{147} \cdot \frac{n^3}{\log_2 n}.$$

Теорема 15 сильнее теоремы 14, т.к. из теоремы 14 вытекает оценка с константой $\frac{5}{9}$. Теорему 15 мы докажем в параграфе 5.3. А в параграфе 5.4 мы дадим некоторые комментарии.

5.2 Доказательство теоремы 14

Пусть дан граф G_n . Занумеруем его вершины произвольно: $V_n = \{1, \dots, N\}$. Нам нужно показать, что с высокой вероятностью его подграф красится в не более $(1 + \varepsilon) \frac{d}{\log_2 d}$ цветов. Применим простейший жадный алгоритм раскраски: красим вершину 1 данного остовного подграфа H графа G_n в

первый цвет, а когда покрашены вершины $1, \dots, i-1$, красим вершину i либо в цвет с минимальным номером, такой, что в графе H нет ребер из вершины i в вершины этого цвета среди $\{1, \dots, i-1\}$, либо в новый цвет. Это стандартная идея (см., например, [45]).

Пусть C_k — событие, которое состоит в том, что при раскраске с помощью жадного алгоритма был использован цвет с номером k . Наша цель — показать, что при $k = \left\lceil (1 + \varepsilon) \frac{d}{\log_2 d} \right\rceil$ вероятность события C_k стремится к нулю. Понятно, что событие C_k вложено в объединение событий $C_{k,i}$, каждое из которых обозначает, что вершина i красится жадным алгоритмом в цвет с номером k .

Оценим, стало быть, вероятность события $C_{k,i}$. Для этого заметим, что цвет вершины i однозначно определяется раскраской уже рассмотренных вершин, и все пространство элементарных событий Ω , состоящее из всех остовных подграфов графа G_n , может быть разбито на события $D_{\varphi_1}, D_{\varphi_2}, \dots$, где событие D_{φ} — это множество тех остовных подграфов графа G_n , для которых вершины среди $\{1, 2, \dots, i-1\}$ имеют раскраску φ в результате применения нашего жадного алгоритма. Запишем

$$\mathbb{P}(C_{k,i}) = \mathbb{P}(C_{k,i} \cap \Omega) = \mathbb{P}\left(C_{k,i} \cap \left(\bigcup_{\varphi} D_{\varphi}\right)\right) \leq \sum_{\varphi} \mathbb{P}(C_{k,i} \cap D_{\varphi}).$$

Раскраска φ однозначно определяет множества вершин $\gamma_1, \gamma_2, \dots$: множество γ_j содержит те вершины графа G_n среди $\{1, \dots, i-1\}$, которые смежны с вершиной i и имеют в раскраске φ цвет j .

Рассмотрим событие $C_{k,i} \cap D_{\varphi}$. Так как оно вложено в $C_{k,i}$, то это значит, что вершина i не может быть раскрашена ни в один из цветов $1, 2, \dots, k-1$. Это равносильно тому, что из вершины i идет хотя бы одно ребро в каждое из множеств $\gamma_1, \gamma_2, \dots, \gamma_{k-1}$. Обозначим $E_{\varphi,j}$ событие, состоящее в том, что из вершины i идет хотя бы одно ребро в множество γ_j . Тогда

$$C_{k,i} \cap D_{\varphi} \subseteq D_{\varphi} \cap \left(\bigcap_{j=1}^{k-1} E_{\varphi,j}\right).$$

В силу того, что множества γ_j не пересекаются между собой, события $E_{\varphi,j}$ являются независимыми. Более того, событие D_{φ} целиком определяется ребрами, оба конца которых принадлежат множеству $\{1, \dots, i-1\}$, а в каждом из событий $E_{\varphi,j}$ принимают участие только ребра, инцидентные i . Стало быть, события D_{φ} и $E_{\varphi,j}$ также независимы, и окончательно имеем

$$\begin{aligned} \mathbb{P}(C_{k,i} \cap D_{\varphi}) &\leq \mathbb{P}(D_{\varphi}) \prod_{j=1}^{k-1} \mathbb{P}(E_{\varphi,j}), \\ \mathbb{P}(C_{k,i}) &\leq \sum_{\varphi} \mathbb{P}(C_{k,i} \cap D_{\varphi}) \leq \sum_{\varphi} \left(\mathbb{P}(D_{\varphi}) \prod_{j=1}^{k-1} \mathbb{P}(E_{\varphi,j}) \right). \end{aligned}$$

Так как события D_{φ} являются попарно несовместными, то

$$\mathbb{P}(C_{k,i}) \leq \sum_{\varphi} \left(\mathbb{P}(D_{\varphi}) \prod_{j=1}^{k-1} \mathbb{P}(E_{\varphi,j}) \right) \leq \max_{\varphi} \left(\prod_{j=1}^{k-1} \mathbb{P}(E_{\varphi,j}) \right).$$

Степень вершины i не превосходит d по условию теоремы. Следовательно, непересекающиеся множества $\gamma_1, \gamma_2, \dots, \gamma_{k-1}$ имеют суммарный размер, не превосходящий d . Поэтому количество тех множеств γ_j , размер которых превышает $\gamma \log_2 d$ с данным $\gamma > 0$, не превосходит величины $m = \left\lceil \frac{d}{\gamma \log_2 d} \right\rceil$. Стало быть, каждое из оставшихся $l = k - m$ множеств имеет размер, не превосходящий $\gamma \log_2 d$. Будем считать, что эти множества имеют номера j_1, j_2, \dots, j_l . Таким образом, для любой раскраски φ выполнено

$$\prod_{j=1}^{k-1} \mathbb{P}(E_{\varphi,j}) = \prod_{j \in \{1, 2, \dots, k-1\}} \mathbb{P}(E_{\varphi,j}) \leq \prod_{j \in \{j_1, j_2, \dots, j_l\}} \mathbb{P}(E_{\varphi,j}).$$

Оценим вероятность события $E_{\varphi,j}$, если j находится в множестве $\{j_1, j_2, \dots, j_l\}$. Напомним, это вероятность того, что вершина i соединена хотя бы с одной вершиной из множества γ_j . В силу выбора цветов j_1, j_2, \dots, j_l , ее можно оценить как

$$\mathbb{P}(E_{\varphi,j}) = 1 - 2^{-|\gamma_j|} \leq 1 - 2^{-\gamma \log_2 d} = 1 - d^{-\gamma}.$$

Значит,

$$\begin{aligned} \prod_{j \in \{j_1, j_2, \dots, j_l\}} \mathbb{P}(E_{\varphi,j}) &\leq (1 - d^{-\gamma})^l, \\ \mathbb{P}(C_{k,i}) &\leq \max_{\varphi} \left(\prod_{j=1}^{k-1} \mathbb{P}(E_{\varphi,j}) \right) \leq (1 - d^{-\gamma})^l, \\ \mathbb{P}(C_k) &\leq \sum_{i=1}^N \mathbb{P}(C_{k,i}) \leq N(1 - d^{-\gamma})^l. \end{aligned}$$

Так как d неограниченно растет с ростом N , то $d^{-\gamma}$ стремится к нулю, и, воспользовавшись неравенством $\ln(1 - x) \leq -x$ при $x \in (0, 1)$, имеем

$$\mathbb{P}(C_k) \leq \exp(\ln N - d^{-\gamma} l) \leq \exp\left(\ln N - d^{-\gamma} \left(k - \frac{d}{\gamma \log_2 d}\right)\right).$$

Напомним, наконец, что

$$k = \left\lfloor (1 + \varepsilon) \frac{d}{\log_2 d} \right\rfloor \sim (1 + \varepsilon) \frac{d}{\log_2 d}, \quad n \rightarrow \infty.$$

Следовательно, при любом $\gamma \in (\frac{1}{1+\varepsilon}, 1)$ искомую вероятность можно переписать в виде

$$\mathbb{P}(C_k) \leq \exp\left(\ln N - \left((1 + \varepsilon)(1 + o(1)) - \frac{1}{\gamma}\right) \frac{d^{1-\gamma}}{\log_2 d}\right).$$

В показателе последней экспоненты из величины $\ln N$ вычитается функция, растущая как некоторая положительная степень d . По условию теоремы разность стремится к $-\infty$, и теорема 14 доказана.

5.3 Доказательство теоремы 15

В доказательстве будет использована конструкция, весьма близкая к той, которая имела место в параграфе 3.2. Поэтому ниже мы будем часто ссылаться на тот параграф, а также опускать некоторые технические детали, коль скоро их легко будет восстановить по аналогии с теми или иными выкладками, подробно проведенными в параграфе 3.2.

Вершины графа $G(n, 5, 2)$ суть пятиэлементные подмножества множества $\mathcal{R}_n = \{1, \dots, n\}$ — “пятерки”. Разобьем их на слои, как это было сделано в параграфе 3.2. Опишем построение первого слоя \mathcal{S}_1 . Для этого разделим n на 24 с остатком: $n = 24s_1 + t_1$, $t_1 \leq 23$. В чем смысл такого, на первый взгляд, странного деления, станет ясно чуть позже.

Положим $L_1 = \mathcal{R}_{12s_1}$, $R_1 = \{12s_1 + 1, \dots, 24s_1\}$, $T_1 = \{24s_1 + 1, \dots, n\}$. Как и в параграфе 3.2, это левая половинка, правая половинка и довесок. Сохраняя обозначения того параграфа, назовем \mathcal{C}_1 множество пятерок, имеющих непустые пересечения с довеском T_1 . В слой же \mathcal{S}_1 отправим все пятерки, которые не лежат целиком ни в одной из половинок (ср. §3.2). Хочется слой разбить на блоки из клик, между которыми нет ребер. Здесь есть два существенно разных случая: пятерка из \mathcal{S}_1 разбивается половинками L_1, R_1 на “тройку” и “двушку”; пятерка из \mathcal{S}_1 разбивается половинками L_1, R_1 на “четверку” и “однушку”. Мы можем считать, что в первом случае тройка находится в L_1 , а во втором случае в L_1 расположена четверка. Если мы найдем количество покрывающих блоков в таком предположении, то итоговое число блоков будет просто вдвое большим. Первый случай проще.

Случай 1. Назовем *совершенным тройкосочетанием* в левой половине любое ее разбиение на непересекающиеся тройки. Такие разбиения существуют, поскольку величина $|L_1| = 12s_1$ делится на 3 (это одна из причин выбора параметра 24). Классическая теорема Бараньяи (см. [46]) утверждает, что множество всех троек в L_1 разбивается на непересекающиеся совершенные тройкосочетания. Общее число этих тройкосочетаний равно $\frac{C_{12s_1}^3}{4s_1} \sim 72s_1^2$ (асимптотика понимается при $n \rightarrow \infty$). Один блок — это фиксированное тройкосочетание, к каждой тройке которого сперва добавлена одна двушка из R_1 (образуется одна клика в графе $G(n, 5, 2)$), потом добавлена вторая двушка из R_1 (образуется еще одна клика в графе $G(n, 5, 2)$), и так далее, пока не закончатся двушки, а вместе с ними и клики блока. Итого имеем $(1 + o(1))72s_1^2$ блоков, состоящих из $C_{12s_1}^2$ клик размера $4s_1$. Между кликами внутри блока нет ребер, т.к. пятерки из разных клик имеют либо меньше двух элементов в пересечении (если отвечающие им тройки в L_1 не пересекаются), либо не меньше трех общих элементов (если отвечающие им тройки совпадают). Очевидно также, что блоками исчерпаны все пятерки в рамках случая.

Если сразу перейти к случайному графу, то с высокой вероятностью число цветов в оптимальной раскраске каждого блока не превзойдет величины $\frac{4s_1}{2 \log_2(4s_1)}$, откуда следует, что общее число цветов не больше

$$(1 + o(1))72s_1^2 \cdot \frac{4s_1}{2 \log_2(4s_1)} \sim \frac{144s_1^3}{\log_2 s_1}.$$

Смысл выражения *высокая вероятность* раскрывается в деталях в параграфе 3.2, и здесь никаких отличий по сути не возникает.

Остается домножить оценку числа цветов на 2 за счет симметричного случая. Однако есть еще Случай 2, который хуже и к рассмотрению которого мы сейчас перейдем.

Случай 2. Здесь сложнее образовать блоки. Чтобы построить нечто подобное конструкции из Случая 1, разобьем левую половину L_1 на две “четвертинки” LL_1 и LR_1 — левую и правую. Это можно сделать, т.к. $12s_1$ делится на 2, и это еще одна (не последняя) причина выбора параметра 24. Таким образом, $|LL_1| = |LR_1| = 6s_1$. Как могут располагаться интересующие нас четверки внутри L_1 ? Они могут пересекаться с LL_1 по тройке и с LR_1 по однушке (плюс симметричная ситуация), могут цеплять каждую из четвертинок по двушке (здесь только одна ситуация), а могут целиком попасть в LL_1 (плюс симметричная ситуация). Попробуем оценить число цветов в каждом из подслучаев.

Подслучай 2.1. Предполагаем, что в левой четвертинке находятся тройки, а в правой — однушки. Поскольку мощность левой четвертинки делится на 3 (очередное пояснение к выбору параметра 24), снова применима теорема Бараньяи, утверждающая, что можно разбить множество всех троек в LL_1 на непересекающиеся совершенные тройкосочетания. Их будет $\frac{C_{6s_1}^3}{2s_1} \sim 18s_1^2$. Фиксируем тройкосочетание и добавляем к каждой тройке в нем любую однушку из LR_1 и любую однушку из R_1 . Образуется клика. Всего для данного тройкосочетания таких клик $6s_1 \cdot 12s_1 = 72s_1^2$. Впрочем, их количество для нас не так важно. Важнее то, что вместе они опять создают блок (между ними нет ребер) и что количество блоков есть $(1 + o(1))18s_1^2$.

Если сразу перейти к случайному графу, то с высокой вероятностью число цветов в оптимальной раскраске каждого блока не превзойдет величины $\frac{2s_1}{2 \log_2(2s_1)}$, откуда следует, что общее число цветов не больше

$$(1 + o(1))18s_1^2 \cdot \frac{2s_1}{2 \log_2(2s_1)} \sim \frac{18s_1^3}{\log_2 s_1}.$$

И столько же цветов в симметричной ситуации.

Подслучай 2.2. Предполагаем, что в обеих четвертинках находятся двушки. Поскольку мощность левой четвертинки делится на 2 (окончательное пояснение к выбору параметра 24), можно разбить множество всех двушек в LL_1 на непересекающиеся совершенные паросочетания. Их будет $\frac{C_{6s_1}^2}{3s_1} \sim 6s_1$. Фиксируем произвольное паросочетание и любую нумерацию пар (двушек) в нем.

К первой двушке добавим первый элемент правой половинки R_1 (именно половинки). Ко второй двушке добавим второй элемент из R_1 . И так далее. Всего будет использовано $3s_1$ элементов правой половинки (а их там $12s_1$). Образуется набор из $3s_1$ непересекающихся троек (тройкосочетание). К каждой тройке этого набора добавим в свою очередь произвольную двушку из правой четвертинки (теперь именно из четвертинки). Получится клика. Для данного паросочетания в LL_1 таких клик $C_{6s_1}^2$, и они формируют блок. Число различных блоков есть $(1 + o(1))6s_1$. Но они не исчерпывают все пятерки в рамках текущего подслучая, ведь мы задействовали не все элементы в R_1 . Мы можем исправить этот пробел следующим образом. Раньше мы добавляли к последовательным двушкам из фиксированного паросочетания первые $3s_1$ однушек из правой половинки, т.е. однушки $\{12s_1 + 1\}, \dots, \{15s_1\}$. Теперь сделаем то же самое с однушками $\{12s_1 + 2\}, \dots, \{15s_1 + 1\}$, затем — с однушками $\{12s_1 + 3\}, \dots, \{15s_1 + 2\}$, и так далее вплоть до $\{24s_1\}, \dots, \{15s_1 - 1\}$. В каждой из этих $12s_1$ конструкций есть $(1 + o(1))6s_1$ блоков, а значит, всего блоков $(1 + o(1))72s_1^2$, и они уже покрывают все наши пятерки.

Если сразу перейти к случайному графу, то с высокой вероятностью число цветов в оптимальной раскраске каждого блока не превзойдет величины $\frac{3s_1}{2\log_2(3s_1)}$, откуда следует, что общее число цветов не больше

$$(1 + o(1))72s_1^2 \cdot \frac{3s_1}{2\log_2(3s_1)} \sim \frac{108s_1^3}{\log_2 s_1}.$$

И тут симметричной ситуации нет.

Подведем промежуточные итоги в рамках Случая 2. Мы уже использовали

$$2(1 + o(1))\frac{18s_1^3}{\log_2 s_1} + (1 + o(1))\frac{108s_1^3}{\log_2 s_1} = (1 + o(1))\frac{144s_1^3}{\log_2 s_1}$$

цветов. Но остается подслучай, в котором четверки целиком лежат в LL_1 (и симметричная ситуация²). Видно, что этот подслучай крайне похож на весь Случай 2, только в Случае 2 мы знали лишь, что четверки локализованы в левой половинке, а теперь мы их загнали в левую четвертинку. Если бы размер левой четвертинки делился на 12, то мы проделали бы с ней абсолютно ту же процедуру, что и в подслучаях 2.1, 2.2, и загнали бы недорассмотренные четверки в левую “осьмушку”. И делали бы мы так порядка $\log_2 \log_2 n$ шагов (ср. рассуждение в параграфе 3.2), чтобы на каждом шаге все еще корректно было говорить о “высокой вероятности” и чтобы недорассмотренные четверки локализовались в множестве, имеющем мощность s порядка $\frac{n}{\log_2 n}$. Сколько бы цветов получилось тогда? Очевидно, что число цветов на шаге с номером i асимптотически равно

$$\frac{1}{8^{i-1}} \left(2 \frac{18s_1^3}{\log_2 s_1} \right) + \frac{1}{4^{i-1}} \left(\frac{108s_1^3}{\log_2 s_1} \right).$$

Здесь важно, что $s_1 = \Theta(n)$ и что при любом из наших i выполнено $\log_2 \left(\frac{s_1}{2^i} \right) \sim \log_2 s_1$ при $n \rightarrow \infty$.

В сумме имеем не больше

$$\begin{aligned} (1 + o(1))\frac{8}{7} \left(2 \frac{18s_1^3}{\log_2 s_1} \right) + (1 + o(1))\frac{4}{3} \left(\frac{108s_1^3}{\log_2 s_1} \right) &\sim \frac{36 \cdot 8 \cdot 3 + 108 \cdot 4 \cdot 7}{7 \cdot 3} \cdot \frac{s_1^3}{\log_2 s_1} = \\ &= \frac{36 \cdot 108}{7 \cdot 3} \cdot \frac{s_1^3}{\log_2 s_1} = \frac{1296}{7} \cdot \frac{s_1^3}{\log_2 s_1}. \end{aligned}$$

Пятерки, оставшиеся недокрашенными, образованы четверками из множества мощности s и однушками из правой половинки. Их можно тривиально покрасить в C_s^3 цветов (даже минуя случайность), но

$$C_s^3 = \Theta(s^3) = \Theta\left(\frac{n^3}{\log_2^3 n}\right),$$

и это пренебрежимо мало по сравнению с ожидаемой оценкой.

²Замечательно то, что четверки из двух симметричных ситуаций не пересекаются, а потому соответствующие пятерки не образуют ребер и про вторую ситуацию можно забыть.

Однако размер левой четвертинки не делится на 12. Поэтому нужно делить с остатком и аккуратно рассматривать возникающие довески. Если четверки уже локализованы в множестве A какой-то мощности s , а довесок T имеет размер $t \leq 11$, то нас беспокоят четверки, имеющие непустые пересечения с довеском, а они образуют пятерки (вместе с однушками из правой половинки), которые легко покрасить в $\Theta(s^2)$ цветов (фиксируя произвольную двушку в $A \setminus T$ и любую однушку из T). Оценивая, как обычно, суммой геометрической прогрессии, получаем $\Theta(n^2)$ цветов, что не значимо.

Таким образом, рассмотрение Случая 2 завершено. В сумме по двум случаям (и им симметричным) получаем следующее число цветов:

$$(1 + o(1)) \frac{144 \cdot 2 \cdot 7 + 1296 \cdot 2}{7} \cdot \frac{s_1^3}{\log_2 s_1} = (1 + o(1)) \frac{4608}{7} \cdot \frac{s_1^3}{\log_2 s_1}.$$

И это мы только разобрались с *первым слоем* \mathcal{S}_1 . Но дальше все стандартно. Строим второй слой внутри левой половинки и не забываем про новый довесок. Все размеры уменьшаются вдвое, поэтому оценка числа цветов уменьшается асимптотически в 8 раз. В правой половинке берем те же цвета, что и в левой. И так сжимаем все, покуда не останется множество, мощность которого имеет порядок $\frac{n}{\log_2 n}$. Пятерки в нем красятся даже без учета случайности в $\Theta\left(\frac{n^3}{\log_2^3 n}\right)$ цветов, что пренебрежимо мало. При этом на каждом шаге $\log_2\left(\frac{s_1}{2}\right) \sim \log_2 s_1 \sim \log_2 n$ при $n \rightarrow \infty$. Значит, применима обычная оценка геометрической прогрессией, дающая окончательно такое число цветов:

$$(1 + o(1)) \frac{8}{7} \cdot \frac{4608}{7} \cdot \frac{s_1^3}{\log_2 s_1} \sim \frac{8}{7} \cdot \frac{4608}{7} \cdot \frac{1}{24^3} \cdot \frac{n^3}{\log_2 n} = \frac{8}{147} \cdot \frac{n^3}{\log_2 n}.$$

Наконец, отметим, что все пятерки, пересекающиеся с довесками, (в частности, пятерки из множества C_1 и т.д.) красятся в $\Theta(n^2)$ цветов, и теорема доказана.

5.4 Некоторые комментарии

Видно, что зазоры в оценках чисел независимости и хроматических чисел наших случайных графов растут с ростом r и s . По-видимому, это свидетельствует о том, что наши методы хороши лишь при постоянных r, s , и ниже мы попробуем продемонстрировать это.

По существу методов у нас 2. С одной стороны, есть оценки, вытекающие из вероятностного аналога теоремы Брукса (теоремы 10 и 14). С другой стороны, есть оценки, получаемые с помощью блоков из клик. Попробуем применить каждый из этих методов в случае, когда $r = \frac{n}{2}$, $s = \frac{n}{4}$. Как мы уже отмечали в параграфе 4.1, в этом случае кликами в графе $G(n, r, s)$ являются матрицы Адамара. Их размер, стало быть, точно не выше n , и до сих пор не доказана гипотеза о том, что при всех n , делящихся на 4, существует клика размера n .

Обсудим сперва метод с блоками из клик. Здесь проще комментировать оценки чисел независимости. Допустим, гипотеза Адамара верна и существуют клики на n вершинах. Предположим далее, что из этих клик удалось сложить большой блок. Это звучит почти беспомощно: сейчас нет никакого способа найти такой блок, ведь и сами клики-то мы не всегда искать умеем. Но представим себе, что способ найден. Все равно у нас сейчас есть только метод с блоками. Какого тогда размера может быть пресловутый блок? Поскольку в блоках по определению между разными кликами ребер нет, разумеется, клик в блоке точно не больше, чем $\alpha(G(n, r, s))$. Хорошо, пусть их ровно $\alpha(G(n, r, s))$. Повторимся: такого скорее всего не бывает, но нам же хочется понять границы применимости нашего метода, и мы пытаемся работать поэтому в идеальной ситуации. Итак, найден блок, состоящий из $\alpha(G(n, r, s))$ клик размера n . Даже такое “чудо” дает нам с высокой вероятностью наличие в случайном графе независимого множества мощности $2(1 + o(1))\alpha(G(n, r, s)) \log_2 n$. Ничего лучшего мы на этом пути не добьемся. Это “идеальная” нижняя оценка в рамках метода.

С другой стороны, результаты типа теорем 6 и 9 гарантируют лишь оценки сверху величинами порядка $\alpha(G(n, r, s)) \log_2 |V(n, r)|$ (ср. замечание, сделанное сразу после формулировки теоремы 5, а также тот факт, что в теореме 9 величина $2r \log_2 n$ как раз практически равна логарифму от $|V(n, r)| = C_n^r \sim \frac{n^r}{r!}$; нетрудно проверить, что этот факт всегда имеет место).

Что же мы имеем в итоге? А имеем мы неустранимый в рамках метода растущий зазор между оценками. Действительно, если при постоянном r логарифм величины $|V(n, r)|$ (см. выше) имел тот же порядок роста, что и функция $\log_2 n$, то при $r = \frac{n}{2}$ справедливо равенство $|V(n, r)| = (2 + o(1))^n$, откуда $\log_2 |V(n, r)| \sim n$, и это значительно больше, чем $\log_2 n$.

Теперь поговорим о методе со степенями вершин. Тут несколько легче давать комментарии по оценкам хроматических чисел. При нынешних параметрах величина d задается формулой $d = \left(C_{n/2}^{n/4}\right)^2$, т.е. $d = (2 + o(1))^n$ и $\frac{d}{\log_2 d} = (2 + o(1))^n$. Но очевидно, что $\chi(\mathcal{G}(G(n, r, s), 1/2)) \leq \chi(G(n, r, s))$. Последняя величина оценивалась в работах [47]–[49], и, грубо говоря,

$$\chi(G(n, n/2, n/4)) \leq (1.139 \dots + o(1))^n.$$

Иными словами, разница между тривиальной оценкой и оценкой типа Брукса катастрофическая.

6 Несколько слов о произвольной вероятности ребра p

В этом разделе мы лишь опишем общую ситуацию, которую мы имеем при произвольной вероятности ребра p . Мы не станем пытаться давать максимально точные формулировки результатов, поскольку, как будет видно из нижеследующей дискуссии, это чисто техническая задача: можно закопаться в тяжелых выкладках, не предложив при этом никаких новых идей. Соответственно, мы постараемся выделить только качественно значимые моменты.

Прежде всего положим $q = \frac{1}{1-p}$. При $p = \frac{1}{2}$ имеем $q = 2$. Какие у нас были общие результаты? Была теорема 6 о верхней оценке числа независимости, и она уже была сформулирована с произвольным p . Все верхние оценки чисел независимости при конкретных r, s (теоремы 4, 9, 12, 13) получались так или иначе из нее. Из доказательств теорем 4, 9, 12 сразу видно, например, что если $pn \rightarrow \infty$ при $n \rightarrow \infty$ (функция p стремится к нулю не слишком быстро или вовсе к нулю не стремится) и $p \leq c < 1$, где c — константа, то в утверждениях этих теорем нужно буквально заменить двоичный логарифм логарифмом по основанию q . И это отлично коррелирует с теоремой 3. Для получения аналога теоремы 13 ограничение на p придется немного усилить: при некотором $\beta \in (0, 1)$ должно быть $pn^\beta \rightarrow \infty$, но суть снова не меняется.

Далее, были теоремы 10 и 14 — аналоги теоремы Брукса. Там тоже меняется только двойка в основании логарифма на все ту же величину q .

Наконец, был ряд теорем “блочного типа”. Разумеется, и в них (за счет теоремы 3) меняется только основание логарифма. Однако здесь-то и содержится основная техническая загвоздка. Ранее мы всякий раз применяли явную экспоненциальную оценку вероятности в теореме 3, и ее нам при $p = \frac{1}{2}$ хватало с огромным запасом. Если мы попытаемся сделать аналогичную выкладку при других p , то мы столкнемся с массой трудностей. Во-первых, надо будет вытаскивать из статьи [22] максимально аккуратные оценки вероятностей. Там они не указаны, и на сей предмет есть множество разного рода результатов. Например, можно ухудшать оценки из теоремы 3, улучшая при этом оценки вероятностей. И на этом пути получатся десятки результатов, смысл явного отыскания которых не вполне ясен. Во-вторых, в теоремах о хроматических числах при раскраске по слоям нужно будет очень аккуратно считать количество клик в каждом слое, и это совершенно неинтересная задача.

В конечном счете результаты блочных теорем заведомо верны (с заменой основания логарифма), коль скоро p стремится к нулю медленнее любого многочлена от n или вовсе имеет порядок константы, отделенной от единицы. Просто в этом случае из работы [22] следует, что вероятности в теореме 3 оцениваются функцией вида $1 - f(n)$, где $f(n)$ стремится к нулю быстрее любого полинома, а в то же время очевидно, что количество клик $g(n)$ в блочной конструкции полиномиально по n , откуда $(1 - f(n))^{g(n)} \rightarrow 1$ при $n \rightarrow \infty$.

Другие случаи мы здесь рассматривать не станем.

Бывают, впрочем, совсем маленькие вероятности ребра: например, $p = o\left(\frac{1}{n}\right)$. При таких p с высокой вероятностью от каждой отдельной клики в каждом блоке остается лес, который красится в 2 цвета. Здесь также вопрос об общем числе цветов упирается в чисто техническую задачу о том, при каких условиях некоторые выражения вида $(1 - f(n))^{g(n)}$ стремятся к единице. Конечно,

исследования такого рода могут привести и к возникновению других, более содержательных, идей. Но в настоящей работе мы не будем углубляться в эту проблематику.

7 Об одной задаче теории Рамсея

7.1 Постановка задачи

Одной из классических задач теории Рамсея является задача об отыскании *чисел Рамсея*. В частности, изучается число $R(k)$, равное наименьшему натуральному n , при котором любой граф на n вершинах либо содержит k -клик, либо содержит независимое множество вершин мощности k . В обозначениях параграфа 2.3

$$R(k) = \min\{n : \forall G = (V, E), |V| = n, \text{ либо } \omega(G) \geq k, \text{ либо } \alpha(G) \geq k\}.$$

Для наших дальнейших целей важны не столько результаты, в разное время полученные для величины $R(k)$, сколько мотивировки более общей постановки вопроса. Поэтому заинтересованного читателя мы отошлем к обзорам и книгам [3], [4], [18], [26], а сами займемся переформулировкой классического определения, которая в итоге и приведет нас к естественному обобщению. Итак, во-первых, наличие в графе G независимого множества равносильно наличию клики в его дополнении до полного графа, обозначаемом \overline{G} . Во-вторых, клика и только клика является индуцированным подграфом полного графа. В третьих, “любой граф на n вершинах” — это то же, что и “любой остовный подграф полного графа K_n ”. В результате мы приходим к такому определению:

$$R(k) = \min\{n : \text{для любого остовного подграфа } G \text{ полного графа } K_n \text{ либо в } G, \text{ либо в } \overline{G}$$

есть подграф на k вершинах, являющийся индуцированным подграфом в $K_n\}$.

Теперь перейдем к обобщению. Пусть, как и в параграфе 1.2, дана последовательность графов $H_n = (V_n, E_n)$, в которой $|V_n| \rightarrow \infty$ при $n \rightarrow \infty$. Обозначим N мощность множества V_n , т.е. N — это растущая функция аргумента n . Пусть G — остовный подграф H_n . Обозначим $H_n \setminus G$ его дополнение до H_n . Например, если $G = H_n$, то $H_n \setminus G$ — это граф на N вершинах без ребер (независимое множество). А если $H_n = K_n$, то $H_n \setminus G = \overline{G}$. Положим

$$R(\{H_n\}, k) = \min\{N : \text{существует такое } n, \text{ что } N = N(n)$$

и для любого остовного подграфа G графа H_n либо в G , либо в

$H_n \setminus G$ есть подграф на k вершинах, являющийся индуцированным подграфом в $H_n\}$.

Заметим, что у H_n вполне могут быть и независимые множества большого размера, а каждое из них, конечно, является индуцированным подграфом H_n . Поэтому разница между классической величиной $R(k) = R(\{K_n\}, k)$ и величиной $R(\{H_n\}, k)$ может быть весьма существенной. Подчеркнем, что для данной последовательности графов $\{H_n\}$ число Рамсея $R(\{H_n\}, k)$ — это функция одного аргумента k . От n эта функция не зависит.

В работе [50] аккуратно изучена величина $R(\{G(n, n/2, n/4)\}, k)$. Однако там не найдено точных по порядку оценок. Оказывается, оценки величин $R(\{G(n, r, s)\}, k)$ тесно связаны с исследованиями, которые мы провели в предшествующих разделах, и в тех случаях, когда нам удалось найти близкие верхние и нижние оценки для $\alpha(\mathcal{G}(G(n, r, s), 1/2))$, удастся найти и близкие оценки для $R(\{G(n, r, s)\}, k)$. Соответствующие результаты мы приведем в следующем параграфе, а докажем мы их в параграфе 7.3.

7.2 Формулировки результатов

Поговорим сперва о верхних оценках. Имеет место весьма общий результат.

Теорема 16. Пусть дана некоторая последовательность графов $H_n = (V_n, E_n)$, в которой $|V_n| \rightarrow \infty$ при $n \rightarrow \infty$ (рост монотонный). Положим $N(n) = |V_n|$. Положим

$$m(k) = \min\{n : \alpha(H_n) \geq k\}.$$

Тогда

$$R(\{H_n\}, k) \leq N(m(k)).$$

Разумеется, для $\{H_n\} = \{K_n\}$ теорема 16 не применима, ведь $\alpha(K_n) = 1$. Однако, как мы увидим ниже, для графов $G(n, r, s)$ теорема 16 дает вполне адекватные следствия. Пока сформулируем столь же общий результат о нижних оценках числа Рамсея.

Теорема 17. Пусть дана некоторая последовательность графов $H_n = (V_n, E_n)$, в которой $|V_n| \rightarrow \infty$ при $n \rightarrow \infty$ (рост монотонный). Положим $N(n) = |V_n|$. Пусть $t = t(n)$ — это минимальное число, с которым для функции

$$f_n(t) = 2 \sum_{A \subset V_n, |A|=t} 2^{-|\{\mathbf{x}, \mathbf{y}\} \in E_n : \mathbf{x}, \mathbf{y} \in A\}|}$$

выполнено неравенство $f_n(t) < 1$. Предположим, мы знаем некоторую оценку $t(n) \leq t'(n)$ (в частности, вполне может быть, что $t'(n) \equiv t(n)$), причем начиная с некоторого n , последовательность $t'(n)$ строго монотонно возрастает и существует такое n_0 , что для любого $n \geq n_0$, для каждого $t'' \geq t'(n)$ также выполнено неравенство $f_n(t'') < 1$. Пусть

$$m(k) = \max\{n : t'(n) < k\}.$$

Тогда при достаточно больших k выполнено

$$R(\{H_n\}, k) \geq N(m(k)).$$

Теорема 16 тривиальна, но мы докажем ее в первом пункте следующего параграфа. Теорему 17 мы докажем в п. 7.3.2.

Приведем следствия из теорем 16, 17 для графов $G(n, r, s)$. Всякий раз будем предполагать, что $r - s$ — степень простого числа.

Следствие 1. Пусть $r \geq 2s + 1$. Тогда

$$R(\{G(n, r, s)\}, k) \geq (1 + o(1)) \cdot \left(\frac{k}{\log_2 k}\right)^{\frac{r}{r-s-1}} \cdot \frac{1}{r!} \cdot \left(\frac{(r-s-1)!(r-s-1)}{2(s+1)}\right)^{\frac{r}{r-s-1}},$$

$$R(\{G(n, r, s)\}, k) \leq (1 + o(1)) \cdot k^{\frac{r}{r-s-1}} \cdot \frac{1}{r!} \cdot ((r-s-1)!)^{\frac{r}{r-s-1}}.$$

Следствие 2. Пусть $r < 2s + 1$. Тогда

$$R(\{G(n, r, s)\}, k) \geq (1 + o(1)) \cdot \left(\frac{k}{\log_2 k}\right)^{\frac{r}{s}} \cdot \frac{1}{r!} \cdot \left(\frac{s(2s-r+1)!(r-s-1)!C_r^{2s-r+1}}{2(r-s)}\right)^{\frac{r}{s}},$$

$$R(\{G(n, r, s)\}, k) \leq (1 + o(1)) \cdot k^{\frac{r}{s}} \cdot \frac{1}{r!} \cdot (s!C_r^s)^{\frac{r}{s}}.$$

Следствие 3. Выполнены неравенства

$$R(\{G(n, 2, 1)\}, k) \geq (1 + o(1)) \cdot \left(\frac{2k}{\log_2 k}\right)^2 \cdot \frac{1}{2},$$

$$R(\{G(n, 2, 1)\}, k) \leq (1 + o(1)) \cdot 2 \cdot k^2.$$

Следствие 4. Пусть $r > 1$. Тогда

$$R(\{G(n, r, 0)\}, k) \sim \frac{1}{r!} \cdot (k(r-1)!)^{\frac{r}{r-1}}.$$

В п. 7.3.3 мы докажем следствия. Уже сейчас видно, что в следствиях 1–3 есть логарифмический зазор между оценками. Однако по k порядок роста числа Рамсея найден. Далее, параметры следствия 3 удовлетворяют условиям следствия 2, и, более того, верхняя оценка в следствии 3 является спецификацией верхней оценки из следствия 2. Разница в нижних оценках. Оценка в следствии 3 в 4 раза больше. И только в следствии 4 найдена асимптотика числа Рамсея.

Оказывается, при $r = 2s + 1$ можно устранить логарифмический зазор.

Теорема 18. Выполнено неравенство

$$R(\{G(n, 2s + 1, s)\}, k) \leq (1 + o(1)) \cdot \left(\frac{k}{\log_2 k} \right)^{\frac{r}{s}} \cdot \frac{1}{r!} \cdot (s \cdot s!)^{\frac{r}{s}}.$$

Теорему 18 мы докажем в п. 7.3.4. Подчеркнем, что в ее условиях $\frac{r}{r-s-1} = \frac{r}{s}$, и это как раз означает устранение зазора.

7.3 Доказательства результатов

7.3.1 Доказательство теоремы 16

По условию $\alpha(H_{m(k)}) \geq k$, т.е. в любом остовном подграфе графа $H_{m(k)}$ есть подграф на k вершинах, образующий независимое множество и являющийся, тем самым, индуцированным подграфом графа $H_{m(k)}$. Теорема доказана.

7.3.2 Доказательство теоремы 17

Пусть монотонность последовательности $t'(n)$ начинается с n_1 . Положим

$$k_1 = \max_{n < n_1} t'(n).$$

Пусть $k > \max\{k_1, N(n_0)\}$. Возьмем любое такое n , что $n \leq m(k)$ и $N(n) \geq k$. Если мы покажем, что в H_n есть такой остовный подграф G , что ни он сам, ни $H_n \setminus G$ не содержат индуцированных подграфов графа H_n на k вершинах, то мы и установим оценку $R(\{H\}_n, k) \geq N(m(k))$. Ограничение $N(n) \geq k$ обусловлено тем, что иначе, конечно, индуцированных подграфов на k вершинах нет.

Рассмотрим случайный граф $\mathcal{G}(H_n, 1/2)$. Пусть $X = X(\mathcal{G}(H_n, 1/2))$ — случайная величина, равная количеству индуцированных подграфов графа H_n на k вершинах, которые являются также подграфами в графе $\mathcal{G}(H_n, 1/2)$ или в его дополнении до графа H_n . Если $\mathbb{E}X < 1$, то по неравенству Маркова в H_n таки есть нужный нам граф и теорема доказана.

Нетрудно видеть, что $\mathbb{E}X = f_n(k)$. Если у нас $n < n_1$, то $t'(n) \leq k_1$ по определению, а значит, $t'(n) < k$. Если же $n \geq n_1$, то $t'(n) < k$, поскольку $n \leq m(k)$, а $t'(m(k)) < k$ и на текущем участке функция t' монотонно растет. Таким образом, в любом случае $t'(n) < k$. В то же время $N(n) \geq k \geq N(n_0)$, откуда $n \geq n_0$. Беря в качестве t'' из условия теоремы величину k , получаем, что $f_n(k) < 1$, а это и требовалось доказать.

Замечание 2. Немного странно, наверное, смотрится столь сложная формулировка только что доказанной теоремы. Зачастую ее можно сильно упростить. Например, в случае классического числа Рамсея случайный граф, который возник бы (и возникает) в доказательстве аналогичного результата, — это просто случайный граф $G(n, 1/2)$ Эрдеша–Реньи. В нем $f_n(k) = C_n^k 2^{1-C_k^2}$. Пусть $m = m(k)$ — максимальное число, при котором все еще $f_m(k) < 1$. Благодаря нынешней простоте функции $f_n(k)$ ясно сразу, что при $n < m$ тем более $f_n(k) < 1$, откуда $R(k) > m$. К сожалению, в общем случае такой монотонности может не быть. А тогда неравенство $f_m(k) < 1$ означает лишь, что $R(\{H_n\}, k) \neq m$, и это не так интересно. Отсюда и вся наша возня с монотонностью. При этом мы ввели дополнительную функцию t' , поскольку, как будет видно из следующего пункта, это удобно для приложений: найти t или даже ее асимптотику трудно, тем более тяжело доказывать для нее нужные свойства, а t' в реальных ситуациях ими обладает с очевидностью.

7.3.3 Доказательства следствий

Начнем со следствия 1, т.е. предположим, что $r \geq 2s + 1$. Мы знаем, что в этом случае

$$\alpha(G(n, r, s)) \geq C_{n-s-1}^{r-s-1} \sim \frac{n^{r-s-1}}{(r-s-1)!}.$$

Отсюда сразу видно, что если дано k , то наименьшее n , при котором $\alpha(G(n, r, s)) \geq k$ (пользуемся теоремой 16), имеет вид

$$(1 + \varphi(k)) ((r-s-1)!k)^{\frac{1}{r-s-1}},$$

где $\varphi(k) \rightarrow 0$ при $k \rightarrow \infty$. Остается лишь подставить полученное выражение в качестве аргумента в функцию $N(n) = C_n^r \sim \frac{n^r}{r!}$ и не забыть, что r — константа. Верхняя оценка из следствия 1 доказана.

Перейдем к нижней оценке из следствия 1. Нужно правильно применить теорему 17. Посмотрим на доказательство теоремы 9. Да ведь там буквально функция $f_n(t)$ написана! Правда, там аргумент t обозначен k и нет умножения на 2. В сущности, все это неувидительно. Просто наличие в графе G индуцированного подграфа графа H_n равносильно наличию в графе $H_n \setminus G$ независимого множества, и наоборот. Так можно было и число Рамсея с самого начала определять — через независимые множества. И если в параграфе 4.2 мы считали среднее число независимых множеств в случайном графе, то теперь величина $f_n(t)$ выражает среднее количество независимых множеств, содержащихся либо в самом графе, либо в его дополнении: это и приводит к удвоению. Но удвоение мало на что влияет. Из выкладок параграфа 4.2 ясно, что в качестве t' можно взять функцию, асимптотически по n равную $2(s+1)\alpha(G(n, r, s)) \log_2 n$ (ср. формулировку теоремы 9). Остается найти $m(k)$, т.е. разрешить неравенство

$$2(s+1)\alpha(G(n, r, s)) \log_2 n < k$$

относительно n и подставить результат в качестве аргумента в функцию $N(n)$. Пользуемся тем, что в нашем случае $\alpha(G(n, r, s)) \leq (1 + o(1))C_n^{r-s-1} \sim \frac{n^{r-s-1}}{(r-s-1)!}$ (см. §4.1), и завершение доказательства — дело нескольких стандартных выкладок.

Доказательства следствий 2–4 полностью аналогичны. Надо использовать теоремы 9, 12, 13.

7.3.4 Доказательства теоремы 18

Рассмотрим блок из параграфа 4.3. Пусть G — остовный подграф графа $G(n, 2s+1, s)$, а $G_1, \dots, G_{C_{n-m}^s}$ (обозначения из §4.3) — это подграфы графа G , порожденные кликами блока. К ним применима классическая теория Рамсея (см. [3], [51]), которая говорит, что для каждого $i \in \{1, \dots, C_{n-m}^s\}$ либо в G_i , либо в \bar{G}_i (в дополнении до соответствующей клики) есть клика C_i размера $(1+o(1))2 \log_2 m' \sim 2 \log_2 n$ (m' — число вершин в каждой клике блока, см. §4.3). По принципу Дирихле без ограничения общности есть хотя бы $\frac{1}{2}C_{n-m}^s \sim \frac{n^s}{2s!}$ клик блока, на каждой из которых соответствующий граф G_i содержит клику того самого размера $(1+o(1))2 \log_2 n$. Значит, исходный граф G содержит не менее $(1+o(1))\frac{n^s}{2s!}$ клик размера $(1+o(1))2 \log_2 n$, причем между ними нет ребер в $G(n, 2s+1, s)$, т.е. их объединение — это индуцированный подграф в $G(n, 2s+1, s)$. Таким образом, в графе с $C_n^{2s+1} = C_n^r$ вершинами

(или в его дополнении) мы с гарантией находим индуцированный подграф исходного графа с числом вершин $(1 + o(1)) \frac{n^s \log_2 n}{s!}$.

Если теперь даны k , $k \rightarrow \infty$, то минимальные n , гарантирующие выполнение рамсеевского свойства, находятся как решения асимптотического равенства

$$k \sim \frac{n^s \log_2 n}{s!},$$

откуда

$$n \sim \left(\frac{k \cdot s \cdot s!}{\log_2 k} \right)^{\frac{1}{s}}, \quad N \sim \frac{1}{r!} \left(\frac{k \cdot s \cdot s!}{\log_2 k} \right)^{\frac{r}{s}},$$

и теорема доказана.

Список литературы

- [1] P. Brass, W. Moser, J. Pach, *Research problems in discrete geometry*, Springer, 2005.
- [2] Z. Nagy, *A certain constructive estimate of the Ramsey number*, Matematikai Lapok, 23 (1972), N 301-302, 26.
- [3] R.L. Graham, B.L. Rothschild, J.H. Spencer, *Ramsey theory*, John Wiley and Sons, NY, Second Edition, 1990.
- [4] А.М. Райгородский, *Вероятность и алгебра в комбинаторике*, Москва, МЦНМО, 2010.
- [5] D.G. Larman, C.A. Rogers, *The realization of distances within sets in Euclidean space*, Mathematika, 19 (1972), 1 - 24.
- [6] J. Balogh, A.V. Kostochka, A.M. Raigorodskii, *Coloring some finite sets in \mathbb{R}^n* , Discussiones Mathematicae Graph Theory, 33 (2013), N1, 25 - 31.
- [7] А.М. Райгородский, *Проблема Борсука и хроматические числа метрических пространств*, Успехи матем. наук, 56 (2001), вып. 1, 107 - 146.
- [8] A.M. Raigorodskii, *Coloring Distance Graphs and Graphs of Diameters*, Thirty Essays on Geometric Graph Theory, J. Pach ed., Springer, 2013, 429 - 460.
- [9] А.М. Райгородский, *Линейно-алгебраический метод в комбинаторике*, М.: МЦНМО, 2007.
- [10] P.K. Agarwal, J. Pach, *Combinatorial geometry*, John Wiley and Sons Inc., New York, 1995.
- [11] L.A. Székely, *Erdős on unit distances and the Szemerédi – Trotter theorems*, Paul Erdős and his Mathematics, Bolyai Series Budapest, J. Bolyai Math. Soc., Springer, 11 (2002), 649 - 666.
- [12] A. Soifer, *The Mathematical Coloring Book*, Springer, 2009.
- [13] V. Klee, S. Wagon, *Old and new unsolved problems in plane geometry and number theory*, Math. Association of America, 1991.
- [14] P. Erdős, A. Rényi, *On random graphs I*, Publ. Math. Debrecen, 6 (1959), 290 - 297.
- [15] P. Erdős, A. Rényi, *On the evolution of random graphs*, Publ. Math. Inst. Hungar. Acad. Sci., 5 (1960), 17 - 61.
- [16] P. Erdős, A. Rényi, *On the evolution of random graphs*, Bull. Inst. Int. Statist. Tokyo, 38 (1961), 343 - 347.
- [17] А.М. Райгородский, *Модели случайных графов*, МЦНМО, Москва, Россия, 2011.
- [18] B. Bollobás, *Random Graphs*, Cambridge Univ. Press, Second Edition, 2001.
- [19] В.Ф. Колчин, *Случайные графы*, Физматлит, Москва, 2002.
- [20] S. Janson, T. Łuczak, A. Ruciński, *Random graphs*, Wiley, NY, 2000.
- [21] B. Bollobás, *The chromatic number of random graphs*, Combinatorica, 8 (1988), 49 - 55.
- [22] T. Łuczak, *The chromatic number of random graphs*, Combinatorica, 11 (1991), 45 - 54.
- [23] K. Weber, *On the independence number of random subgraphs of the n -cube*, Annals of Discrete Math., 33 (1987), 333 - 337.
- [24] M. Krivelevich, B. Sudakov, *Pseudo-random graphs*, More sets, graphs and numbers, E. Győri, G.O.H. Katona and L. Lovász, Eds., Bolyai Society Mathematical Studies, 15 (2006), 199 - 262.

- [25] Ф. Харари, *Теория графов*, Москва, “Мир”, 1973.
- [26] Н. Алон, Дж. Спенсер, *Вероятностный метод*, Москва: Бином. Лаборатория знаний, 2007.
- [27] D.G. Larman, *A note on the realization of distances within sets in Euclidean space*, Comment. Math. Helvet., 53 (1978), 529 - 535.
- [28] P. Frankl, R. Wilson, *Intersection theorems with geometric consequences*, Combinatorica, 1 (1981), 357 - 368.
- [29] V.G. Boltyanski, H. Martini, P.S. Soltan, *Excursions into combinatorial geometry*, Universitext, Springer, Berlin, 1997.
- [30] A.M. Raigorodskii, *Three lectures on the Borsuk partition problem*, London Mathematical Society Lecture Note Series, 347 (2007), 202 - 248.
- [31] А.М. Райгородский, *Вокруг гипотезы Борсука*, Итоги науки и техники. Серия “Современная математика”, 23 (2007), 147 - 164.
- [32] А.М. Райгородский, *Проблемы Борсука и Грюнбаума для решетчатых многогранников*, Известия РАН, 69 (2005), N3, 81 - 108.
- [33] А.М. Райгородский, *Проблема Эрдеша–Хадвигера и хроматические числа конечных геометрических графов*, Мат. сборник, 196 (2005), N1, 123 - 156.
- [34] А.Э. Гутерман, В.К. Любимов, А.М. Райгородский, А.С. Усачев, *О числах независимости дистанционных графов с вершинами в $\{-1, 0, 1\}^n$: оценки, гипотезы и приложения к проблемам Нельсона–Эрдеша–Хадвигера и Борсука*, Итоги науки и техники. Серия “Современная математика”, 65 (2009), 82 - 100.
- [35] A.M. Raigorodskii, *On the chromatic numbers of spheres in \mathbb{R}^n* , Combinatorica, 32 (2012), N1, 111 - 123.
- [36] A.M. Raigorodskii, A.B. Kupavskii, *Counterexamples to Borsuk’s conjecture on spheres of small radii*, Moscow Journal of Combinatorics and Number Theory, 2 (2012), N4, 27 - 48.
- [37] Е.И. Пономаренко, А.М. Райгородский, *Улучшение теоремы Франкла–Уилсона о числе ребер гиперграфа с запретами на пересечения*, Доклады РАН, 454 (2014), N3, 268 - 269.
- [38] Е.И. Пономаренко, А.М. Райгородский, *Новые оценки в задаче о числе ребер гиперграфа с запретами на пересечения*, Проблемы передачи информации, 49 (2013), N4, 98 - 104.
- [39] М. Холл, *Комбинаторика*, Москва, “Мир”, 1970.
- [40] Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн, *Теория кодов, исправляющих ошибки*, М.: Радио и связь, 1979.
- [41] V. Rödl, *On a packing and covering problem*, European J. Combin., 6 (1985), 69 - 78.
- [42] J. Matoušek, *Using the Borsuk–Ulam theorem*, Universitext, Springer, Berlin, 2003.
- [43] P. Erdős, Ch. Ko, R. Rado, *Intersection theorems for systems of finite sets*, J. Math. Oxford, Sec., 12 (48) (1961).
- [44] M. Deza, P. Frankl, *Erdős–Ko–Rado theorem: 22 years later*, SIAM J. Alg. Disc. Methods, 4 (1983), 419 - 431.
- [45] B. Bollobás, P. Erdős, *Cliques in random graphs*, Math. Proc. Cambridge Phil. Soc., 80 (1976), 419 - 427.

- [46] Zs. Baranyai, *On the factorization of the complete uniform hypergraph*, in A. Hajnal, R. Rado, V. Sós, Infinite and Finite Sets, Proc. Coll. Keszthely, 1973, Colloquia Math. Soc. János Bolyai 10, North-Holland, 91 - 107.
- [47] А.М. Райгородский, *Проблема Борсука для $(0,1)$ -многогранников и кросс-политопов*, Доклады РАН, 371 (2000), 600 - 603.
- [48] А.М. Райгородский, *Проблема Борсука для $(0,1)$ -многогранников и кросс-политопов*, Доклады РАН, 384 (2002), 593 - 597.
- [49] А.М. Райгородский, *Проблемы Борсука и Грюнбаума для некоторых классов многогранников и графов*, Доклады РАН, 388 (2003), N6, 738 - 742.
- [50] А.М. Райгородский, К.А. Михайлов, *О числе Рамсея для полных дистанционных графов с вершинами в $\{0,1\}^n$* , Матем. сборник, 200 (2009), N12, 63 - 80.
- [51] P. Erdős, G. Szekeres, *A combinatorial problem in geometry*, Compositio Math., 2 (1935), 463 - 470.

COLORING SOME FINITE SETS IN \mathbb{R}^n

JÓZSEF BALOGH[†], ALEXANDR KOSTOCHKA[‡], AND ANDREI RAIGORODSKII^{*}

ABSTRACT. This note relates to bounds on the chromatic number $\chi(\mathbb{R}^n)$ of the Euclidean space, which is the minimum number of colors needed to color all the points in \mathbb{R}^n so that any two points at the distance 1 receive different colors. In [6] a sequence of graphs G_n in \mathbb{R}^n was introduced showing that $\chi(\mathbb{R}^n) \geq \chi(G_n) \geq (1 + o(1))\frac{n^2}{6}$. For many years, this bound has been remaining the best known bound for the chromatic numbers of some low-dimensional spaces. Here we prove that $\chi(G_n) \sim \frac{n^2}{6}$ and find an exact formula for the chromatic number in the case of $n = 2^k$ and $n = 2^k - 1$.

Keywords: chromatic number, independence number, distance graph.

MSC Primary: 52C10, **Secondary:** 05C15.

Dedicated to the 70th Birthday of Mieczyslaw Borowiecki

1. INTRODUCTION

In this note, we study the classical chromatic number $\chi(\mathbb{R}^n)$ of the Euclidean space. The quantity $\chi(\mathbb{R}^n)$ is the minimum number of colors needed to color all the points in \mathbb{R}^n so that any two points at a given distance a receive different colors. By a well-known compactness result of Erdős and de Bruijn (see [1]), the value of $\chi(\mathbb{R}^n)$ is equal to the chromatic number of a *finite* distance graph $G = (V, E)$, where $V \subset \mathbb{R}^n$ and $E = \{\{\mathbf{x}, \mathbf{y}\} : |\mathbf{x} - \mathbf{y}| = a\}$.

Date: Dec 12 2011.

[†] Department of Mathematics, University of Illinois, Urbana, IL 61801, USA. E-mail address: jobal@math.uiuc.edu. Research of this author is supported in part by NSF CAREER Grant DMS-0745185, UIUC Campus Research Board Grant 11067, and OTKA Grant K76099.

[‡]Department of Mathematics, University of Illinois, Urbana, IL, 61801, USA and Institute of Mathematics, Novosibirsk, Russia. E-mail address: kostochk@math.uiuc.edu. Research of this author is supported in part by NSF grant DMS-0965587 and by the Ministry of education and science of the Russian Federation (Contract no. 14.740.11.0868).

^{*}Department of Mechanics and Mathematics, Moscow State University, Leninskie gory, Moscow, 119991, Russia and Department of Discrete Mathematics, Moscow Institute of Physics and Technology, Dolgoprudny, Russia. E-mail address: mraigor@yandex.ru. Research of this author is supported in part by the grant of the President of Russian Federation (Contract no. MD-666.2012.1) and by the grant of the Russian Foundation for Basic Research (Contract no. 12-01-00683).

Now we know that

$$(1.239 \dots + o(1))^n \leq \chi(\mathbb{R}^n) \leq (3 + o(1))^n,$$

where the lower bound is due to the third author of this paper (see [8]) and the upper bound is due to Larman and Rogers (see [6]). Also, in [3] one can find an up-to-date table of estimates obtained for the dimensions $n \leq 12$.

It is worth noting that the linear bound $\chi(\mathbb{R}^n) \geq n + 2$ is quite simple, and the first superlinear bound was discovered by Larman, Rogers, Erdős, and Sós in [6]. They considered a family of graphs $G_n = (V_n, E_n)$ with

$$V_n = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = 3\}, E_n = \{\{\mathbf{x}, \mathbf{y}\} : |\mathbf{x} - \mathbf{y}| = 2\}.$$

In other words, the vertices of G_n are all the 3-subsets of the set $[n] = \{1, \dots, n\}$ and two vertices A, B are connected with an edge iff $|A \cap B| = 1$. Larman et al. used in [6] an earlier result by Zs. Nagy who proved the following theorem.

Theorem 1.1 ([6]). *Let s and $t \leq 3$ be nonnegative integers and let $n = 4s + t$. Then*

$$\alpha(G_n) = \begin{cases} n, & \text{if } t = 0, \\ n - 1, & \text{if } t = 1, \\ n - 2, & \text{if } t = 2 \text{ or } t = 3. \end{cases}$$

The standard inequality $\chi(G_n) \geq \frac{|V_n|}{\alpha(G_n)}$ combined with the above theorem gives an obvious corollary.

Corollary 1.1 ([6]). *Let s and $t \leq 3$ be nonnegative integers and let $n = 4s + t$. Then*

$$\chi(G_n) \geq \begin{cases} \frac{(n-1)(n-2)}{6}, & \text{if } t = 0, \\ \frac{n(n-2)}{6}, & \text{if } t = 1, \\ \frac{n(n-1)}{6}, & \text{if } t = 2 \text{ or } t = 3. \end{cases}$$

The bounds from the corollary are applied to estimate from below the chromatic numbers $\chi(\mathbb{R}^{n-1})$, since the vertices of G_n lie in the hyperplane $x_1 + \dots + x_n = 3$. Now all these bounds are surpassed due to the consideration of some other distance graphs (see [3]). However, it could happen that actually $\chi(G_n)$ is much bigger than the ratio $\frac{|V_n|}{\alpha(G_n)}$. It turns out that this is not the case, and the main result of this note is as follows.

Theorem 1.2. *If $n = 2^k$ for some integer $k \geq 2$, then*

$$\chi(G_n) = \frac{(n-1)(n-2)}{6}.$$

Additionally, if $n = 2^k - 1$ for some integer $k \geq 2$, then

$$\chi(G_n) = \frac{n(n-1)}{6}.$$

Finally, there is a constant c such that for every n ,

$$\chi(G_n) \leq \frac{(n-1)(n-2)}{6} + cn.$$

Our proof yields that $c \leq 5.5$. With some more work we could prove that $c \leq 4.5$. On the other hand, since $n(n-1)/6 - (n-1)(n-2)/6 = (n-1)/3$, we have $c \geq 1/3$.

In the next section, we prove Theorem 1.2.

2. PROOF OF THEOREM 1.2

Easily,

$$\chi(G_3) = 1, \chi(G_4) = 1, \chi(G_5) = 3.$$

Let $f(n) := \frac{(n-1)(n-2)}{6}$. We show by induction on k that $\chi(G_{2^k}) = f(2^k)$. For $k = 2$ it is trivial. Assume that for some k we established the induction hypothesis. Partition the set $[n] = [2^{k+1}]$ into the equal parts $A_1 = [\frac{n}{2}]$, $A_2 = [n] \setminus [\frac{n}{2}]$ of size 2^k . Denote by U_1 and U_2 the sets of vertices of $G = G_{2^{k+1}}$ lying in the sets A_1 and A_2 respectively. By the induction assumption, each of the induced subgraphs $G[U_1]$ and $G[U_2]$ can be properly colored with at most $f(2^k)$ colors. Cover all pairs of elements of A_1 with disjoint perfect matchings $N_1, \dots, N_{2^{k-1}}$ and all pairs of elements of A_2 with matchings $M_1, \dots, M_{2^{k-1}}$. We form a color class $C(i, j)$ for $1 \leq i \leq 2^k - 1, 1 \leq j \leq 2^{k-1}$ as follows. Consider the matchings N_i, M_i and assume that the edges are $\{u_1, u_2\}, \{u_3, u_4\}, \dots$ in N_i and $\{v_1, v_2\}, \{v_3, v_4\}, \dots$ in M_i . For $j = 1, \dots, 2^{k-1}$ let $D(i, j)$ denote the following set of quadruples (indices are considered modulo 2^k):

$$\{u_1, u_2, v_{2j-1}, v_{2j}\}, \{u_3, u_4, v_{2j+1}, v_{2j+2}\}, \dots, \{u_{2^k-1}, u_{2^k}, v_{2j-3}, v_{2j-2}\}.$$

For $i = 1, \dots, 2^k - 1$ and $j = 1, \dots, 2^{k-1}$, the color class $C(i, j)$ is formed by the collection of triples contained in the members of $D(i, j)$. The intersection sizes are all 0 or 2, so the triples in $C(i, j)$ form an independent set in G . Moreover, each triple is contained in a member of some $D(i, j)$. The total number of used colors is

$$2^{k-1}(2^k - 1) + f(2^k) = 2^{2k-1} - 2^{k-1} + \frac{(2^k - 1)(2^k - 2)}{6} = f(2^{k+1}).$$

This proves the first statement of the theorem. Since $\chi(G_n) \leq \chi(G_{n+1})$, this also implies the statement of the theorem for $n = 2^k - 1$.

It remains to show that there exists a constant c such that $\chi(G_n) \leq \frac{n^2}{6} + cn$ for every n . Consider our coloring in steps.

Step 1: Let $n = 4s_1 + t_1$ where $t_1 \leq 3$. First, color all triples containing the elements $4s_1 + 1, \dots, 4s_1 + t_1$ with at most $t_1(n - 1) < 3n$ colors. Now consider the set $[4s_1]$ and all the triples in this set. Partition $[4s_1]$ into $A_1 = [2s_1]$ and $A_2 = [4s_1] - [2s_1]$ and color the triples intersecting both A_1 and A_2 with $s_1(2s_1 - 1) < \frac{n}{4} \left(\frac{n}{2} - 1\right)$ colors as above.

Step 2: Since the triples contained in A_1 are disjoint from the triples contained in A_2 , we will use for coloring the triples contained in A_2 the same colors and the same procedure as for the triples contained in A_1 . Consider A_1 . Let $n_1 = |A_1| = 2s_1 = 4s_2 + t_2$ where $t_2 \leq 3$. Since $2s_1$ is even, $t_2 \leq 2$. By construction, $n_1 \leq \frac{n}{2}$. Similarly to Step 1, color all triples containing the elements $4s_2 + 1, \dots, 4s_2 + t_2$ with at most $t_2(n_1 - 1) < 2n_1$ colors. Partition $[4s_2]$ into $A_{1,1} = [2s_2]$ and $A_{1,2} = [4s_2] - [2s_2]$ and color the triples intersecting both $A_{1,1}$ and $A_{1,2}$ with at most $\frac{n}{8} \left(\frac{n}{4} - 1\right)$ new colors.

Step i (for $i \geq 3$): If $2s_{i-1} \leq 2$, then Stop. Otherwise, repeat Step 2 with $[2s_{i-1}]$ in place of $[2s_1]$.

Altogether, we use at most

$$\begin{aligned} & \left(3n + \frac{n}{4} \left(\frac{n}{2} - 1\right)\right) + \left(\frac{2n}{2} + \frac{n}{8} \left(\frac{n}{4} - 1\right)\right) + \left(\frac{2n}{4} + \frac{n}{16} \left(\frac{n}{8} - 1\right)\right) + \dots < \\ & < 5n + \frac{n^2}{8} \cdot \frac{4}{3} = \frac{n^2}{6} + 5n = \frac{(n-1)(n-2)}{6} + 5.5n - 1/3 \end{aligned}$$

colors. The theorem is proved.

3. DISCUSSION

First of all, we note that the constant 5 in the bound $\chi(G_n) \leq \frac{n^2}{6} + 5n$ is not the best possible. Certainly, it can be improved. However, to find the exact value of the chromatic number is still interesting. For example, we know that $\chi(\mathbb{R}^{12}) \geq 27$ (see [3]). At the same time, $\chi(G_{13}) \geq \left\lfloor \frac{\binom{13}{3}}{12} \right\rfloor = 24$ (due to Corollary 1.1), and the proof of Theorem 1.2 applied for $n = 13$ yields a bound $\chi(G_{13}) \leq 31$.

It would be quite interesting to study more general graphs. Let $G(n, r, s)$ be the graph whose set of vertices consists of all the r -subsets of the set $[n]$ and whose set of edges is formed by all possible pairs of vertices A, B with $|A \cap B| = s$. Larman proved in [5] that

$$\chi(\mathbb{R}^n) \geq \chi(G(n, 5, 2)) \geq \frac{\binom{n}{5}}{\alpha(G(n, 5, 2))} \geq (1 + o(1)) \frac{\binom{n}{5}}{1485n^2} \sim \frac{n^3}{178200}.$$

Thus, the main result of Larman was in finding the bound $\alpha(G(n, 5, 2)) \leq (1 + o(1))1485n^2$. However, the so-called linear algebra method ([2], see also [8]) can be directly applied here to show that $\alpha(G(n, 5, 2)) \leq (1 + o(1))\binom{n}{2} \sim \frac{n^2}{2}$. This

substantially improves Larman's estimate and gives $\chi(G(n, 5, 2)) \geq (1 + o(1))\frac{n^3}{60}$. We do not know any further improvements on this result. On the other hand, observe that for any 3-set A , the collection of 5-sets containing A forms an independent set in $G(n, 5, 2)$, yielding $\chi(G(n, 5, 2)) \leq \binom{n}{3} \sim \frac{n^3}{6}$. It is plausible that $\chi(G(n, 5, 2)) \sim cn^3$ with a constant $c \in [1/60, 1/6]$, but this constant is not yet found and even no better bounds for c have been published.

Furthermore, the graphs $G(n, 5, 3)$ have been studied, since the best known lower bound $\chi(\mathbb{R}^9) \geq 21$ is due to the fact that $\chi(G(10, 5, 3)) = 21$ (see [4]). No related results concerning the case of $n \rightarrow \infty$ have apparently been published.

Now, the consideration of graphs $G(n, r, s)$ with some small r, s and growing n is motivated. So assume that r and s are fixed and $n \rightarrow \infty$. We have

$$\chi(G(n, r, s)) \leq \min\{O(n^{r-s}), O(n^{s+1})\}.$$

The first bound follows from Brooks' theorem, since the maximum degree of $G(n, r, s)$ is

$$\binom{r}{s} \binom{n-r}{r-s} = (1 + o(1)) \frac{r!}{s!(r-s)!(r-s)!} n^{r-s}.$$

The second bound is a simple generalization of the above-mentioned bound $\chi(G(n, 5, 2)) \leq (1 + o(1))n^3/6$.

Note that the second bound can be somewhat improved. Assume $s < r/2$, so $q := \lceil (r-1)/s \rceil$ is at least 2. Assuming that q divides n , partition $[n]$ into q equal classes, A_1, \dots, A_q . Let \mathcal{C} be the family of $(s+1)$ -sets that are subsets of some A_i . For each $B \in \mathcal{C}$, the r -sets containing B form an independent set in $G(n, r, s)$, and by the pigeonhole principle every r -set contains such B , hence

$$\chi(G(n, r, s)) \leq |\mathcal{C}| = q \binom{n/q}{s+1} = (1 + o(1)) \frac{n^{s+1}}{q^s (s+1)!}.$$

In particular, $\chi(G(n, 5, 2)) \leq (1 + o(1))\frac{n^3}{24}$, which improves the previous bound $\frac{n^3}{6}$.

It is worthwhile to look at the construction in Section 2 from a different point of view. For $n = 2^k$ we constructed a 4-uniform hypergraph \mathcal{H} with the property that every 3-subset of vertices is covered exactly once. Note that $e(\mathcal{H}) = \binom{n}{3}/4$. Then we decomposed $E(\mathcal{H})$ into $\binom{n}{3}$ perfect matchings. Each matching gives a color class of our coloring. Note that instead of providing the explicit decomposition, we could have used a classical theorem of Pippenger and Spencer [7], which claims the existence of $(1 + o(1))\binom{n}{3}$ covering matchings.

This motivates the following possible approach to the case $r = 2s + 1$. The discussion here is not a proof, just sketching a possible way of a generalization of our argument. Assume that we managed to construct an $(r+s)$ -uniform hypergraph \mathcal{H} that covers every r -set exactly once. Then $e(\mathcal{H}) = \binom{n}{r} / \binom{r+s}{s}$. Assume that \mathcal{H} can be decomposed into t hypergraphs, $\mathcal{N}_1, \dots, \mathcal{N}_t$, such that for every i and every $A, B \in \mathcal{N}_i$

we have $|A \cap B| \leq s - 1$. Then the r -sets covered by sets in \mathcal{N}_i form an independent set, yielding $\chi(G(n, r, s)) \leq t$. If true, a generalization of the theorem of Pippenger and Spencer [7] would give $t \leq (1 + o(1)) \binom{n}{r} / \binom{n}{s} = (1 + o(1)) (s!/r!) n^{r-s}$. This bound, if true, would be asymptotically best possible, since the already mentioned linear algebra method (see [2], [8]) ensures that $\alpha(G(n, 2s + 1, s)) \leq (1 + o(1)) \binom{n}{s}$ and so $\chi(G(n, 2s + 1, s)) \geq (1 + o(1)) \binom{n}{r} / \binom{n}{s}$, provided $s + 1$ is a prime power. In particular, we would get $\chi(G(n, 5, 2)) \sim \frac{n^2}{60}$.

The case of simultaneously growing n, r, s has also been studied. Namely, $r \sim r'n$ and $s \sim s'n$ with any $r' \in (0, 1)$ and $s' \in (0, r')$ have been considered. This is due to the fact that the first exponential estimate to the quantity $\chi(\mathbb{R}^n)$, $\chi(\mathbb{R}^n) \geq (1.207 \dots + o(1))^n$, was obtained by Frankl and Wilson in [2] with the help of some graphs $G(n, r, s)$ having $r \sim r'n$ and $s \sim \frac{r'}{2}n$. Lower bounds are usually based on the linear algebra (see [8]) and upper bounds can be found in [9].

REFERENCES

- [1] N.G. de Bruijn, P. Erdős, *A colour problem for infinite graphs and a problem in the theory of relations*, Proc. Koninkl. Nederl. Acad. Wet., Ser. A **54** (1951), 371–373.
- [2] P. Frankl, R. Wilson, *Intersection theorems with geometric consequences*, Combinatorica **1** (1981), 357–368.
- [3] A.B. Kupavskiy, *On coloring spheres embedded into \mathbb{R}^n* , Sb. Math. **202** (2011), N6, 83–110.
- [4] A.B. Kupavskiy, A.M. Raigorodskii, *On the chromatic number of \mathbb{R}^9* , J. of Math. Sci. **163** (2009), N6, 720–731.
- [5] D.G. Larman, *A note on the realization of distances within sets in Euclidean space*, Comment. Math. Helvet. **53** (1978), 529–535.
- [6] D.G. Larman, C.A. Rogers, *The realization of distances within sets in Euclidean space*, Mathematika **19** (1972), 1–24.
- [7] N. Pippenger, J. Spencer, *Asymptotic behavior of the chromatic index for hypergraphs*, J. Combin. Theory, Ser. A **51** (1989), 24–42.
- [8] A.M. Raigorodskii, *On the chromatic number of a space*, Russian Math. Surveys **55** (2000), N2, 351–352.
- [9] A.M. Raigorodskii, *The Borsuk and Grünbaum problems for lattice polytopes*, Izvestiya of the Russian Acad. Sci., **69** (2005), N3, 81–108; English transl. in Izvestiya Math., **69** (2005), N3, 513–537.

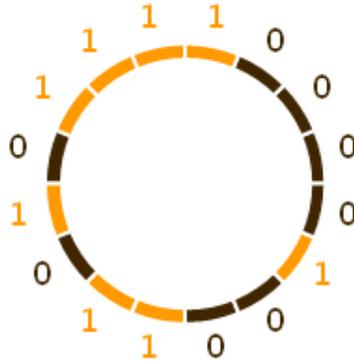
Последовательности де Брёйна и Универсальные Циклы.

Константин Матвеев и Иван Митрофанов

Ну, — радостно откликнулся Дронт, — лучший способ объяснить - это самому сделать! Так как вам, может быть, тоже захочется попробовать в морозный денек, что это за штука Кросс по Инстанциям, я расскажу, что Дронт сделал. Прежде всего он, как он выразился, «разметил инстанцию», — то есть нарисовал на земле круг (не очень ровный, но «точность тут не обязательна», сказал Дронт). Далее он расставил всех присутствующих по этому кругу (строго как попало). А потом . . .

Льюис Кэрролл. Алиса в Стране Чудес.

Последовательность 0000100110101111 примечательна тем, что если читать её по кругу, то ровно один раз можно прочесть любое двоичное слово длины 4.



Такую последовательность называют последовательностью де Брёйна или *универсальным циклом* для множества двоичных слов длины 4. Иногда (см. раздел D) количество универсальных циклов можно точно подсчитать, но иногда вообще неизвестно, существует ли хоть один.

В некоторых задачах этого цикла, в том числе, конечно, в открытых вопросах, принимаются любые частичные продвижения. Более того, ознакомившись с разделом C, Вам, возможно, захочется попробовать поставить перед собой и порешать другие задачи про универсальные циклы, обогатив эту сравнительно недавно развивающуюся теорию новыми интересными идеями.

А Для начала

A.1 Можно ли расположить $\binom{100}{5}$ чисел по кругу так, чтобы любая пятёрка различных чисел из множества $\{1, 2, \dots, 100\}$ встречалась где-нибудь в пяти последовательных позициях?

A.2 Существует ли бесконечная последовательность натуральных чисел, такая что любая пятёрка различных натуральных чисел ровно один

раз встречается где-нибудь в этой последовательности в пяти последовательных позициях?

А.3 а) Можно ли раскрасить клетчатую плоскость в 2 цвета так, чтобы раскраска переходила бы в себя при сдвиге на 4 клетки по горизонтали или вертикали, и можно было бы найти любую из 16-ти раскрасок квадрата 2×2 ?

б) Можно ли раскрасить клетчатую плоскость в 2 цвета так, чтобы раскраска переходила бы в себя при сдвиге на 4 клетки по горизонтали или вертикали, и можно было бы найти любую из 16-ти раскрасок *диагонального квадрата* (диагональным квадратиком будем называть множество из четырех клеток, соседних по стороне некоторой клетке)?

В Последовательности де Брёйна и ориентированные графы.

Определение В.1 (Последовательность де Брёйна) Последовательность де Брёйна ранга n над k -буквенным алфавитом – это циклическая последовательность из букв длины k^n такая, что любая n -буквенная последовательность встречается как подпоследовательность ровно один раз.

Определение В.2 (Ориентированный граф) Ориентированный граф G состоит из множества вершин $V = \{v_1, \dots, v_p\}$ и множества рёбер $v_i \rightarrow v_j$. В нём могут быть кратные рёбра между v_i и v_j в обоих направлениях, а также петли $v_i \rightarrow v_i$. G называется сильно связным, если из любой вершины можно добраться в любую другую по рёбрам (двигаясь по направлению). Он называется сбалансированным, если для каждой вершины входящая степень (число входящих рёбер) равно исходящей степени (числу исходящих рёбер). Эйлеров цикл – замкнутый путь по рёбрам графа, проходящий по каждому ребру ровно один раз.

В.4 Докажите, что в ориентированном графе без изолированных вершин есть эйлеров цикл в том и только в том случае, если граф сильно связан и сбалансирован.

В.5 Докажите, что последовательность де Брёйна ранга n над k -буквенным алфавитом существует для любых k и n .

В.6 Пусть G — ориентированный граф, в котором входящая и исходящая степень каждой вершины равна k . Докажите, что его рёбра можно покрасить в k цветом так, чтобы у каждой вершины было ровно одно входящее и ровно одно исходящее ребро каждого цвета.

В.7 а) Докажите, что последовательность де Брёйна из символов 0 и 1 ранга n может быть построена при помощи следующего алгоритма. Начинаем с $n - 1$ последовательных нулей и приписываем символы согласно следующему правилу. На каждом шаге добавляем 1, если это не приводит к повтору какой-либо n -буквенной подпоследовательности, в противном случае добавляем 0. Делаем $2^n - n + 1$ шаг и рассматриваем полученный результат как циклическую последовательность.

б) Как можно модифицировать этот алгоритм для получения последовательности де Брёйна ранга n над k -буквенным алфавитом?

С Фокусы и универсальные циклы.

Если Вы решили немного другую задачу, чем в условии, расскажите нам: это может быть интересно. А ещё будут оцениваться решения, работающие «не для всех n ».

С.1 Фокусник собирается провести такой фокус: он достаёт колоду, в которой в некотором порядке расположены $n!$ карточек со всеми числами от 1 до $n!$, и вызывает из зала n добровольцев.

После чего один из добровольцев несколько раз сдвигает колоду, таким образом порядок карт меняется неким циклическим образом. Далее n человек по очереди берут себе по одной карте с верха колоды. После чего они изучают карты (не показывая их фокуснику) и встают друг за другом в порядке возрастания чисел на их картах. Глядя на порядок, в котором они стоят, фокусник угадывает их карты. Объясните секрет фокуса.

С.2 а) Фокусник собирается проделать точно такой же фокус, но хочет использовать как можно меньше различных чисел. От заготовливает колоду с $n!$ картами, на каждой написано число от 1 до C , где $C < n!$. Добровольцы совершают те же самые действия, при этом, если среди n вытащенных подряд карточек встречается пара одинаковых, то фокус проваливается. Попробуйте для как можно меньшего C доказать, что фокуснику хватит C различных карт.

б) В 2006 году Дж.Роберт Джонсон доказал стоявшую более 10 лет гипотезу, что хватит $n + 1$ различной карты. Попробуйте получить такой же результат.

С.3 У фокусника в колоде 52 карточки, на которых написаны числа (не обязательно разные). На сцену выходят пять добровольцев, сдвигают колоду и берут по порядку по одной карте сверху. После этого фокусник просит их разбиться на группы так, чтобы в разных группах были бы люди с разными карточками, а внутри каждой группы числа на карточках у всех были равны. Глядя на это разбиение, фокусник может определить расположение всех остальных карт в колоде. Объясните секрет фокуса.

С.4 При каких n можно расположить по кругу C_n^2 чисел так, чтобы любые два различных числа из множества $\{1, 2, \dots, n\}$ встречались рядом?

С.5 Докажите, что если $n \geq 8$ и n не делится на 3, то по кругу можно расположить C_n^3 чисел так, чтобы любые три различных числа из множества $\{1, 2, \dots, n\}$ встречались на каких-то трёх последовательных позициях.

С.6 (ответ неизвестен) При каких k и n можно так расположить по кругу C_n^k чисел, чтобы любые k различных чисел из множества $\{1, 2, \dots, n\}$ встречались на каких-то k последовательных позициях?

Д Начало перечисления

В этом разделе нас в первую очередь будет интересовать $B(2, n)$ — число последовательностей де Брёйна ранга n над 2-буквенным алфавитом. Последовательности, различающиеся только циклическим сдвигом, считаются

одинаковыми. Обозначим через $\epsilon(G)$ число эйлеровых циклов в ориентированном графе G .

Определение D.1 (Ориентированный граф рёбер) Пусть $G = (V, E)$ — ориентированный граф. Его ориентированный граф рёбер $\mathcal{L}G$ — ориентированный граф со множеством вершин E (рёбра графа G) и множеством рёбер $e \rightarrow f$ для тех пар рёбер e и f графа G , для которых $s(f) = t(e)$ (от английских *source* и *target*, начало ребра f является концом e).

D.1 Пусть у G более одного ребра и нет изолированных вершин. Докажите, что $\mathcal{L}G$ связан тогда и только тогда, когда G связан.

D.2 Пусть в графе G для любой вершины v исходящая и входящая степени равны 2. Пусть вершина x является концом рёбер P и Q и началом рёбер R и S , ни одно из этих четырёх рёбер не является петлёй. Пусть G_1 — граф, полученный из G удалением x и склейкой P с R и Q с S ; G_2 — граф, полученный из G удалением x и склейкой P с S и Q с R . Докажите, что

$$\epsilon(\mathcal{L}G) = 2(\epsilon(\mathcal{L}G_1) + \epsilon(\mathcal{L}G_2)).$$

D.3 Найдите $B(2, n)$.

**Последовательности де Брейна и Универсальные Циклы.
После промежуточного финиша.**

Илья Богданов, Константин Матвеев, Иван Митрофанов.

Е Торы де Брейна

Определение Е.1 (Торы де Брейна) Тором де Брейна типа $(R, S, u, v)_k$ ($RS = k^{uv}$) будем называть заполнение клетчатой плоскости числами $1, 2, \dots, k$, инвариантное относительно вертикального сдвига на R и горизонтального сдвига на S , для которого найдутся прямоугольники $u \times v$ (u строк и v столбцов), заполненные всеми k^{uv} возможными способами.

Гипотеза Е.2 Для любых R, S, u, v, k , таких что $RS = k^{uv}$, $R > u$, $S > v$, существует тор де Брейна типа $(R, S, u, v)_k$.

Эта гипотеза доказана только в некоторых частных случаях, например для $u = v = 2$. Помимо конструкций из нижеприведенных задач, мы также будем принимать все другие бесконечные серии конструкций, которые вы придумаете.

Е.1 Докажите, что для всех $k, u \geq 2$, $(k, u) \neq (2, 2)$ существует тор типа $(k^{u-1}, k, u, 1)_k$.

Е.2 Докажите, что для всех нечетных $k > 1$ существует тор типа $(k^2, k^2, 2, 2)_k$.

Е.3 Докажите, что для всех $k, u, v \geq 2$, кроме случая, когда $v = 2$ и k четно, существует тор типа $(k^u, k^{u(v-1)}, u, v)_k$.

Е.4 Докажите, что также для всех четных $k \geq 2$ существует тор типа $(k^2, k^2, 2, 2)_k$.

Е.5 Докажите, что для всех $k > 1$ существует тор типа $(k^4, k^2, 2, 3)_k$.

Е.6 Предположим, что существует тор типа $(k^r, k^s, u, v)_k$ ($uv = r + s$), такой что сумма чисел в каждом столбце (то есть вертикальном периоде длины R) делится на k . Докажите, что существует тор типа $(k^r, k^{s+v}, u + 1, v)_k$.

Е.7 Докажите, что для всех $k > 1$ существует тор типа $(k^8, k^8, 4, 4)_k$.

Е.8 Докажите, что для всех нечетных $k > 1$, если n четно или k — точный квадрат, то существует тор типа $(k^{n^2/2}, k^{n^2/2}, n, n)_k$.

Е.9 Докажите то же самое для всех четных $k > 1$.

Е.10 Докажите, что для всех s, t существует тор типа $(4st^2, 4s^3t^2, 2, 2)_{2st}$.

Ф Продолжение Перечисления

Обозначим через $B(k, n)$ количество последовательностей де Брейна ранга n над алфавитом из k букв. Как и прежде, последовательности, отличающиеся циклическим сдвигом, считаются одинаковыми

Определение F.1 (Ориентированное остовное дерево) *Ориентированным остовным деревом в G называется ациклический (в неориентированном смысле) подграф, в котором выделена вершина — корень v , и из любой вершины $u \in V$ существует единственный путь в v по ребрам этого подграфа. Обозначим через $\tau(G, v)$ количество ориентированных остовных деревьев с корнем v .*

F.1 Пусть G — сильно связанный сбалансированный ориентированный граф. Докажите, что для любого $v \in V$

$$\epsilon(G) = \tau(G, v) \prod_{u \in V} (\text{outdeg}(u) - 1)!$$

Theorem F.2 Теорема Левина *G — ориентированный граф, в котором в каждую вершину входит хотя бы одно ребро. Пусть x_e — переменная, соответствующая ребру e графа G . Определим многочлены от нескольких переменных*

$$\kappa^{\text{edge}}(G) = \sum_{\substack{\mathcal{T} \text{ — ориентированное} \\ \text{остовное дерево в } G}} \prod_{e \text{ — ребро } \mathcal{T}} x_e$$

и

$$\kappa^{\text{vertex}}(\mathcal{L}G) = \sum_{\substack{\mathcal{T} \text{ — ориентированное} \\ \text{остовное дерево в } \mathcal{L}G}} \prod_{\omega \text{ — ребро } \mathcal{T}} x_{t(\omega)}.$$

Тогда

$$\kappa^{\text{vertex}}(\mathcal{L}G) = \kappa^{\text{edge}}(G) \prod_{v \in V} \left(\sum_{e: s(e)=v} x_e \right)^{\text{indeg}(v)-1}.$$

F.2 Вычислите $B(k, n)$ (вы можете пользоваться теоремой Левина).

F.3 Докажите теорему Левина.

Г Последовательности де Брейна через рекурренты

Рассмотрим следующий способ построения периодической последовательности из 0 и 1. Начнем с 00001 и шаблона длины 5, скажем $X00XX$. На каждом шаге будем накладывать наш шаблон на последние пять цифр имеющейся последовательности и определять следующую цифру как сумму по модулю 2 тех цифр, которые оказались под знаком X . В нашем случае мы получаем

$$0000110110 \dots$$

В общем начнем с $0^{n-1}1$ и шаблона длины n (шаблон должен начинаться с X). Назовем шаблон *полезным*, если получающаяся последовательность содержит все возможные подпоследовательности длины n кроме 0^n .

G.1 Докажите, что для любого n существует полезный шаблон длины n .

G.2 Можно ли применить похожие методы при конструировании почти де Брейновских тортов? (открытый вопрос, как можно догадаться)

Последовательности де Брёйна и Универсальные Циклы РЕШЕНИЯ

А Для начала

А.1 Ответ. Нет.

Предположим, что такая расстановка существует. Рассмотрим какое-нибудь число, например, 1. Пусть оно написано k раз, тогда оно встречается в $5k$ различных пятёрках. С другой стороны, количество пятёрок, в которых оно должно встречаться — это количество способов выбрать 4 числа из оставшихся. Но C_{99}^4 не делится на 5, поэтому получаем противоречие.

А.2 Ответ. Такая последовательность существует.

Сначала пронумеруем как-нибудь все возможные пятёрки натуральных чисел: например, пятёрку из чисел $(1, 2, 3, 4, 5)$ занумеруем единицей, потом занумеруем все пятёрки с суммой 16, потом с суммой 17 и так далее.

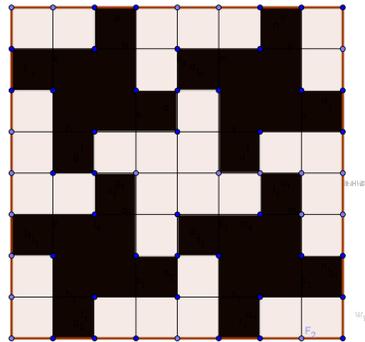
Пусть есть какая-то конечная последовательность натуральных чисел такая, что в ней встречаются все пятёрки с 1-й по k -ю и никакая пятёрка не повторяется дважды (при этом могут встречаться пятёрки с номерами, большими k). Покажем, что эту последовательность можно продолжить на конечное число членов вправо так, чтобы встретились пятёрка с номером $k + 1$ и не возникло повторов.

В самом деле, если $(k + 1)$ -я пятёрка уже встречается, то ничего делать не требуется. Иначе допишем справа 10 чисел $b_1, b_2, b_3, b_4, b_5, a_1, a_2, a_3, a_4, a_5$, где a_1, \dots, a_5 — числа $(k + 1)$ -й пятёрки, а b_i — произвольные различные числа, большие всех остальных записанных (включая a_1, \dots, a_5).

Бесконечное количество раз продолжая так последовательность, получим бесконечную последовательность натуральных чисел. То, что в ней встретятся все пятёрки, очевидно. Покажем, что никакая пятёрка не встретится дважды. В самом деле, пусть какая-то пятёрка записана дважды, тогда она оказалась записана дважды после какого-то шага, чего быть не может.

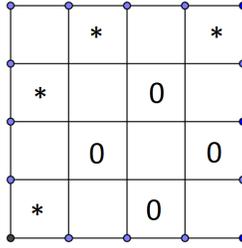
А.3 а) Ответ. Можно.

На рисунке приведён кусок плоскости 8×8 . Попробуйте отыскать подобный узор, выглянув из окна.



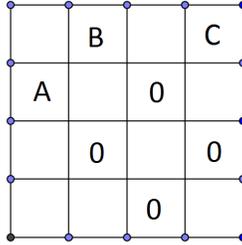
б) Ответ. Нельзя.

Показывается это несложным перебором. Предположим, что такая расстановка нулей и единиц существует, тогда все различные диагональные квадратики раскрашены по-разному (различными называются диагональные квадратики, не переводящиеся друг в друга параллельным переносом на вектор вида $(4a, 4b)$.) Всё дальнейшее будем рисовать на развёртке *тора* 4×4 , белый и чёрный цвета заменим единичками и нулями.



Сначала найдём диагональный квадратик, в котором стоят четыре нуля.

Покажем, что во всех клетках, отмеченных звёздочками, должны стоять единицы. Эти четыре клетки по отношению к четырём найденным нулям расположены *одинаково*, поэтому достаточно показать для одной из них.

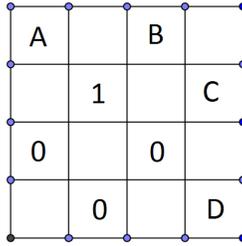


Пусть в A стоит 0, тогда в B и C стоит 1 (иначе ещё раз встретятся четыре нуля.) Но тогда два раза встретится расстановка «1 сверху, три нуля снизу».

Если на месте звёздочек стоят единицы, то уже есть все восемь расстановок единиц и нулей, в которых единиц чётное число. Заметим, что любой диагональный квадратик состоит либо из четырёх неотмеченных клеток, либо из четырёх отмеченных.

В восьми неотмеченных клетках должны встречаться всевозможные расстановки типа «три нуля и единица» и «три единицы и ноль».

Не умаляя общности, в четырёх клетках цифры стоят так же, как на рисунке.



Предположим, что на месте A стоит 0. Тогда из соображений чётности на месте B и C стоят нули, а на месте D — единица, легко видеть, что такая расстановка не подходит.

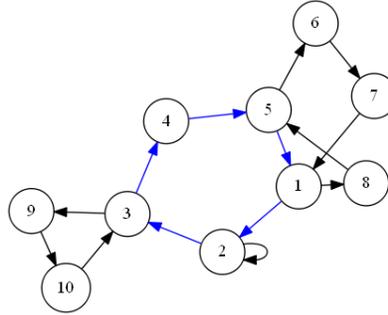
Если же на месте A стоит 1, то на месте B и C также должны стоять единицы, а на месте D — ноль. Тоже не подходит.

В Последовательности де Брёйна и ориентированные графы

В.4 Если есть эйлеров цикл, то, двигаясь по нему, в каждую вершину заходим столько же раз, сколько и выходим (сбалансированность); между любыми двумя рёбрами есть путь по циклу, а так как нет изолированных вершин, к каждой вершине примыкает по ребру и между любыми двумя вершинами есть путь по циклу (сильная связность).

Пусть орграф сильносвязан и сбалансирован. Существование эйлерова цикла будем доказывать по индукции по количеству рёбер, база (0 рёбер) очевидна.

Выйдем из какой-нибудь вершины и будем идти по стрелкам, пока не придём в вершину, в которой уже были. Таким образом, в графе есть цикл C .



Удалим из орграфа рёбра этого цикла. Полученный орграф будет сбалансированным, но не обязательно связным.

Лемма. Если сбалансированный орграф связан (то есть связан как граф, если забыть про ориентацию рёбер), то он сильно связан.

Доказательство. Рассмотрим произвольную вершину v . Пусть A – множество вершин, в которые можно добраться из v , а B – все остальные вершины. Пусть B непусто. Тогда есть рёбра из B в A , но нет рёбер из A в B , значит, сумма по всем вершинам множества A количества входящих рёбер будет больше, чем количества исходящих. Но она – ноль из-за сбалансированности графа, противоречие. \square

Итак, при удалении C граф распадается на сбалансированные сильносвязные компоненты, в каждой из которых по предположению индукции есть эйлеров цикл. Для каждой из этих компонент отметим на цикле C по одной вершине. Тогда искомым эйлеров цикл во всём графе строится так: идём по отрезку цикла C до очередной отмеченной точки, проходим по эйлерову циклу компоненты, возвращаясь в ту же точку, снова идём по C до следующей отмеченной точки и так далее.

В.5 Построим ориентированный граф, который в дальнейшем будем называть *графом де Брёйна* $G(n, k)$.

Вершинами его будут k^{n-1} последовательностей длины $n - 1$ над k -буквенным алфавитом, а из вершины $a_1 a_2 \dots a_{n-1}$ ведёт ребро в $b_1 b_2 \dots b_{n-1}$, если $a_2 = b_1, a_3 = b_2, \dots, a_{n-1} = b_{n-2}$. Таким образом, рёбра $G(n, k)$ соответствуют последовательностям длины n и их всего k^n .

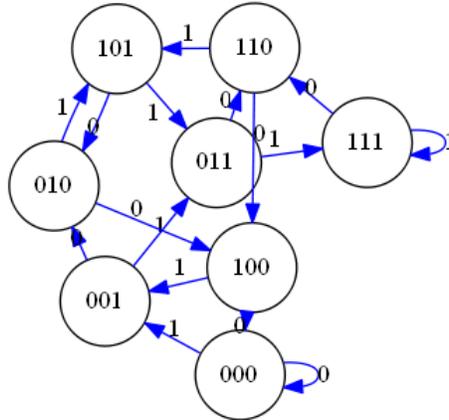


Рис. 1: $G(4, 2)$.

Вообще, каждому слову длины $n + a$ соответствует ориентированный путь длины $a + 1$. Вершины этого пути – это $(n - 1)$ -буквенные подслова нашего слова в порядке их появления.

На каждом ребре напишем последнюю букву соответствующего слова. Тогда, если последнее ребро пути соответствует слову $a_1 a_2 \dots a_k$, то буквы, написанные на предыдущих $k - 1$ рёбрах этого пути, образуют слово $a_1 a_2 \dots a_{k-1}$.

Исходящая и входящая степень любой вершины равны k . Граф сильно связан, так как слово $a_1 a_2 \dots a_{k-1}$ соединено с $b_1 b_2 \dots b_{k-1}$ путём, соответствующим слову $a_1 a_2 \dots a_{k-1} b_1 b_2 \dots b_{k-1}$.

Значит, в $G(n, k)$ есть эйлеров цикл. Циклическая последовательность, образованная буквами, записанными на его последовательных рёбрах, будет последовательностью де Брёйна, так как подслова длины n соответствуют различным рёбрам графа.

В.6 База индукции: $k = 0$.

Если мы сможем выбрать несколько рёбер так, чтобы из каждой вершины выходило ровно одно выбранное и в каждую вершину входило ровно одно выбранное, то мы покрасим эти рёбра в первый цвет, удалим их и воспользуемся индукционным предположением для $k - 1$.

Воспользуемся *леммой Холла*: если есть несколько девушек и юношей и для любого m любые m юношей знают в совокупности хотя бы m девушек, то можно для каждого юноши выбрать знакомую девушку так, чтобы для разных юношей были бы выбраны разные девушки.

Поместим в каждую вершину графа по юноше и по девушке и познакомим каждого юношу с теми девушками, к которым от него ведёт ориентированное ребро.

Предположим, что условия леммы Холла не выполняются: есть группа из m_1 юношей, и они знают в совокупности $m_2 < m_1$ девушек. Из вершин, в которых сидят эти юноши, выходит в совокупности km_1 рёбер, при этом все рёбра идут в множество из m_2 вершин. Значит, в какую-то из вершин ведёт хотя бы $\frac{km_1}{m_2} > k$ рёбер, противоречие.

Итак, выберем при помощи леммы Холла пары «юноша-девушка» и выберем в графе соответствующие рёбра. Из каждой вершины будет выходить ровно одно выбранное, в каждую вершину будет входить ровно одно выбранное, получили то, что хотели.

В.7 б) Упорядочим все буквы. Алгоритм будет выглядеть так: начинаем с $k - 1$ нуля, на каждом шаге пишем максимальную возможную букву с тем условием, чтобы никакое слово длины k не повторилось дважды. Если получится сделать так $k^n - n + 1$ операцию, то если зациклить полученный результат, получится последовательность де Брёйна.

Интерпретация: дан граф де Брёйна $G(n, k)$, начинаем с вершины $000 \dots 0$. Движемся по рёбрам, каждый раз выбирая непроведённое ребро с наибольшей написанной буквой.

Предположим, что пришли в вершину, все рёбра из которой уже проведены. Это может быть только первая вершина пути, то есть $00 \dots 0$, так как во все остальные входили столько же раз, сколько из них выходили.

В этом пути должно встречается ребро $00 \dots 0$, иначе можно было бы двигаться дальше, добавив его к концу пути.

Рассмотрим все рёбра, по которым построенный путь не проходит, и покрасим их в серый цвет, серые рёбра, на которых написан 0, покрасим в чёрный цвет.

Лемма: ориентированного цикла, состоящего из чёрных рёбер, нет. Предположим противное. Найдётся путь длины k из чёрных рёбер, тогда последнее ребро этого пути соответствует слову $0 \dots 00$, но по этому ребру мы проходили. Противоречие.

Пусть есть хотя бы одно чёрное или серое ребро $v_1 v_2$. В вершину v_2 входило меньше k раз, значит, из неё выходило меньше k раз и не выходило по ребру с написанным нулём. Значит, из v_2 выходит некоторое чёрное ребро $v_2 v_3$. Аналогично, есть чёрное ребро $v_3 v_4$ и так далее, в конечном итоге получим цикл из чёрных рёбер, а этого не может быть по лемме.

Пункт а) – частный случай при $k = 2$.

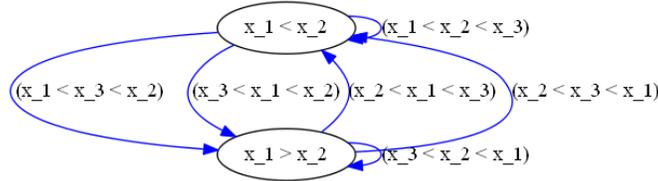
С Фокусы и универсальные циклы.

С.1 Пусть есть две последовательности чисел a_1, a_2, \dots, a_n и b_1, b_2, \dots, b_n такие, что в каждой из последовательностей все числа различны. Будем говорить, что они упорядочены одинаковым образом, если для любой пары индексов $i \neq j$ либо $a_i < a_j$ и $b_i < b_j$, либо, наоборот, $a_j > a_i$ и $b_j > b_i$.

Рассмотрим множество S_n способов упорядочить множество $\{1, 2, \dots, n\}$. В S_n ровно $n!$ элементов, каждый из них называется *перестановкой длины n* . Фокуснику удастся фокус, если он придумает циклическую последовательность из $n!$ различных чисел такую, что все $n!$ различных кусков последовательности длины n упорядочены по-разному.

Для этого построим ориентированный граф \mathbb{S}_n , вершинами которого являются всевозможные перестановки длины $n - 1$, а рёбра проводятся согласно следующему правилу. Для каждой перестановки $s \in S_n$ определим её *начало* как перестановку длины $n - 1$, упорядоченную так же, как элементы s без последнего. Аналогично определим *конец* перестановки s (например, у перестановки 31542 началом является 2143, а концом — 1432). Наконец, для каждой $s \in S_n$ проведём ребро из её начала в конец.

Элементы S_n удобно записывать в виде системы неравенств на переменных x_1, \dots, x_n , как показано на рисунке.



Граф \mathbb{S}_3

Покажем, что в S_n есть эйлеров цикл. В самом деле, из каждой вершины выходит n рёбер и в каждую вершину входит n рёбер, это — количество способов расположить новое число на числовой прямой относительно $n - 1$ различных чисел. Проверим сильную связность: пусть s_1 и s_2 — две перестановки длины $n - 1$. Рассмотрим какую-нибудь последовательность длины $2n - 2$, состоящую из различных чисел и такую, что первые $n - 1$ членов упорядочены способом s_1 , а последние $n - 1$ членов — способом s_2 . Тогда рёбра пути, соединяющего s_1 с s_2 в графе \mathbb{S}_n — это перестановки, соответствующие всем кускам последовательности длины n .

Выберем какой-нибудь эйлеров цикл в \mathbb{S}_n , пусть его рёбра в порядке следования соответствуют перестановкам $s_1, s_2, \dots, s_{n!}$. Возьмём $n!$ переменных $y_1, \dots, y_{n!}$ и будем считать, что $y_{n!+k} = y_k$. Каждая перестановка s_i задаёт систему неравенств на переменных x_1, \dots, x_n . Запишем такую же систему неравенств, заменив каждую переменную x_k на y_{i+k-1} . Например, если s_3 задавала систему $x_2 > x_1 > x_3$, то мы запишем $y_4 > y_3 > y_5$. Наша цель — заменить переменные y_i числами так, чтобы выполнялось каждое из записанных неравенств.

Для каждой s_i проведём $\frac{n(n-1)}{2}$ ориентированных рёбер между y_i, \dots, y_{i+n-1} , стрелка $y_{i_1} \rightarrow y_{i_2}$ соответствует неравенству $y_{i_1} > y_{i_2}$. Мы получили новый ориентированный граф H на вершинах $y_1, \dots, y_{n!}$.

Лемма. В графе H нет ориентированных циклов.

Доказательство. Ребро $y_i \rightarrow y_j$ графа H назовём *идушим вправо*, если $j - i \in \{1, 2, \dots, n - 1\}$, и *идушим влево*, если тому же множеству принадлежит $i - j$. При $n > 2$ каждое ребро H принадлежит ровно одному из этих множеств, и если в H есть ребро $y_i \rightarrow y_j$, то рёбра $y_j \rightarrow y_i$ в H нет.

Предположим противное. Рассмотрим в H ориентированный цикл с наименьшим количеством рёбер. Пусть у него есть два последовательных ребра, идущих в разные стороны — скажем, $y_i \rightarrow y_j$, идущее влево, и $y_j \rightarrow y_k$, идущее вправо. Все эти рёбра проведены для перестановки s_j ; по той же причине ребро $y_i \rightarrow y_k$ также существует, и наш цикл можно сократить. Это противоречит выбору цикла.

Итак, если в H есть ориентированный цикл, то есть и ориентированный цикл C , все рёбра которого ведут в одном направлении — скажем, влево. С другой стороны, для некоторого индекса t перестановка s_t задаёт неравенства $x_1 < x_2 < \dots < x_n$; тогда в H есть рёбра $y_{t+n-1} \rightarrow y_{t+n-2} \rightarrow \dots \rightarrow y_t$. Но в цикле C должны встретиться две вершины из y_t, \dots, y_{t+n-1} ; ребро между ними будет идти вправо. Это противоречие завершает доказательство леммы. \square

Поскольку циклы в H отсутствуют, мы можем ввести на переменных y_i частичный порядок: $y_{i_1} \succ y_{i_2}$, если из y_{i_1} в y_{i_2} ведёт путь в H .

Возьмём один из минимальных элементов, присвоим ему значение 1. Возьмём какой-нибудь минимальный из оставшихся, присвоим значение 2, и так далее для всех переменных y_i . Все нужные неравенства будут автоматически выполнены.

С.2 Решение можно найти в статье J. R. Johnson, Universal cycles for permutations, Discrete Math., 309(2009), pp. 5264–5270.

С.3 Решение во многом аналогично решению **С.1**.

Будем говорить, что две последовательности (a_1, a_2, \dots, a_n) и (b_1, b_2, \dots, b_n) *разбиты одинаково*, если для любых $i \neq j$ либо $a_i = a_j$ и $b_i = b_j$, либо $a_i \neq a_j$ и $b_i \neq b_j$. Обозначим через P_n множество разных разбиений последовательностей длины n .

Можно проверить, что в P_5 ровно 52 элемента, поэтому фокус удастся, если фокусник сумеет расположить по окружности 52 числа так, что все 52 последовательных пятёрок чисел будут разбиты по-разному. Вот пример такой последовательности:

БББББКЧЧЧККББКККЧКЧКПЧЧПБПБППЧПББКЧППКЧПЧБЧПКЧПДКБК

Здесь вместо чисел стоят буквы П, К, Б, Ч, обозначающие карточные масти, и одна буква Д, обозначающая джокера. Можно взять обычную карточную колоду, заменить пиковую даму на джокера и продемонстрировать этот фокус.

Сейчас мы покажем, как получить такую последовательность с минимумом перебора (правда, у нас может получиться больше пяти различных чисел); мы работаем с P_5 , но подобный метод позволяет находить универсальные циклы для P_n при всех $n > 4$.

Рассмотрим ориентированный граф \mathbb{P}_5 , вершинами которого являются элементы P_4 , а рёбра соответствуют элементам P_5 следующим образом. Для разбиения p из P_5 определим его *начало* и *конец* как разбиения из P_4 , разбитые так же, как первые и последние $n - 1$ элемент в p , соответственно. В графе \mathbb{P}_5 для каждого $p \in P_5$ проведём ребро от начала π к его концу. Скажем, разбиение 12324 задаст ребро $1232 \rightarrow 1213$.

Покажем, что \mathbb{P}_n сильно связан. Пусть нужно найти путь между разбиениями p_1 и p_2 . Рассмотрим последовательность длины $2n - 2$, первая половина которой разбита так же, как p_1 , а вторая — так же, как p_2 . Тогда подпоследовательности длины n образуют рёбра нужного пути.

Сбалансированность также легко проверяется: если элемент P_4 содержит k различных элементов, то каждое исходящее и входящее ребро соответствует добавлению нового элемента, который либо равен одному из имеющихся, либо отличен от всех; таким образом, исходящая и входящая степени нашего элемента равны $k + 1$.

Значит, в графе \mathbb{P}_5 можно найти эйлеров цикл. Каждый эйлеров цикл в \mathbb{P}_5 задаёт систему равенств и неравенств на множестве переменных y_1, \dots, y_{52} , расставленных по циклу (способом, аналогичным введённому в **С.1**).

Если в системе есть равенство $y_i = y_j$, соединим эти переменные белым ребром, если же есть неравенство $y_i \neq y_j$, то соединим их чёрным ребром. Будем говорить, что полученная система противоречива, если есть две переменные, между которыми есть чёрное ребро и цепочка белых рёбер (это соответствует тому, что можно вывести соотношение $y_i \neq y_i$). Если система непротиворечива, то нужную расстановку чисел по кругу можно получить, заменив на одно и то же число те переменные, между которыми есть путь из белых рёбер.

Итак, осталось показать, что эйлеров цикл можно выбрать так, чтобы полученная система была непротиворечивой.

Прежде всего, заметим по аналогии с **С.1**, что если система противоречива, то существует противоречие вида

$$y_{i_1} = y_{i_2} = \dots = y_{i_k} \neq y_{i_1},$$

где все стрелки $y_{i_j} \rightarrow y_{i_{j+1}}$ ведут вправо.

Рассмотрим последовательность $W = 113112222213311$. Она соответствует пути длины 11 в графе \mathbb{P}_5 .

Лемма 1. *Если эйлеров цикл содержит сей путь, то получается непротиворечивая система.*

Доказательство. Рассмотрим 15 переменных (не умаляя общности, y_1, \dots, y_{15}), участвующих в системах рёбер этого пути. Легко видеть, что любой путь, ведущий вправо и соединяющий какую-либо переменную

среди y_1, \dots, y_5 с какой-либо из переменных y_{11}, \dots, y_{15} , содержит хотя бы два чёрных ребра. Значит, противоречивого пути указанного вида нет. \square

Лемма 2. *Путь, определённый последовательностью W , продолжается до эйлерова цикла.*

Доказательство. Удалим из \mathbb{P}_5 рёбра этого пути, заменив их на одно ребро из начала пути в его конец. Нам надо показать, что полученный граф сбалансирован и сильно связан. Первое очевидно; для второго (из-за сбалансированности) достаточно показать слабую связность.

Покажем, что любую последовательность из 4 символов можно продолжить вправо так, что полученная последовательность будет кончатся на 5 различных цифр, и при этом в ней не встретится подслово длины 5, разбитого так же, как какое-либо из подслов слова W .

Рассмотрим последовательность (a, b, c, d) , где некоторые символы одинаковые. Попробуем приписать справа абсолютно новый символ e , это получится, если никакое подслово W не разбито так же, как (a, b, c, d, e) . Попробуем к полученной последовательности приписать ещё один абсолютно новый символ, и так далее. Если удастся сделать так 4 раза, то мы получили что хотели. Иначе в некий момент добавление нового символа привело к появлению разбиения, соответствующего пятибуквенному подслову из W .

Что это может быть за подслово? Его последняя буква должна отличаться от остальных, значит, есть три варианта.

- (a) Появилось 12113. Тогда вместо приписывания 3 припишем 2345.
- (b) Появилось 33331. Но все рёбра, идущие из вершины, соответствующей разбиению 0000, уже входят в путь, соответствующий W , так что эту вершину следует просто удалить из нового графа.
- (c) Появилось 33312. Тогда вместо 2 припишем 3245.

Лемма доказана. \square

Эти две леммы дадут в совокупности всё, что нужно.

- С.4** Рассмотрим полный граф на n вершинах, занумерованных числами $1, 2, \dots, n$. Тогда то, что требуется сделать — этой найти в этом (неориентированном) графе эйлеров цикл. Он, очевидно, существует при нечётных n и не существует при чётных n .
- С.5** Рассмотрим окружность, разбитую на n равных частей, и пронумеруем точки разбиения последовательно числами от 1 до n . Тогда тройка чисел задаёт разбиение окружности на три дуги. Будем говорить, что два трёхэлементных подмножества *имеют один разностный тип*, если упорядоченные с точностью до циклического сдвига тройки длин этих дуг равны. (Чтобы определить длины дуг, можно упорядочить числа и найти три циклические разности.)

Пример: при $n = 8$ множества $\{1, 3, 7\}$ и $\{1, 5, 3\}$ имеют один разностный тип $(2, 2, 4)$. Множества $\{1, 2, 5\}$ и $\{1, 4, 5\}$ имеют разные типы $(1, 3, 4)$ и $(3, 1, 4)$ соответственно.

Если n не делится на 3, то количество разностных типов есть $\frac{C_n^3}{n} = \frac{(n-1)(n-2)}{6}$.

Для начала покажем, как построить требуемую в условии конструкцию при $n = 8$. Всего есть 7 разностных типов:

$$(1, 1, 6), \quad (2, 2, 4), \quad (2, 3, 3), \quad (1, 2, 5), \quad (5, 2, 1), \quad (1, 3, 4), \quad (4, 3, 1).$$

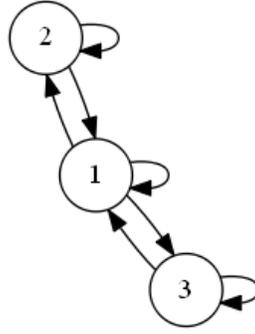
Далее мы хотим выбрать в каждом типе (x, y, z) одну из упорядоченных пар $x \rightarrow y$, $y \rightarrow z$ или $z \rightarrow x$. Сделаем в этих семи типах соответственно такой выбор:

$$1 \rightarrow 1, \quad 2 \rightarrow 2, \quad 3 \rightarrow 3, \quad 1 \rightarrow 2, \quad 2 \rightarrow 1, \quad 1 \rightarrow 3, \quad 3 \rightarrow 1.$$

Получился связный и сбалансированный ориентированный граф. В нём есть эйлеров цикл, при этом сумма чисел в цикле сравнима с 5 по модулю 8:

$$(1 \rightarrow 1 \rightarrow 2 \rightarrow 2 \rightarrow 1 \rightarrow 3 \rightarrow 3 \rightarrow 1) \rightarrow \dots$$

Запишем этот цикл в виде бесконечной периодической последовательности (a_k) . Тогда последовательность $b_k = a_1 + \dots + a_k$, взятая по модулю 8, будет периодична с периодом $7 \cdot 8 = 56$.



Покажем, что в этой последовательности любая тройка остатков по модулю 8 встречается. В самом деле, любую тройку остатков можно представить в виде $(x, x+k_1, x+k_1+k_2) \pmod 8$ так, что в последовательности a_i встречается подряд пара k_1, k_2 . Пусть $a_i = k_1, a_{i+1} = k_2$. Тогда $a_{i+8n} = k_1, a_{i+1+8n} = k_2$ для любого n . Так как $a_1 + \dots + a_8 \equiv 5 \pmod 8$, то найдётся такое n , что число $b_{8n+i-1} \equiv a_1 + \dots + a_{i-1} + n(a_1 + \dots + a_8)$ сравнимо с x по модулю 8.

Тогда тройка $b_{8n+i-1}, b_{8n+i}, b_{8n+i+1}$ — это именно то, что нам надо.

Перейдём к общей конструкции.

Лемма. Для любого $n \geq 8$, не делящегося на 3, в каждом из разностных типов можно выбрать упорядоченную пару так, чтобы $\frac{(n-1)(n-2)}{6}$ полученных рёбер образовывали сбалансированный сильносвязный орграф. (Естественно, вершинами графа будут ровно те числа, из которых выходит хотя бы одно ребро.)

Доказательство. Рассмотрим два случая.

Случай 1: n чётно. Если в разностном типе есть два одинаковых числа, мы возьмём эти два числа; получим петли $i \rightarrow i$ для всех i от 1 до $n/2 - 1$. Если же все три числа различные, выбросим наибольшее. Полученный граф на вершинах $1, \dots, n/2 - 1$ будет сбалансированным, так как вместе с каждым ребром $i \rightarrow j$ есть ребро $j \rightarrow i$, и сильно связным, так как каждое из чисел $2, \dots, n/2 - 1$ соединено рёбрами обоих направлений с 1.

Случай 2: n нечётно. Множеством вершин будут числа от 1 до $(n-1)/2$. Если в типе есть пара равных чисел, выбираем её; получается по петле на каждой из вершин. Если все три числа разные, то выбираем наибольшее число, кроме двух случаев. Эти случаи — две тройки $(2, (n-1)/2 - 1, (n-1)/2)$ и $(2, (n-1)/2, (n-1)/2 - 1)$. Для них мы выбираем соответственно $(n-1)/2 \rightarrow 2$ и $2 \rightarrow (n-1)/2$.

Полученный граф снова сбалансирован, а сильно связан он потому, что каждое число, кроме $(n-1)/2$, соединено с 1 напрямую, а $(n-1)/2$ соединено с двойкой. \square

Обозначим построенный граф через L_n ; в нём $\lfloor \frac{n-1}{2} \rfloor$ вершин и есть петля $1 \rightarrow 1$. Нам потребуется ещё один граф, который обозначим \mathbb{L}_n . В \mathbb{L}_n будет $n \lfloor \frac{n-1}{2} \rfloor$ вершин, каждая вершина кодируется парой (k, i) , где k — остаток по модулю n , i — вершина в L_n . Для каждого ребра $i \rightarrow j$ графа L_n в графе \mathbb{L}_n проводится n рёбер (по одному для каждого k) вида $(k, i) \rightarrow (k+i, j)$.

Из сбалансированности L_n следует сбалансированность \mathbb{L}_n . Покажем, что он сильно связан. Для сбалансированного графа сильная связность эквивалентна связности, поэтому достаточно показать, что из любой вершины можно добраться до $(0, 1)$. В самом деле, так как в L_n из любой вершины можно добраться до 1, то в \mathbb{L}_n из любой вершины можно попасть в вершину вида $(k, 1)$. При этом для всех k в \mathbb{L}_n есть ребро $(k, 1) \rightarrow (k+1, 1)$. Двигаясь по таким рёбрам, можно дойти до $(0, 1)$.

Итак, в \mathbb{L}_n есть эйлеров цикл. Его длина равна C_n^3 , и для любого k и любого ребра $i \rightarrow j$ графа L_n в этом цикле встретится последовательная тройка вершин $(k, i), (k+i, j), (k+i+j, *)$ (нас не интересует, что стоит на месте звёздочки). Значит, если записать последовательность первых координат вершин цикла, в этой последовательности встретится любая тройка остатков по модулю n .

D Начало перечисления

D.1 Граф $\mathcal{L}G$ связан тогда и только тогда, когда для любых двух рёбер e_1, e_2 графа G есть ориентированный путь, первым ребром которого является e_1 , а последним — e_2 .

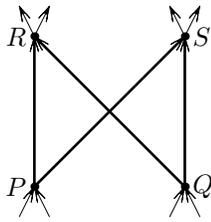
Пусть G связан и e_1, e_2 — два его ребра. Из конца e_1 можно прийти в начало e_2 по некоторой последовательности рёбер T , тогда G есть путь $e_1 T e_2$.

Пусть $\mathcal{L}G$ связан. Граф G будет связан, если любая вершина является началом некоторого ребра и концом некоторого ребра. Действительно, тогда для нахождения пути из v_1 в v_2 достаточно найти путь от ребра с началом в v_1 до ребра с концом в v_2 .

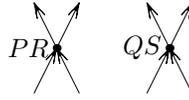
Предположим, что это не выполняется; не умаляя общности, из вершины v не выходит ни одного ребра. Так как v не изолирована, в неё входит какое-то ребро e . Кроме этого ребра, в G есть другое ребро e' . Но тогда не существует пути, первым ребром которого является e , а последним — e' . Противоречие.

D.2 В графе $\mathcal{L}G$ исходящие и входящие степени каждой вершины также равны двум. В $\mathcal{L}G$ есть вершины P, Q, R, S , из вершин P и Q идёт по ребру в R и S .

Граф $\mathcal{L}G_1$ получается из $\mathcal{L}G$ так: рёбра PS, PR, QS и QR удаляются, вершины P и R склеиваются в вершину (PR) , а вершины Q и S склеиваются в (QS) . Аналогично можно описать $\mathcal{L}G_2$: удаляются те же четыре ребра, вершины P и S склеиваются в (PS) , вершины Q и R склеиваются в (QR) .



Graph $\mathcal{L}G$



Graph $\mathcal{L}G_1$



Graph $\mathcal{L}G_2$

Рёбра PR, QS, PS и QP графа $\mathcal{L}G$ будем называть *особыми*, вершины $(PR), (QS), (PS)$ и (QP) в графах $\mathcal{L}G_1$ и $\mathcal{L}G_2$ также будем называть особыми.

Назовём *великой четвёркой* неупорядоченное множество из четырёх путей в графе $\mathcal{L}G$ таких, что их множества рёбер не пересекаются и в объединении дают все рёбра графа $\mathcal{L}G$, кроме четырёх особых. Таким образом, в каждой великой четвёрке есть по два пути, начинающиеся в R , два пути, начинающиеся в S , два пути, заканчивающиеся в Q , и два пути, заканчивающиеся в P .

В графе $\mathcal{L}G_1$ (аналогично в $\mathcal{L}G_2$) великая четвёрка соответствует четвёрке путей, содержащих все рёбра графа, начинающихся и кончающихся в особых вершинах и не содержащих особых вершин кроме начальных и конечных. Будем считать, что в графах $\mathcal{L}G, \mathcal{L}G_1$ и $\mathcal{L}G_2$ великая четвёрка одна и та же.

Каждый эйлеров цикл в $\mathcal{L}G$ особыми рёбрами разбивается на четыре куска, образующие великую четвёрку. Аналогично, эйлеров цикл в $\mathcal{L}G_1$ или $\mathcal{L}G_2$ через каждую из особых вершин проходят по два раза и разбиваются на великую четвёрку.

Задача будет решена, если мы докажем, что каждой великой четвёрке в $\mathcal{L}G$ соответствует 4 эйлерова цикла, а в $\mathcal{L}G_1$ и $\mathcal{L}G_2$ суммарно 2 эйлеровых цикла.

Великая четвёрка путей в $\mathcal{L}G$ может быть трёх типов.

- (a) По одному пути, ведущему из R в P , из R в Q , из S в P и из S в Q .
- (b) По два пути, ведущих из R в P и из S в Q .
- (c) По два пути, ведущих из R в Q и из S в P .

Разберём все случаи.

- (a) Будем обозначать пути великой четвёрки $R \dots P, R \dots Q, S \dots P$ и $S \dots Q$. Есть 6 способов циклически их упорядочить. Каждый способ можно записать в виде

$$X_1 \dots Y_1 X_2 \dots Y_2 X_3 \dots Y_3 X_4 \dots Y_4,$$

где X_i — это начала путей, а Y_i — их концы. При каждом способе возникают четыре пары вершин $Y_i X_{i+1}$. Если множества этих пар совпадают с $\{PS, PR, QS, QR\}$, то этому способу соответствует эйлеров цикл в $\mathcal{L}G$. Если получается $\{PR, PR, QS, QS\}$, то это эйлеров цикл в $\mathcal{L}G_1$, если $\{PS, PS, QR, QR\}$ — то эйлеров цикл в $\mathcal{L}G_2$. Выпишем эти способы.

- (i) $R \dots PR \dots QS \dots PS \dots Q$ — множество $\{PR, QS, QR, PS\}$, цикл в $\mathcal{L}G$;
- (ii) $R \dots PR \dots QS \dots QS \dots P$ — множество $\{PR, QS, QS, PR\}$, цикл в $\mathcal{L}G_1$;
- (iii) $R \dots PS \dots PR \dots QS \dots Q$ — цикл в $\mathcal{L}G$;
- (iv) $R \dots PS \dots PS \dots QR \dots Q$ — цикл в $\mathcal{L}G_2$;
- (v) $R \dots PS \dots QR \dots QS \dots P$ — цикл в $\mathcal{L}G$;
- (vi) $R \dots PS \dots QS \dots PR \dots Q$ — цикл в $\mathcal{L}G$.

Итак, имеем 4 цикла в $\mathcal{L}G$ и по циклу в $\mathcal{L}G_1$ и $\mathcal{L}G_2$.

- (b) Всё происходит так же, как в предыдущем пункте, но у двух пар путей будет одинаковое обозначение: два (разных) пути $R \dots P$ и два разных пути $S \dots Q$.

- (i) $R \dots PR \dots PS \dots QS \dots Q$ — цикл в $\mathcal{L}G$;
- (ii) $R \dots PR \dots PS \dots QS \dots Q$ — снова цикл в $\mathcal{L}G$. Хотя написано то же самое, следует иметь в виду, что это другой порядок, так как два из путей великой четвёрки переставлены.
- (iii) $R \dots PS \dots QR \dots PS \dots Q$ — цикл в $\mathcal{L}G_2$;
- (iv) $R \dots PS \dots QS \dots QR \dots P$ — цикл в $\mathcal{L}G$;
- (v) $R \dots PS \dots QR \dots PS \dots Q$ — цикл в $\mathcal{L}G_2$;
- (vi) $R \dots PS \dots QS \dots QR \dots P$ — цикл в $\mathcal{L}G$.

4 цикла в $\mathcal{L}G$ и два цикла в $\mathcal{L}G_2$.

- (c) Полностью аналогично предыдущему пункту.

D.3 Ответ: $2^{2^{n-1}-n}$,

Мы приводим решение, предложенное А. Зиминим.

Понятно, что $B(2, n) = \epsilon(G(2, n))$. Будем доказывать по индукции, что $\epsilon(G(2, n)) = \frac{2^{2^{n-1}}}{2^n}$.

Несложно понять, что $\mathcal{L}G(2, n) = G(2, n+1)$. В самом деле, вершины $G(2, n+1)$ соответствуют рёбрам $G(2, n)$, а рёбра $G(2, n+1)$ соответствуют бинарным словам длины $n+1$, то есть путям в $G(2, n)$ длины 2.

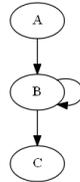
Лемма. Пусть орграф G содержит n вершин, исходящие и входящие степени всех вершин равны 2. Тогда $\epsilon(\mathcal{L}G) = 2^{n-1} \epsilon(G)$.

Заметим, что индукционный переход мгновенно следует из леммы: в $G(2, n)$ число вершин равно 2^{n-1} , поэтому

$$\epsilon(\mathcal{L}G(2, n)) = 2^{2^{n-1}-1} 2^{2^{n-1}-n} = \frac{2^{2^n}}{2^{n+1}}.$$

Доказательство леммы. Будем доказывать лемму индукцией по количеству вершин. База: $n = 1$. Такой граф является вершиной с двумя петлями, в нём один эйлеров обход, в его рёберном графе, как несложно убедиться, тоже.

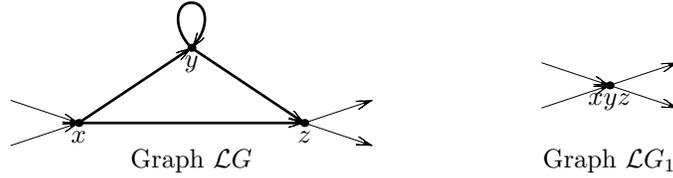
Переход $n \rightarrow n+1$. Пусть в G есть вершина с двумя петлями, тогда она даёт отдельную компоненту связности и у обоих графов нет эйлеровых циклов.



Пусть в G есть вершина B с петлёй. Тогда в эйлеровом цикле после прохода по ребру AB нужно идти по петле $B \rightarrow B$, а после по ребру $B \rightarrow C$. Заменой вершины B на ребро AC получим граф G_1 .

При этом $\epsilon G = \epsilon G_1$. Графы $\mathcal{L}G$ и $\mathcal{L}G_1$ отличаются в одном фрагменте, как показано на рисунке ниже ($x = A \rightarrow B, y = B \rightarrow B, z = B \rightarrow C$).

Каждому эйлерову циклу в $\mathcal{L}G_1$ соответствуют два цикла в $\mathcal{L}G$: дважды входим и выходим в вершину xyz и в $\mathcal{L}G$ есть два способа её обойти: $x \rightarrow y \circlearrowleft y \rightarrow z$ и $x \rightarrow z$. Два цикла получаются в зависимости от того, в каком порядке мы их применяем.



Тогда

$$\epsilon(G) = \epsilon(G_1) = \frac{1}{2^{n-1}} \epsilon(\mathcal{L}G_1) = \frac{1}{2^n} \epsilon(\mathcal{L}G).$$

Посмотрим теперь на вершину, в которой нет петель. Построим графы G_1 и G_2 , как в задаче **D2**. В каждом из них по $n - 1$ вершине и они удовлетворяют условию леммы. Каждый эйлеров цикл в G соответствует одному циклу в G_1 или в G_2 . Итак, $\epsilon(G) = \epsilon(G_1) + \epsilon(G_2)$,

$$\epsilon(\mathcal{L}G) = 2(\epsilon(\mathcal{L}G_1) + \epsilon(\mathcal{L}G_2)) = 2 \cdot 2^{n-1} (\epsilon(G_1) + \epsilon(G_2)) = 2^n \epsilon(G).$$

Лемма доказана.

Е Торы де Брейна

Общее замечание. В этой секции мы будем рассматривать буквы алфавита $X_k = \{1, 2, \dots, k\}$ как остатки по модулю k , чтобы с ними можно было производить арифметические операции. Имея дело с клетчатой решеткой, мы обычно будем обозначать j -ю клетку в i -й строке через (i, j) .

Е.1 Для удобства построим тор типа $(k, k^{u-1}, 1, u)_k$ и отразим его относительно главной диагонали.

Для начала предположим, что $u \geq 3$. Пусть $c_1, c_2, c_3, \dots, c_{k^{u-1}}$ - последовательность де Брейна ранга $u - 1$ над алфавитом $X_k = \{1, 2, \dots, k\}$; продолжим ее, чтобы получить бесконечную k^{u-1} -периодическую последовательность. Поставим в клетку (i, ℓ) , $\ell > 0$, решетки число

$$a_{i,\ell} = i + \sum_{s=1}^{\ell} c_s$$

(сложение происходит по модулю k). Аналогично продолжим расстановку и для $\ell \leq 0$.

Каждое число встречается в периоде $c_1, c_2, \dots, c_{k^{u-1}}$ ровно k^{u-2} раз; так как $u \geq 3$, сумма $\sum_{s=1}^{k^{u-1}} c_s$ делится на k . Тогда расстановка действительно является k^{u-1} -периодической по горизонтали и k -периодической по вертикали, то есть дает тор искомого размера. (Обратите внимание, что периодичность также выполняется для $u = 2$ и нечетного k .)

Остается показать, что каждые u чисел x_0, \dots, x_{u-1} встречаются подряд в некоторой строке. Поскольку (c_i) - последовательность де Брейна, найдется ℓ , для которого $c_{\ell+i} = x_i - x_{i-1}$ при $i = 1, \dots, u - 1$. Поскольку числа $a_{1,\ell}, \dots, a_{k,\ell}$ попарно различны, найдется r такой что $a_{r,\ell} = x_0$. По нашей конструкции

$$a_{r,\ell+i} = a_{r,\ell} + \sum_{s=1}^i c_{\ell+s} = x_0 + \sum_{s=1}^i (x_s - x_{s-1}) = x_i,$$

то есть мы нашли необходимый прямоугольник $1 \times u$.

Теперь рассмотрим случай $u = 2$ и $k \geq 3$. Нам нужно заполнить строки тора $k \times k$ числами $1, 2, \dots, k$, так что каждая пара чисел встречается подряд в некоторой строке. В терминах графа де Брейна $G(2, k)$, определенного в решении задачи **В.5**, нам нужно разбить ребра этого графа на k циклов длины k .

Если k нечетно, $k = 2t + 1$, можно использовать циклы

$$(a \rightarrow (a + 1) \rightarrow a \rightarrow (a + 2) \rightarrow a \rightarrow \dots \rightarrow a \rightarrow (a + t) \rightarrow a \rightarrow a)$$

при $a = 1, 2, \dots, k$. (В этом случае также проходит и предыдущий метод.)

Если k четно, $k = 2t$, мы можем начать с циклов

$$C_a = (a \rightarrow (a + 1) \rightarrow a \rightarrow (a + 2) \rightarrow a \rightarrow \dots \rightarrow a \rightarrow (a + t - 1) \rightarrow a)$$

при $a = 1, 2, \dots, 2t$. Длина каждого из этих циклов равна $2t - 2$, и они покрывают все ребра кроме ребер вида $x \rightarrow x$ и $x \rightarrow x + t$. Несложно проверить, что можно добавить к циклу C_{2i-1} ребра $(t + i - 1) \rightarrow (i - 1) \rightarrow (t + i - 1)$, а к циклу C_{2i} две петли $2i \rightarrow 2i$ и $(2i + 1) \rightarrow (2i + 1)$. Получим искомое разбиение.

Е.2 Пусть $\dots, c_1, c_2, \dots, c_{k^2}, \dots$ - периодически продолженная в обе стороны последовательность де Брейна ранга 2 над алфавитом X_k . Мы поместим в строки решетки сдвиги этой последовательности. В i -й строке запишем последовательность, сдвинутую вправо на $0 + 1 + \dots + (i - 1)$ клеток. То есть i -я строка будет представлять собой $i - 1$ -ю, сдвинутую на $i - 1$. По сравнению с первой строкой $(k^2 + 1)$ -я сдвинута на $1 + 2 + \dots + k^2$; что делится на k^2 , то есть расстановка действительно задает тор $k^2 \times k^2$.

Для любого квадрата 2×2 , его нижний и верхний ряды встречаются в последовательности де Брейна. Если верхний ряд встречается на расстоянии s влево от нижнего, то искомый квадратик встретится в объединении s -й и $s + 1$ -й строк.

Е.3 Для решения этой задачи можно модифицировать метод из предыдущей. Опять же, будем строить тор $(k^{u(v-1)}, k^u, v, u)_k$. Пусть $R = k^{u(v-1)}$ и $S = k^u$.

Возьмем последовательность де Брейна ранга u (с периодом длины S). Мы будем записывать ее сдвиги в строки, причем сдвинем i -ю строку относительно $i - 1$ -й на d_i вправо (то есть i -я строка будет сдвинута относительно нулевой на $d_1 + \dots + d_i$). Для того, чтобы расстановка была R -периодичной по вертикали, нам нужно условие $d_{i+R} = d_i$ и чтобы сумма $d_1 + \dots + d_R$ делилась на S . Чтобы получить все возможные прямоугольники $v \times u$, просто нужно, чтобы все последовательности из $v - 1$ сдвигов встречались в последовательности (d_i) . Тогда в качестве (d_i) можно взять последовательность де Брейна ранга $v - 1$ над алфавитом X_S .

Но сумма чисел в периоде (d_i) равна

$$k^{u(v-2)} \cdot (1 + 2 + \dots + k^u),$$

и это число делится на k^u для $k, u, v \geq 2$, за исключением случая, когда $v = 2$ и k четно.

Е.4 Решение для случая $k = 2$ уже было приведено для задачи **А.3а**); поэтому будем предполагать, что $k \geq 4$.

Шаг 1. Построим последовательность де Брейна $C = (c_1, \dots, c_{k^2})$ ранга 2 с дополнительным условием $c_{k^2/2} = c_{k^2}$. Рассмотрим граф де Брейна $G(2, k)$ и разобьем его ребра на группы $M_i = \{(\ell, \ell + i) : \ell = 1, 2, \dots, k\}$. Распределим эти группы на два равных семейства, так чтобы M_1 и M_{k-1} были в разных семействах. То есть мы разделили все ребра между двумя подграфами, каждый из которых сильно связный и сбалансированный.

Возьмем эйлеровы циклы в этих подграфах и склеим их в общей вершине v . Мы получим эйлеров цикл во всем графе, который дает нужную последовательность.

Шаг 2. Теперь сделаем почти такую же процедуру как в **Е.2**. Рассмотрим построенную последовательность C и обозначим через A и B ее первую и вторую половины. Заметим, что каждая последовательность из двух букв встречается либо в последовательности с периодом A , либо в последовательности с периодом B . (Здесь как раз пригождается дополнительное свойство последовательности)

Поставим последовательность с периодом C в строки с номерами с 4 по k^2 , так что относительные сдвиги двух соседних строк принимают значения от 0 до $k^2 - 1$, кроме 0, 1, $k^2/2$, и $k^2/2 + 1$. Сумма всех чисел от 0 до $k^2 - 1$ сравнима с $k^2/2$ по модулю k^2 , так что k^2 -я (как и нулевая) строка будет сдвинута относительно четвертой на $k^2/2 - 2$.

Поместим во вторую строку ту же самую последовательность, сдвинув ее на одну клетку влево относительно четвертой строки. Наконец, поместим последовательность с периодом A в первую строку и

последовательность с периодом B в третью строку. Сдвинем их так, чтобы части A в первой и второй строке были строго одна над другой и то же самое для частей B в третьей и четвертой строках (см. рисунок).

Поскольку мы несколько изменили расстановку по сравнению с **Е.2**, необходимо проверить, что квадратики 2×2 в строках с нулевой по четвертую такие же, как они были бы при использовании обычных последовательностей де Брейна с относительными сдвигами $0, 1, k^2/2$, и $k^2/2 + 1$. Легко видеть, что квадратики в строках 1–2 и 3–4 такие же, как они были бы для обычных строк де Брейна с относительными сдвигами на 0 и $k^2/2$, тогда как квадратики в строках 0–1 и 2–3 такие же, как они были бы в парах строк со сдвигами на 1 и $k^2/2 + 1$.

$$\begin{array}{c} \vdots \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \\ 0 \\ \vdots \end{array} \left\{ \begin{array}{|c|c|c|c|} \hline & A & B & A & B \\ \hline A & & & & \\ \hline B & & & & \\ \hline A & B & A & B & \\ \hline A & A & A & A & \\ \hline B & A & B & A & \\ \hline \end{array} \right\} \sim \left\{ \begin{array}{|c|c|c|c|} \hline B & A & B & A \\ \hline A & B & A & B \\ \hline B & A & B & A \\ \hline B & A & B & A \\ \hline B & A & B & A \\ \hline \end{array} \right.$$

Е.5 Есть несколько подобных конструкций. Мы изложим ту, которая использует задачу **Е.6**

Предположим, что $k > 2$. Возьмем тор де Брейна типа $(k^2, k^2, 2, 2)_k$, построенный в **Е.2** (для нечетных k) или в **Е.4** (для четных k). Можно проверить, что в обеих конструкциях сумма буква в каждой строке 0 (это почти тривиально для обычной последовательности де Брейна, для половинок из задачи **Е.4** нужно вспомнить явную конструкцию). Тогда можно применить **Е.6** к этому тору и отразить относительно диагонали, чтобы получить нужный тор типа $(k^4, k^2, 2, 3)_k$.

К сожалению, этот метод не работает для $k = 2$, поскольку в (в сущности единственной) конструкции тора де Брейна типа $(4, 4, 2, 2)_2$ суммы по строкам нечетны. Но можно применить следующий подход. Два столбца тора $(4, 4, 2, 2)_2$ содержат все восемь различных прямоугольников 3×1 , то есть нужно скомпоновать их так, чтобы получить все возможные сочетания. Одна из таких расстановок приведена на картинке снизу.

1	1	0	0	1	0	1	1	1	0	0	1	1	0	1	1
0	0	1	1	0	1	1	1	0	0	1	1	0	0	1	0
0	0	1	1	0	0	0	1	0	1	1	0	0	0	0	1
0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1

Е.6 Для последующего применения мы докажем более общее утверждение, в котором R и S не обязательно степени k , но просто натуральные числа, для которых $RS = k^{uv}$. Рассуждение будет похоже на то, которое применялось для **Е.1**.

Шаг 1. Теперь нам нужно построить последовательность длиннее, чем обычная последовательность де Брейна. А именно, нам понадобится циклическая последовательность букв алфавита X_k с периодом $p_1, p_2, \dots, p_{Sk^v}$, такая что для любого слова $x_1 \dots x_v$ и числа $\ell = 1, 2, \dots, S$ найдется такое $i \equiv \ell \pmod{S}$, такое что $p_{i+1} = x_1, p_{i+2} = x_2, \dots, p_{i+v} = x_v$. То есть любое слово длины v в алфавите X_k встретится ровно S раз в периоде.

Чтобы доказать это, рассмотрим другой граф G' . Его вершины будут иметь вид $(w; i)$, где w - слово длины $v - 1$ в алфавите X_k , а $i \in \{1, 2, \dots, S\}$ (мы будем рассматривать индексы i как остатки по модулю S). Если обычный граф де Брейна $G(v, k)$ содержит ребро из w_1 в w_2 , проведем ребро из $(w_1; i)$ в $(w_2; i+1)$ для любого $1, 2, \dots, S$. Очевидно, что G' сбалансирован и сильно связан, то есть в нем найдется эйлеров цикл. Посмотрев на этот цикл как на слово, мы получим нашу последовательность. Нужное слово $x_1 \dots x_v$ в позиции, сравнимой с i по модулю S , в точности соответствует ребру $(x_1 \dots x_{v-1}; i) \rightarrow (x_2 \dots x_v; i+1)$.

Шаг 2. Теперь построим нужный тор типа $(R, Sk^v, u, v)_k$. Обозначим через $a_{i,j}$ букву в позиции (i, j) в данном торе. Рассмотрим клетку (I, J) в новом торе и пусть $j = J \pmod{S}$. Тогда мы поставим в эту

клетку число

$$A_{I,J} = p_J + \sum_{m=1}^I a_{m,j}.$$

Из-за условий, наложенных на первоначальный тор, новая расстановка R -периодична по вертикали. Очевидно, что она также Sk^v -периодично по горизонтали.

Каждая строка нового тора удовлетворяет тем же условиям, что и последовательность, построенная в Шаге 1. Действительно, подслово из $of(p_j)$ в позициях, сравнимых с i по модулю S - это просто всевозможные слова, и при переходе к другой строке в тех же местах будут встречаться эти слова, к которым покомпонентно прибавлено фиксированное слово.

Легко видеть, что построенный тор содержит любой прямоугольник $(u+1) \times v$. Пусть $(x_{i,j})$ - расположение чисел в таком прямоугольнике. Пусть $y_{i,j} = x_{i+1,j} - x_{i,j}$. Расстановка $(y_{i,j})$ встречается где-то в старом торе, скажем, в позиции с $(\alpha + 1, \beta + 1)$ по $(\alpha + u, \beta + v)$. Тогда новый тор содержит необходимую расстановку в одной из k^v позиций $(\alpha + 1, \beta + 1 + \mu S) - (\alpha + u + 1, \beta + v + \mu S)$ при $\mu = 0, 1, \dots, k^v - 1$, аналогично **Е.1**.

Замечание. Исходя из свойств строк несложно заметить, что суммы в строках полученного тора делятся на k . Поэтому можно применить это действие несколько раз, каждый раз отражая получившийся тор относительно главной диагонали.

Более того, можно показать, что достаточно отражать через раз, если Sk^{v-2} делится на k . Действительно, пусть p_1, \dots, p_{Sk^v} - период в некоторой строке в торе, получившемся после первой итерации. Столбец после второй итерации будет иметь вид

$$\alpha, \quad \alpha + p_1, \quad \alpha + (p_1 + p_2), \quad \dots, \quad \alpha + (p_1 + \dots + p_{Sk^{v-1}}).$$

Сумма этих чисел сравнима по модулю k с

$$-p_1 - 2p_2 - \dots - (Sk^v - 1)p_{Sk^v-1} \equiv -(p_1 + p_{k+1} + \dots + p_{Sk^v-k+1}) - 2(p_2 + p_{k+2} + \dots + p_{Sk^v-k+2}) - \dots$$

В каждой скобке любая буква встречается Sk^{v-2} раз; это число делится на k , то есть общая сумма также делится на k .

Е.7 Начав с конструкции из **Е.5**, применим **Е.6** трижды, чтобы получить

$$(k^4, k^2, 2, 3)_k \xrightarrow{(1)} (k^4, k^5, 3, 3)_k \xrightarrow{(2)} (k^4, k^8, 4, 3)_k \xrightarrow{(3)} (k^8, k^8, 4, 4)_k;$$

иногда отражая. Чтобы доказать, что **Е.6** применимо в данном случае, нам нужно показать, что соответствующие суммы в строке/столбце делятся на k на каждом из трех шагов. Для шага (3) это следует из замечания после **Е.6**. Если $k > 2$, то то же выполнено для шагов (1) и (2), мы получали тор $(k^4, k^2, 2, 3)_k$ по тому же алгоритму. В исключительном случае $k = 2$, можно проверить необходимое условие вручную (картинка в конце **Е.5**).

В этом месте стоит сказать, что не все торы типа $(k^4, k^2, 2, 3)_k$ удовлетворяют необходимому условию.

Е.8 Для начала докажем утверждение для четных $n = 2t$ индукцией по t . Случаи $t = 1, 2$ уже разбирались выше.

Предположим, что тор типа $(k^{2t^2}, k^{2t^2}, 2t, 2t)$ уже был построен, и **Е.6** было применено несколько раз, чтобы увеличить вертикальную сторону тора. Тогда достаточно применить **Е.6** еще несколько раз

$$\begin{aligned} (k^{2t^2}, k^{2t^2}, 2t, 2t)_k &\longrightarrow (k^{2t^2}, k^{2t(t+1)}, 2t+1, 2t)_k \\ &\longrightarrow (k^{2t^2+2t+1}, k^{2t(t+1)}, 2t+1, 2t+1)_k \\ &\longrightarrow (k^{2(t+1)^2}, k^{2t(t+1)}, 2t+1, 2t+2)_k \\ &\longrightarrow (k^{2(t+1)^2}, k^{2(t+1)^2}, 2t+2, 2t+2)_k. \end{aligned}$$

Каждый раз утверждение **Е.6** применимо благодаря замечанию после доказательства.

Предположим, что n нечетно, но k - точный квадрат, то есть $n = 2t + 1$ и $k = a^2$, a нечетно. Тогда можем провести похожую индукцию. Для базового случая $t = 0$, достаточно расположить $1, 2, \dots, a^2$ в клетках

квадрата $a \times a$, так чтобы сумма в каждом столбце делилась бы на a^2 (нам нужно это условие, чтобы применить **Е.6**). Для этого нужно разбить эти числа на a групп с равными суммам, что как известно возможно.

Для шага индукции предположим, что тор типа $(a^{(2t+1)^2}, a^{(2t+1)^2}, 2t+1, 2t+1)_k$ уже построен, и **Е.6** было применено в прошлый раз, чтобы увеличить вертикальную сторону тора (если вообще было применено). Тогда достаточно применить **Е.6** следующим образом

$$\begin{aligned} (a^{(2t+1)^2}, a^{(2t+1)^2}, 2t+1, 2t+1)_k &\longrightarrow (a^{(2t+1)^2}, a^{(2t+1)(2t+3)}, 2t+2, 2t+1)_k \\ &\longrightarrow (a^{2t^2+8t+5}, a^{(2t+1)(2t+3)}, 2t+2, 2t+2)_k \\ &\longrightarrow (a^{(2t+3)^2}, a^{(2t+1)(2t+3)}, 2t+2, 2t+3)_k \\ &\longrightarrow (a^{(2t+3)^2}, a^{(2t+3)^2}, 2t+3, 2t+3)_k. \end{aligned}$$

Опыт-таки, применимость следует из замечания.

Е.9 Случай четного n полностью аналогичен этому случаю в предыдущей задаче.

Предположим, что $n = 2t + 1$ и $k = a^2$, a четно. Если $n = 1$, то утверждение очевидно. Для $n \geq 3$, мы также используем индукцию по t , но нам надо сперва проверить случай $t = 1$. Мы проверим его при помощи **Е.10**. По этой задаче найдется тор де Брейна типа $(a^5, a^3, 2, 2)$. Кроме того, анализ конструкции в **Е.10** показывает, что сумма чисел в каждой строке делится на k . То есть мы можем применить **Е.6** дважды, чтобы получить

$$(a^5, a^3, 2, 2)_k \longrightarrow (a^9, a^3, 2, 3)_k \longrightarrow (a^9, a^9, 3, 3)_k,$$

как и требовалось.

Шаг индукции доказывается в точности как в предыдущей задаче.

Е.10 Как обычно, введем обозначения $k = 2st$, $R = 4st^2$, $S = 4s^3t^2$.

Шаг 1. Найдем s циклических последовательностей L_1, L_2, \dots, L_s , каждая длины $R = k^2/s$, таких что любое двухбуквенное слово в алфавите X_k встречается как подслово ровно в одной из этих последовательностей. Это может быть сделано в точности как в шаге 1 из **Е.4**, только теперь нужно разбить все ребра на s групп G_1, \dots, G_s , каждая из R ребер, так что эти группы дают сбалансированные сильно связанные подграфы. Эйлеровы циклы в этих подграфах тогда дают искомые последовательности.

Мы снова разбиваем ребра $G(2, k)$ на k групп $M_i = \{(\ell, \ell + i) : \ell = 1, 2, \dots, k\}$. В начале мы распределяем в G_i ребра групп M_{i-1} и M_{k-i} ; из этого уже следует, что все подграфы будут сильно связны. Затем мы распределяем остальные группы поровну между G_i -ми. Это завершает построение.

Шаг 2. Теперь мы построим нужный тор. Каждый столбец будет содержать лишь одну из последовательностей L_1, \dots, L_s , сдвинутую некоторым образом. Мы фиксируем начальный элемент каждой из последовательностей L_i ; после чего можно говорить о сдвигах любых из них друг относительно друга.

Пусть $C = (c_1, \dots, c_s)$ - последовательность де Брейна ранга 2 над алфавитом X_s . Теперь заполним столбцы следующим образом. Пусть I - номер столбца, и i - его остаток по модулю s^2 , так что $I = i + s^2 \cdot j$. Тогда этот столбец будет содержать L_{c_i} , и будет сдвинут на j относительно предыдущего столбца.

Рассмотрим столбцы с нулевого по S -й. Мы утверждаем, что любой квадратик 2×2 встречается в этих столбцах. Действительно, для любых двух индексов i, i' последовательность L_i будет следовать за $L_{i'}$ ровно R раз, и все эти относительные сдвиги будут различны; это доказывает наше утверждение.

Остается найти период нашей расстановки. Поскольку $S = Rs^2$, S -й столбец будет сдвинут относительно нулевого на $(0 + 1 + \dots + (R - 1)) \cdot s^2$. Если s четно, то это число делится на R , то есть мы получили тор с периодами R и S .

Предположим, что s нечетно. Тогда, к сожалению, общий сдвиг делится только на $R/2$. Но в этом случае мы можем применить ту же модификацию, что и в **Е.4**. А именно, в шаге 1 мы можем разбить одну из групп G_i (скажем, G_2) на две сбалансированные сильно связанные половинки. Тогда соответствующая последовательность L_2 также может быть построена так, чтобы состоять из двух половинок, заканчивающихся на одну и ту же букву. Тогда можно применить тот же трюк, что и в **Е.4**. Детали остаются читателю для проверки.

Примечание: Для решения этой задачи можно применить и другую конструкцию.

Ф Продолжение перечисления

Ф.1 Зафиксируем некоторое ребро, выходящее из v , и будем считать, что оно является первым в любом эйлеровом цикле. Рассмотрим произвольный эйлеров цикл C . Для каждой вершины $u \neq v$, отметим последнее ребро этого цикла, выходящее из u . Обозначим подграф из отмеченных рёбер через T .

Предположим, что в T нашёлся неориентированный цикл ω ; так как исходящая степень каждой вершины в T равна единице, ω также является ориентированным циклом. Возьмем в ω ребро e , которое встречается в C последним. Пусть $u = t(e)$; заметим, что $u \neq v$, ибо в графе T из v не выходит рёбер. Но тогда ребро f цикла ω , выходящее из u , должно встречаться в C позже; в противном случае при построении C после ребра e уже не получится выйти из u , а закончиться цикл должен в v . Это противоречие показывает, что T ацикличесок. Значит, если пойти из любой вершины графа G по отмеченным ребрам, рано или поздно мы придём в вершину, из которой рёбер не идёт, а это может быть только v . Таким образом, T является ориентированным остовным деревом с корнем в v .

Итак, каждому эйлерову циклу C мы сопоставили ориентированное остовное дерево T ; посчитаем, скольким циклам соответствует T . Оно соответствует тем эйлеровым циклам, которые, выйдя из v по фиксированному ребру, проходили по какому-то ребру дерева T только тогда, когда это ребро оставалось единственной возможностью продолжить обход; сейчас мы научимся восстанавливать все эти циклы.

В каждой вершине $u \neq v$ есть ровно $(outdeg(u) - 1)!$ способов установить порядок, в котором цикл должен проходить по исходящие из u ребрам не из T (оставшееся ребро обязано быть последним). В вершине v есть ровно $(outdeg(v) - 1)!$ способов установить порядок, в котором цикл должен проходить исходящие ребра после фиксированного. Покажем, что любому выбору этих порядков действительно соответствует эйлеров цикл.

Выйдем из v по фиксированному ребру и пойдём по ребрам, придерживаясь порядков во всех вершинах, пока не остановимся. Произойти это может только в вершине v ; обозначим полученный цикл через C . Предположим, что C не прошёл по какому-то ребру из вершины u ; тогда он не прошёл и по ребру e графа T , выходящему из u . Рассмотрев в T путь из u в v , мы найдём в T такие ребра e_1 и e_2 , что $t(e_1) = s(e_2)$, а C прошёл по e_2 , но не по e_1 . Но тогда все рёбра из $s(e_2)$ должны принадлежать C , однако ребро e_1 , входящее в неё, не принадлежит C . Это противоречит сбалансированности G .

Таким образом, данному дереву соответствует ровно $\prod_{u \in V(G)} (outdeg(u) - 1)!$ разных циклов, откуда и следует утверждение задачи.

Замечание. В качестве следствия мы немедленно получаем, что в сильно связном сбалансированном ориентированном графе число ориентированных остовных деревьев с данным корнем не зависит от выбора корня.

Ф.2 Ответ. $B(k, n) = k!^{k^{n-1}} / k^n$.

Из предыдущей задачи следует, что число $B(k, n)$ ровно в $(k-1)!^{k^{n-1}}$ раз больше числа ориентированных остовных деревьев с фиксированным корнем в графе де Брейна $G(k, n)$, то есть $B(k, n)$ в $\frac{(k-1)!^{k^{n-1}}}{k^{n-1}}$ раз больше общего числа $\tau(G(k, n))$ ориентированных остовных деревьев. Докажем индукцией по n , что $\tau(G(k, n)) = k^{k^{n-1}-1}$; отсюда немедленно воспоследует ответ.

База для $n = 1$ очевидна. Заметим, что $G(k, n+1) = \mathcal{L}G(k, n)$. Тогда, подставив в тождество Левина единицы вместо всех переменных, получим

$$\tau(G(k, n+1)) = \tau(G(k, n)) \cdot k^{(k-1)k^{n-1}},$$

откуда и следует переход индукции.

Ф.3 Доказательство приводится по статье Н. Bidkhorі, S. Kishore. A bijective proof of a theorem of Knuth. *Combinatorics, Probability and Computing*, vol. 20, is. 01, 2011, и картинки позаимствованы оттуда же.

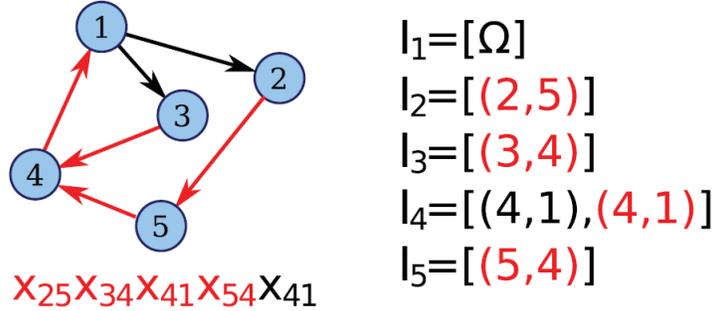
Раскроем все скобки в обеих частях предполагаемого равенства и докажем, что получаются одинаковые наборы мономов. Для этого нам потребуется следующее понятие.

Определение Ф.3 *Древесным массивом в графе G будем называть набор из упорядоченных списков ℓ_v для каждой вершины v , удовлетворяющий следующим условиям:*

а) Каждый список l_v имеет длину $\text{indeg}(v)$. Все элементы этого списка — ребра, исходящие из v (возможно, с повторами), за исключением последнего элемента ровно одного из списков, соответствующего некоторой вершине v_0 ; этот элемент является символом Ω .

б) Последние элементы всех остальных списков образуют ориентированное остовное дерево с корнем в вершине v_0 .

На рисунке ниже показан пример древесного массива.



Сопоставим каждому древесному массиву моном, в который каждая переменная x_e входит в такой степени, сколько раз ребро e содержится в массиве. Нетрудно видеть тогда, что древесные массивы в точности соответствуют мономам из правой части требуемого равенства (при этом массивы, в которых последние ребра списков образуют фиксированное дерево, соответствуют мономам, полученным из монома этого дерева из $\kappa^{\text{edge}}(G)$).

Таким образом, для доказательства нашего равенства достаточно построить биекцию между древесными массивами в G и остовными деревьями в $\mathcal{L}G$, при которой каждому дереву в $\kappa^{\text{vertex}}(\mathcal{L}G)$ соответствует тот же моном, который сопоставлен соответствующему ему древесному массиву. Пусть \mathcal{A} — множество всех древесных массивов в G , а \mathcal{T} — множество всех остовных ориентированных деревьев в $\mathcal{L}G$. Тогда мы собираемся построить алгоритмически взаимно-обратные отображения

$$\Sigma : \mathcal{A} \rightarrow \mathcal{T} \quad \text{и} \quad \Pi : \mathcal{T} \rightarrow \mathcal{A},$$

обладающие вышеуказанным свойством.

Пронумеруем все ребра G произвольным образом.

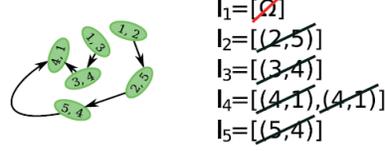
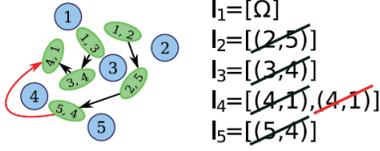
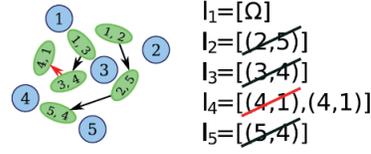
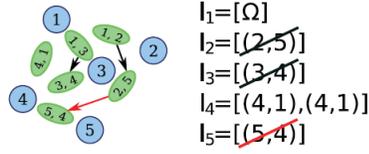
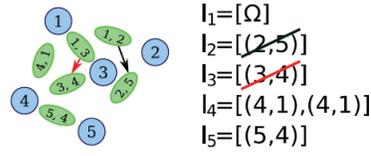
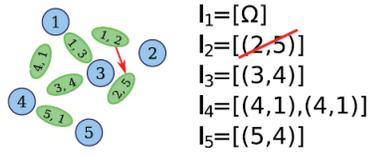
Построение Σ . Рассмотрим массив $A \in \mathcal{A}$. Будем наращивать подграф T графа $\mathcal{L}G$ шаг за шагом, соответственно уменьшая A . Мы начнём с пустого T ; когда A опустеет, определим $\Sigma(A)$ как получившийся подграф T . Обозначим текущее состояние массива A и подграфа T после k -го шага через $A(k)$ и $T(k)$ соответственно.

На $(k+1)$ -м шаге выберем ребро e с наименьшим номером, не входящее в $A(k)$ и имеющее нулевую исходящую степень в $T(k)$. Пусть g — первый элемент из списка $l_{t(e)}$ (в массиве $A(k)$). Определим $A(k+1)$, выкинув g из начала этого списка. Если $g = \Omega$, то закончим алгоритм, в противном случае добавим ребро $e \rightarrow g$ к графу $T(k)$, получая $T(k+1)$. На рисунке ниже показана работа этого процесса для того же древесного массива.

Пусть в G имеется d ребер. После k шагов найдутся k ребер, имеющих ненулевую исходящую степень в $T(k)$, а массив $A(k)$ будет содержать не более $d-1-k$ различных ребер. Значит, на $(k+1)$ -м шаге можно будет выбрать искомое ребро e . При этом список $l_{t(e)}$ окажется не пустым, поскольку длина этого списка уменьшалась ровно тогда, когда использовалось входящее в $l_{t(e)}$ ребро, то есть не более, чем $\text{indeg}(t(e)) - 1$ раз.

Покажем, что в T нет ориентированных циклов. Действительно, если мы уже добавили к подграфу T рёбра $e_1 \rightarrow e_2, \dots, e_{n-1} \rightarrow e_n$, то после этого добавить ребро $e_n \rightarrow e_1$ и замкнуть цикл нельзя, ибо уже в момент добавления ребра $e_1 \rightarrow e_2$ ребро e_1 отсутствовало в массиве.

Пусть теперь M — дерево в G , состоящее из последних ребер массива A , а r — его корень. Пусть $e = (u, w)$ — произвольное ребро в M (это ребро лежит в l_u). Предположим, что в некоторый момент процесса



список ℓ_v опустел. Тогда в T уже есть рёбра, выходящие из всех рёбер графа G с концом в v ; в частности, исходящая степень ребра e в графе T не равна нулю. Это значит, что оно было выбрано раньше, и в момент его выбора оно уже отсутствовало в A . Тогда в этот момент список ℓ_u был уже пуст. Итак, если список ℓ_v в какой-то момент опустел, то список ℓ_u опустел до этого.

Из этого следует, что в момент, когда опустеет список ℓ_r , все остальные списки должны быть уже пустыми. Значит, алгоритм закончится ровно через d шагов, и $T = \Sigma(A)$ будет ориентированным остовным деревом. Несложно заметить, что получившееся дерево будет соответствовать тому же моному.

Построение П. Рассмотрим теперь ориентированное остовное дерево $S \in \mathcal{T}$ с корнем r . Начнем с пустого массива B и будем шаг за шагом увеличивать его, убирая ребра из S . Обозначим текущее состояние массива B и подграфа S через k шагов через $B(k)$ и $S(k)$ соответственно.

На k -м шаге рассмотрим все вершины в $S(k)$, исходящие степени которых равны 1, а входящие равны 0, и выберем среди них вершину e с наименьшим номером (напомним, что вершины $S(k)$ являются рёбрами в G). Пусть $e \rightarrow f$ — ребро графа $S(k)$, выходящее из e . Удалим это ребро из S и добавим f в конец списка $\ell_{t(e)}$. Когда в S не останется рёбер (что произойдёт через $d - 1$ шагов), добавим Ω в конец списка $\ell_{t(r)}$.

Когда алгоритм прервется, длина каждого списка ℓ_v в B будет равна $\text{indeg}(v)$. Рассмотрим подграф M графа G , образованный последними ребрами всех списков. Пусть в нем есть ребро $f = (u, w)$, лежащее в ℓ_u . Покажем, что тогда список ℓ_v заполнился позже, чем список ℓ_u . Действительно, после заполнения списка ℓ_w вершина f графа S должна быть изолированной; значит, все рёбра, входящие в неё в исходном графе S , были уже обработаны раньше, а тогда и в списке ℓ_u вершина f появилась в последний раз раньше.

Отсюда следует, что в подграфе M не будет ориентированных циклов. Так как в нем из каждой вершины, кроме $t(r)$, исходит ровно одно ребро, M является ориентированным остовным деревом. Таким образом, B является древесным массивом, и мы полагаем $B = \Pi(S)$.

Осталось показать, что алгоритмы, строящие Σ и Π , дают взаимно обратные отображения. Пусть, например, $T = \Sigma(A)$, и первые k шагов алгоритма, строящего $\Sigma(A)$, удаляют из A ребра f_1, \dots, f_k и вставляют в T ребра $e_1 \rightarrow f_1, \dots, e_k \rightarrow f_k$ в таком порядке. Покажем индукцией по k , что первые k шагов алгоритма, строящего $B = \Pi(T)$, вставляют в массив B ребра f_1, \dots, f_k и выкидывают из T ребра $e_1 \rightarrow f_1, \dots, e_k \rightarrow f_k$ в таком же порядке.

База при $k = 0$ очевидна. Для перехода рассмотрим $(k+1)$ -й шаг работы Π . По предположению индукции, ребро $e_{k+1} \rightarrow f_{k+1}$ есть в подграфе $T(k)$. Далее, в $T(k)$ не может быть ребра вида $e \rightarrow e_{k+1}$, поскольку в противном случае оно было бы добавлено в T в процессе работы алгоритма Σ на шаге с номером $\ell > k + 1$; но перед этим шагом в массиве $A(\ell - 1)$ уже не было ребра e_{k+1} — противоречие. Итак, e_{k+1} имеет в $T(k)$ нужные степени.

С другой стороны, если в $T(k)$ есть ребро $e \rightarrow e'$, и входящая степень e равна нулю, то номер e больше номера e_{k+1} ; в противном случае мы должны были бы добавить в T ребро $e \rightarrow e'$ вместо $e_{k+1} \rightarrow f_{k+1}$ на $(k+1)$ -м шаге работы Σ . Таким образом, на $(k+1)$ -м шаге работы Π мы действительно должны выкинуть из T ребро $e_{k+1} \rightarrow f_{k+1}$ и добавить в массив B ребро f_{k+1} .

Из доказанного утверждения следует, что $\Pi(\Sigma(A)) = A$ для всех $A \in \mathcal{A}$. Аналогично показывается, что $\Sigma(\Pi(T)) = T$ для любого $T \in \mathcal{T}$.

Примечание. Первоначальное доказательство Левина носило алгебраический характер и использовало технику работы с определителями.

G Последовательности де Брёйна через рекурренты

G.1 Доказательство утверждения этой задачи будет использовать алгебраическую технику, которая, возможно, неизвестна читателю. Если это так, то вы сможете впоследствии вернуться к нему, изучив соответствующие главы алгебры. Мы будем использовать некоторые классические алгебраические факты без доказательства.

Известно, что для любого n можно найти многочлен f степени n , неприводимый над полем F_2 из двух элементов; при этом остатки по модулю многочлена f образуют поле K из 2^n элементов. Для любого ненулевого элемента $u \in K$ выполнено равенство $u^{2^n-1} = 1$; более того, известно, что найдется такой ненулевой $\xi \in K$, что $\xi^t \neq 1$ для любого $0 < t < 2^n - 1$; тогда все ненулевые элементы поля K являются степенями элемента ξ .

Рассмотрим такой неприводимый многочлен g над F_2 , что $g(\xi) = 0$. Тогда g делит многочлен $x^{2^n} - x$, все корни которого различны (это просто все элементы поля K). Значит, все корни g также различны и лежат в K . Его степень равна n , поскольку в $F_2(u)$ ровно 2^n элементов. Пусть $g = x^{k_1-1} + \dots + x^{k_s-1} + x^n$, где $k_1 < k_2 < \dots < k_s$. Определим шаблон, поставив символ X ровно в места с номерами k_1, k_2, \dots, k_s .

Пусть $\xi = \xi_1, \xi_2, \dots, \xi_n$ — корни g . Система линейных уравнений

$$\begin{cases} x_1 + x_2 + \dots + x_n = 0 \\ \xi_1 x_1 + \xi_2 x_2 + \dots + \xi_n x_n = 0 \\ \vdots \\ \xi_1^{n-2} x_1 + \xi_2^{n-2} x_2 + \dots + \xi_n^{n-2} x_n = 0 \\ \xi_1^{n-1} x_1 + \xi_2^{n-1} x_2 + \dots + \xi_n^{n-1} x_n = 1 \end{cases}$$

имеет единственное решение, поскольку определитель соответствующей матрицы не равен нулю как определитель Вандермонда. Нетрудно понять, что последовательность, заданная при помощи нашего шаблона, может быть определена про помощи формулы

$$a_k = x_1 \xi_1^k + \dots + x_n \xi_n^k.$$

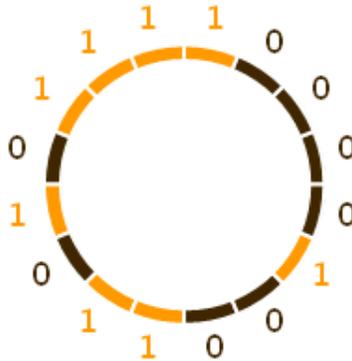
При $n > 1$ мы имеем $k_1 = 1$, поскольку g неприводим. Несложно видеть, что последовательность (a_k) будет периодична без предпериода, поскольку по любому ее куску длины n можно однозначно определить и следующий, и предыдущий куски. Если длина периода равна t , то из равенств $a_t = a_0$, $a_{t+1} = a_1, \dots, a_{t+n-1} = a_{n-1}$ и единственности решения линейной системы получаем, что $x_1 \xi_1^t = x_1, \dots, x_n \xi_n^t = x_n$. Поскольку хотя бы одно из x_i отлично от нуля, то $\xi_i^t = 1$. Значит, $t \geq 2^n - 1$, так как $F_2(\xi_i)$ изоморфно $F_2(u)$. С другой стороны, $t \leq 2^n - 1$, так как подпоследовательность из n нулей в нашей последовательности не встретится, а первое же повторение куска длины n приведет к периодичности.

de Bruijn Sequences and Universal cycles Konstantin Matveev and Ivan Mitrofanov

Why,' said the Dodo, 'the best way to explain it is to do it.' (And, as you might like to try the thing yourself, some winter day, I will tell you how the Dodo managed it.) First it marked out a race-course, in a sort of circle, ('the exact shape doesn't matter,' it said,) and then all the party were placed along the course, here and there.

Lewis Carroll. Alice's Adventures in Wonderland

The sequence 0000100110101111 has an interesting feature: if considered as a cyclic sequence, it contains precisely once each binary word of length 4.



Such sequence is called a de Bruijn sequence or a *universal cycle* for a set of binary words of length 4. Sometimes (see section D) the number of universal cycles can be computed exactly, but in some other cases it is not even known whether universal cycles exist at all.

In some problems of this project, including of course the open questions, any partial results will be accepted. Moreover, after getting acquainted with the section C, you might want to try to pose and solve your own problems about universal cycles, thus enriching this relatively recent theory with new interesting ideas.

A For starters

- A.1** Can one put $\binom{100}{5}$ integers on a circle, so that every five distinct integers from $\{1, 2, \dots, 100\}$ occur somewhere on a circle at five consecutive positions?
- A.2** Does there exist an infinite sequence of positive integers, such that every five distinct positive integers occur precisely once at five consecutive positions somewhere in this sequence?
- A.3** a) Is it possible to color the cells of the square grid with two colors, so that the coloring would be invariant with respect to horizontal and vertical shifts by 4 and it would contain a 2×2 square colored in each of the 16 possible ways?
- b) Is it possible to color the cells of the square grid with two colors, so that the coloring would be invariant with respect to horizontal and vertical shifts by 4 and it would contain a *diagonal square* colored in each of the 16 possible ways (a diagonal square is a set of four cells adjacent to a given cell)?

B de Bruijn sequences and directed graphs.

Definition B.1 (de Bruijn sequence) A de Bruijn sequence of rank n in the alphabet of k letters is a cyclic sequence of letters of length k^n , such that every sequence of letters of length n occurs precisely once as its subsequence.

Definition B.2 (Directed graph) A directed graph G consists of a vertex set $V = \{v_1, \dots, v_p\}$ together with a set of edges $v_i \rightarrow v_j$. It might have multiple edges between v_i and v_j in both directions and loops $v_i \rightarrow v_i$. G is said to be **connected** if one can get from any vertex to any other vertex by going along the edges (respecting the directions). It is said to be **balanced** if for each vertex the indegree (the number of incoming edges) is equal to the outdegree (the number of emanating edges). An **Eulerian tour** is a closed walk along edges of the graph which uses each edge exactly once.

B.4 Prove that a directed graph without isolated vertices has an Eulerian tour if and only if it is connected and balanced.

B.5 Prove that a de Bruijn sequence of rank n in the alphabet of k letters exists for each k and n .

B.6 Let G be a directed graph in which every vertex has indegree and outdegree equal to k . Prove that its edges can be colored with k colors, so that each vertex has precisely one incoming edge of each color and precisely one outgoing edge of each color.

B.7 a) Prove that some de Bruijn sequence of 0's and 1's of rank n can be constructed via the following algorithm. Start with $n - 1$ consecutive 0's and start adding symbols via the following rule. At each step add 1 if it doesn't cause repeating subsequences of length n , otherwise add 0. Do $2^n - n + 1$ steps and consider the result as a cyclic sequence.

b) How to modify this algorithm to obtain a de Bruijn sequence of rank n in the alphabet of k letters?

C Magic tricks and universal cycles.

If you have solved a slightly different problem than given to you, tell us, it might be interesting. We will also give points for solutions that work "not for all n ".

C.1 A magician is performing the following trick. He brings a deck of $n!$ cards marked with integers from 1 to $n!$ in some order and asks for n volunteers. He asks one of them to give deck a cut (i.e. shift the order of cards cyclically). Then volunteers take each one card from the top of the deck (in some prescribed order) and then form a line according to the relative order of their cards. Volunteer with the biggest card comes first, volunteer with the second biggest card stands next to him and so on. By looking at their order the magician is able to tell who has which card. Explain how the trick might be performed.

C.2 a) The magician is performing the same trick, but now he is trying to use as few numbers as possible. He brings a deck with $n!$ cards, each with an integer from 1 to C , $C < n!$. Volunteers do the same thing, but now if two of them get cards with the same value, the trick fails. Try to prove that the trick can be performed for as small C as possible.

b) In 2006 J. Robert Johnson proved that one can take $C = n + 1$. That was an open conjecture for more than 10 years. Try to get the same result.

C.3 The magician has a deck of 52 cards marked with integers (not necessarily distinct). Five volunteers give a cut to the deck and take each one card from the top. Then the magician asks them to split into groups according to the values of the cards (people with the same value go to the same group). After taking a look at this splitting the magician is able to tell the precise positions of cards in the rest of the deck. Explain how this trick might be performed.

- C.4** For which n can one put $\binom{n}{2}$ integers on a circle, so that every two distinct integers from $\{1, 2, \dots, n\}$ occur somewhere on a circle at two consecutive positions?
- C.5** Show that for $n \geq 8$ and not divisible by 3 it is possible to put $\binom{n}{3}$ integers on a circle, so that every three distinct integers from $\{1, 2, \dots, n\}$ occur somewhere on a circle at three consecutive positions.
- C.6 (open question)** For which k and n can one put $\binom{n}{k}$ integers on a circle, so that every k distinct integers from $\{1, 2, \dots, n\}$ occur somewhere on a circle at k consecutive positions?

D The beginning of enumeration

In this section we are mainly concerned with computing $B(2, n)$ - the number of de Bruijn sequences of rank n in the alphabet of 2 letters. Sequences obtained from each other by a cyclic shift are considered to be the same. Let's denote by $\epsilon(G)$ the number of Eulerian tours in a directed graph G .

Definition D.1 (Directed line graph) Let $G = (V, E)$ be a directed graph. The directed line graph $\mathcal{L}G$ is a directed graph with vertex set E (edges of G), and with an edge $e \rightarrow f$ for every pair of edges e and f of G with $s(f) = t(e)$ (the source of f equal to the target of e).

- D.1** Suppose G has more than one edge and no isolated vertices. Prove that $\mathcal{L}G$ is connected if and only if G is connected.
- D.2** Suppose that in G every vertex v has $\text{indeg}(v) = \text{outdeg}(v) = 2$. Suppose x is a vertex which is a target of edges P and Q and a source of edges R and S , none of which is a loop. Let G_1 be a graph obtained from G by erasing x and identifying P with R and Q with S ; G_2 be a graph obtained from G by erasing x and identifying P with S and Q with R . Prove that

$$\epsilon(\mathcal{L}G) = 2(\epsilon(\mathcal{L}G_1) + \epsilon(\mathcal{L}G_2)).$$

- D.3** Compute $B(2, n)$.

**de Bruijn Sequences and Universal Cycles.
After the Semifinal.**

Ilya Bogdanov, Konstantin Matveev, Ivan Mitrofanov.

E de Bruijn tori

Definition E.1 (de Bruijn torus) *A de Bruijn torus of type $(R, S, u, v)_k$ ($RS = k^{uv}$) is a filling of the cells of the square grid with $1, 2, \dots, k$, which is invariant with respect to the vertical shift by R and the horizontal shift by S , and contains a $u \times v$ (u rows and v columns) rectangle filled in each of the k^{uv} possible ways.*

Conjecture E.2 *Given R, S, u, v, k such that $RS = k^{uv}$, $R > u$, $S > v$, there always exists a de Bruijn torus of type $(R, S, u, v)_k$.*

It is proved only in certain special cases, in particular for $u = v = 2$. Apart from those listed in the problems below, we will also accept all other infinite series of constructions of de Bruijn tori that you will come up with.

E.1 Show that for all $k, u \geq 2$, $(k, u) \neq (2, 2)$ there exists a torus of type $(k^{u-1}, k, u, 1)_k$.

E.2 Show that for all odd $k > 1$ there exists a torus of type $(k^2, k^2, 2, 2)_k$.

E.3 Show that for all $k, u, v \geq 2$, except for the case when $v = 2$ and k is even, there exists a torus of type $(k^u, k^{u(v-1)}, u, v)_k$.

E.4 Show that also for all even $k \geq 2$ there exists a torus of type $(k^2, k^2, 2, 2)_k$.

E.5 Show that for all $k > 1$ there exists a torus of type $(k^4, k^2, 2, 3)_k$.

E.6 Suppose there exists a torus of type $(k^r, k^s, u, v)_k$ ($uv = r + s$), such that the sum of elements in each column (i.e. a vertical period of length R) is divisible by k . Show that there exists a torus of type $(k^r, k^{s+v}, u + 1, v)_k$.

E.7 Show that for all $k > 1$ there exists a torus of type $(k^8, k^8, 4, 4)_k$.

E.8 Show that for odd $k > 1$, if n is even or k is a perfect square, there exists a torus of type $(k^{n^2/2}, k^{n^2/2}, n, n)_k$.

E.9 Show the same for even $k > 1$.

E.10 Show that for all s, t there exists a torus of type $(4st^2, 4s^3t^2, 2, 2)_{2st}$.

F The continuation of Enumeration

Denote by $B(k, n)$ the number of de Bruijn sequences of rank n in the alphabet of k letters. As before, sequences obtained from each other by a cyclic shift are considered to be the same.

Definition F.1 (Oriented spanning tree) An oriented spanning tree of G is an acyclic (as undirected graph) subgraph of G with a distinguished node, the root v , in which there is a unique path from every vertex $u \in V$ to v . Denote by $\tau(G, v)$ the number of oriented spanning trees with root v .

F.1 Let G be a strongly connected balanced directed graph. Prove that for every $v \in V$

$$\epsilon(G) = \tau(G, v) \prod_{u \in V} (\text{outdeg}(u) - 1)!$$

Theorem F.2 Levine's theorem Let G be a directed graph in which every vertex has at least one incoming edge. Let x_e be the variable corresponding to an edge e of G . Define polynomials in several variables

$$\kappa^{\text{edge}}(G) = \sum_{\substack{\mathcal{T} - \text{oriented} \\ \text{spanning tree in } G}} \prod_{e - \text{edge of } \mathcal{T}} x_e$$

and

$$\kappa^{\text{vertex}}(\mathcal{L}G) = \sum_{\substack{\mathcal{T} - \text{oriented} \\ \text{spanning tree in } \mathcal{L}G}} \prod_{\omega - \text{edge of } \mathcal{T}} x_{t(\omega)}.$$

Then

$$\kappa^{\text{vertex}}(\mathcal{L}G) = \kappa^{\text{edge}}(G) \prod_{v \in V} \left(\sum_{e: s(e)=v} x_e \right)^{\text{indeg}(v)-1}.$$

F.2 Compute $B(k, n)$ (you can assume the Levine's theorem).

F.3 Prove the Levine's theorem.

G de Bruijn sequences via recurrences

Consider the following way of constructing a periodic sequence of 0's and 1's. Start with 00001 and a template of length 5, e.g. $XooXX$. At each step attach the template to the last 5 digits of the sequence that we have at the moment and define the next digit to be the sum modulo 2 of digits attached to X . In our case we get a sequence

0000110110...

In general, start with $0^{n-1}1$ and a template of length n (a template must start with X). Call a template *useful* if the resulting sequence contains all possible subsequences of length n but 0^n .

G.1 Show that for every n there exists a useful template of length n .

G.2 Is it possible to apply the same methods to obtain almost de Bruijn tori? (open question as you might guess)

de Bruijn Sequences and Universal cycles

SOLUTIONS

A For starters

A.1 Answer. No.

Assume that such an arrangement exists. Assume that some number, e.g. number 1, appears k times along the circle. Then it is contained in $5k$ contiguous 5-tuples. On the other hand, this number should appear exactly once in any 5-tuple containing it. The total number of such 5-tuples is $\binom{99}{4}$, so we have $k = \binom{99}{4}/5$, which is not an integer. A contradiction.

A.2 Answer. Such a sequence exists.

To prepare, let us enumerate all 5-tuples of positive integers: the first one is $(1, 2, 3, 4, 5)$, then follow all the tuples with the sum 16, and so on.

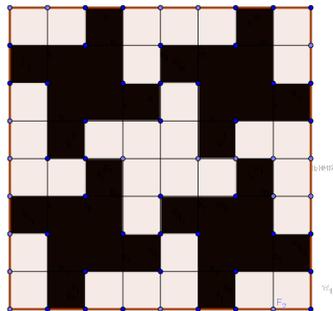
We will construct our sequence iteratively. Assume that at some moment we have obtained a finite sequence such that it contains all 5-tuples from 1st to k th (together with some extra 5-tuples), and no 5-tuple occur twice. We will augment this sequence by some terms so that it will satisfy the same condition with k replaced by $k + 1$.

If the $(k + 1)$ st tuple already occurs somewhere, then we do nothing. Otherwise, if $(a_1, a_2, a_3, a_4, a_5)$ is the $(k + 1)$ st tuple, we will augment the sequence by ten numbers $b_1, b_2, b_3, b_4, b_5, a_1, a_2, a_3, a_4, a_5$, where b_1, \dots, b_5 are distinct numbers which are greater than all used numbers (including the numbers a_1, \dots, a_5). It is easy to see that we have obtained a desired prolongation.

Acting so, after an infinite time we will get an (infinite) sequence containing each 5-tuple exactly once. Indeed, by the construction every 5-tuple occurs in this sequence; if some tuple occurs twice, then this happens on some finite initial segment of our sequence, which is impossible.

A.3 a) Answer. Yes.

A picture below shows an 8×8 piece of plane colored in a required manner. One may look out of the window and try to find a similar pattern.

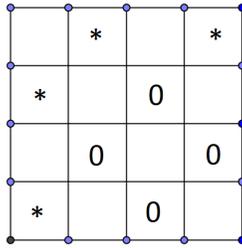


6) Answer. No.

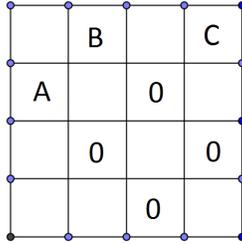
We will establish the answer by an easy case distinction.

Arguing indirectly, we have that all “diagonal squares” within one period are colored distinctly. We depict the further arguments on a 4×4 square which is a “period” of our coloring; the two colors are replaced by zeroes and ones, respectively. To start, let us find a square with four zeroes in it.

We claim that all cells marked by stars should contain ones. Due to the symmetry, it suffices to deal with one of these cells. Assume that A contains 0; then both B and C contain ones, otherwise there would appear two

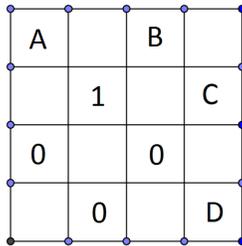


squared with four zeroes in each. But then we will have two squares having the pattern “one at the top, zeroes in all other positions”, which is prohibited.



So all the starred cells contain ones. Thus we already have all eight arrangements with an even number of ones. Notice also that each “diagonal square” contains either four filled cells or four cells which are still empty. Those eight empty cells thus should contain all arrangements with an odd number of ones.

Without loss of generality, four of these cells contain the digits as shown in the picture below.



Assume that cell A contains 0. Then the parity reasons yield that the cells B and C contain zeroes, while D contains 1; one can easily see that this arrangement does not fit.

Otherwise A contains one; then B and C contain ones as well, while D contains 0. This arrangement also does not fit.

B de Bruijn sequences and directed graphs

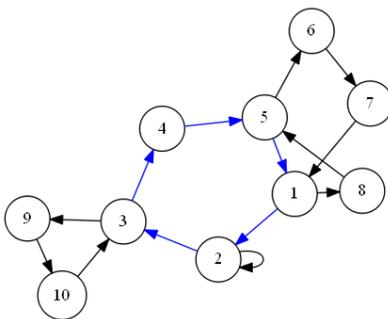
B.4 Assume that an Eulerian tour exists. If we move along this tour, we come into each vertex as many times as we leave it, so the graph must be balanced. Next, while moving along the cycle one can get from any vertex to any other vertex, so the graph is strongly connected.

Conversely, assume that a directed graph is strongly connected and balanced. We will prove that an Eulerian tour exists by induction on the number of edges in this graph. The base case when a graph has no edges is trivial.

For the step, let us start from any vertex and move along the edges until we come to an already visited vertex. Thus we have found some cycle C in our graph.

Now let us delete the edges of this cycle from our graph. The remaining graph is still balanced, but it might become disconnected.

Lemma. *If a balanced graph is weakly connected (i.e. if it is connected when we regard it as a usual non-directed graph), then it is connected.*



Proof. Take an arbitrary vertex v . Let A be a set of vertices reachable from v , and let B be the set of all other vertices. Assume that B is nonempty. Then there are no edges from A to B , but there should be some edges from B to A due to the weak connectedness. Now comparing the total in- and out-degree of the vertices of A we come to a contradiction: these sums should be equal due to balancedness, but the first one is greater due to the edges from B to A . A contradiction. \square

Thus, after C has been deleted, the graph splits into several components each of which is balanced and connected, so each has an Eulerian tour. Then a desired tour can be constructed as follows: we move along the edges of C until we come to some vertex of some component; then we walk along the Eulerian tour of this component, and then we move further along C , and so on.

B.5 Let us construct a special graph which is called a *de Bruijn graph* $G(n, k)$. Its vertices are all k^{n-1} $(n - 1)$ -letter words in a k -letter alphabet, and a vertex of the form $a_1 \dots a_{n-1}$ is connected to every vertex of the form $a_2 \dots a_n$. Thus the edges correspond to n -letter words of the form $a_1 \dots a_n$, and there are k^n edges.

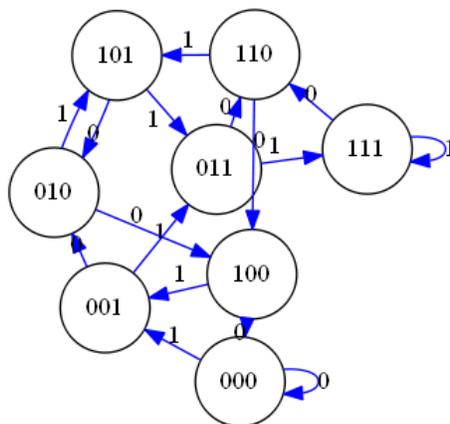


Рис. 1: $G(4, 2)$.

More generally, each word of length $n + a$ corresponds to an (oriented) path of length $a + 1$ in $G(n, k)$. The vertices of this path are just all $(n - 1)$ -letter subwords of our word in the order of their appearance.

Let us write on each edge $a_1 \dots a_{n-1} \rightarrow a_2 \dots a_n$ the last letter a_n of the corresponding word. Thus, if the last edge of a path corresponds to the word $a_1 \dots a_k$, then the letters written on the previous $k - 1$ edges form the word $a_1 \dots a_{k-1}$.

Every in- and out-degree of a vertex in G is equal to k . Moreover, the graph is connected, since for every two vertices there exists a path connecting them (this path corresponds to a concatenation of these words).

Thus graph $G(n, k)$ has an Eulerian tour. The sequence of letters written on the edges of this cycle form a de Bruijn sequence, since all the subwords correspond to the different edges of our graph.

B.6 We will use induction on k . Base for $k = 0$ is clear.

If we can mark some edges, so that there is precisely one marked edge going from each vertex and precisely one edge coming to each vertex, then we will be able to color marked edges with color 1 and use the inductive assumption for $k - 1$.

We will apply *Hall's lemma*: If there are several gentlemen and ladies, so that every m gentlemen are acquainted with at least m ladies in total (for each m), then each gentleman can propose to a lady he knows, so that there will be no conflicts.

Put a gentleman and a lady in each vertex and say that a particular gentleman is acquainted with a particular lady if there is an edge from him to her. Assume that conditions of the Hall's lemma are not satisfied: there is a group of m_1 gentlemen who are acquainted in total with $m_2 < m_1$ ladies. From vertices in which these gentlemen are located a total km_1 edges are emanating, and these edges are all going to a set m_2 vertices. So at least one of them has indegree at least $\frac{km_1}{m_2} > k$, contradiction.

Now we can just select pairs «gentleman-lady» with the help of the Hall's lemma and mark the corresponding edges.

B.7 b) Suppose we are working over the alphabet $\{0, 1, \dots, k-1\}$. Algorithm will be the following: start with $k-1$ zeroes, on each step put the maximal possible letter, such that no word of length k is repeated. If it is possible to make $k^n - n + 1$ such steps, then the resulting cyclic sequence will be of de Bruijn type.

In other words, given the de Bruijn graph $G(n, k)$, start with the vertex $000\dots 0$ and walk along the edges, each time choosing an edge we haven't used yet with the maximal possible label.

Suppose we are stuck at some vertex. Then it must be $00\dots 0$.

We have already gone through the edge $00\dots 0$, for otherwise we could have proceeded along it.

Consider all unused edges and color those with label 0 in black and those with nonzero label in gray.

Lemma: There is no oriented cycle of black edges.

Assume there exists one. Then if we go along it, at some point we must go through the edge $0\dots 00$, but it is not colored. Contradiction.

Suppose there exists at least one black or gray edge v_1v_2 . We came to v_2 less than k times, so we left it less than k times and didn't use the edge with label 0. So there is some black edge v_2v_3 , then some black edge v_3v_4 and so on. As a result we get an oriented cycle of black edges which contradicts the lemma.

Part a) is a particular case for $k = 2$.

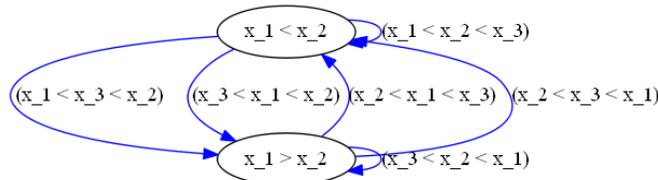
C Magic tricks and universal cycles

C.1 Let a_1, a_2, \dots, a_k and b_1, b_2, \dots, b_k be two sequences such that the numbers in each sequence are pairwise distinct. We will say that these sequences are *equiordered* if for every pair of indices $i \neq j$ we have either $a_i < a_j$ and $b_i < b_j$, or $a_j > a_i$ and $b_j > b_i$.

Let S_n be the set of orderings of the set $\{1, 2, \dots, n\}$. Then S_n contains $n!$ elements, each of which is a *permutation of length n* . The magician will be able to perform the trick if he finds a cyclic sequence of length $n!$ such that no two of $n!$ its pieces of length n are equiordered.

For this purpose, we construct a directed graph \mathbb{S}_n whose vertices are the permutations of length $n-1$. The edges are constructed as follows. For every permutation $s \in S_n$ we define its *head* as the permutation of length $n-1$ equiordered with the first $n-1$ elements of s . A *tail* of s is defined similarly (e.g., the head and the tail of 31542 are 2143 and 1432, respectively). Now for every $s \in S_n$ we draw an edge from its head to its tail.

It is convenient for us to write the elements of S_n as the system of inequalities in variables x_1, \dots, x_n ; see example in the picture below.



Graph \mathbb{S}_3

First, let us show that \mathbb{S}_n admits an Eulerian tour. Indeed, the out-degree of every vertex is n (this is the number of ways to put a new element onto a line relatively to $n-1$ existing ones), as well as the in-degree of

every vertex. To check the connectedness, take any two permutations s_1 and s_2 of length $n - 1$ and consider some sequence t of $2n - 2$ distinct numbers such that the first $n - 1$ of them are equiordered with s_1 , while the last ones are equiordered with s_2 . Then there exists a path from s_1 to s_2 whose edges are determined by the n -element pieces of t .

Let us now choose any Eulerian tour in \mathbb{S}_n ; let its edges correspond to the permutations $s_1, s_2, \dots, s_{n!}$ (in order of appearance in the tour). Take $n!$ variables $y_1, \dots, y_{n!}$ (we assume that $y_{n!+k} = y_k$). Each permutation s_i defines the system of inequalities in variables x_1, \dots, x_n ; let us write down this system replacing each x_k by y_{i+k-1} . For instance, if s_3 determines the system $x_2 > x_1 > x_3$, then we write down the inequalities $y_4 > y_3 > y_5$. Our aim is to plug the numbers in all y_i 's so that all the written inequalities hold.

For every permutation s_i , let us draw $\frac{n(n-1)}{2}$ oriented edges between y_i, \dots, y_{i+n-1} , namely we draw an arrow $y_{i_1} \rightarrow y_{i_2}$ if $y_{i_1} > y_{i_2}$ in s_i . We obtain a new directed graph H on the vertices $y_1, \dots, y_{n!}$.

Lemma. *Graph H contains no oriented cycles.*

Proof. We say that an edge $y_i \rightarrow y_j$ of H *faces right* if $j - i \in \{1, 2, \dots, n - 1\}$; similarly, it *faces left* if $i - j$ belongs to the same set. If $n > 2$ then every edge of H faces exactly one of two directions; moreover, if H contains an edge $y_i \rightarrow y_j$ then it does not contain $y_j \rightarrow y_i$.

Assume the contrary. Consider an oriented cycle C in H with the smallest number of vertices. Suppose that C contains two consecutive edges facing different directions — say, $y_i \rightarrow y_j$ facing left and $y_j \rightarrow y_k$ facing right. Both these edges are drawn according to the permutation s_j , so the edge $y_i \rightarrow y_k$ also exists by the same reason. Therefore, the cycle is contractible, which contradicts our choice.

Thus, all the edges of C face the same direction — say, all of them face left. Now, there exists an index t such that permutation s_t defines the inequalities $x_1 < x_2 < \dots < x_n$, which provide the edges $y_{t+n-1} \rightarrow y_{t+n-2} \rightarrow \dots \rightarrow y_t$ in H . But cycle C should contain an edge connecting two of the vertices y_t, \dots, y_{t+n-1} ; this edge then faces right. This contradiction finishes the proof. \square

Now, as H contains no oriented cycles, we may introduce a partial order on the variables y_i by setting $y_{i_1} \succ y_{i_2}$ if H contains a path from y_{i_1} to y_{i_2} .

Now we may take any variable which is minimal with respect to this order and assign 1 to it. Remove it from the set of variables, take any minimal variable in the remaining set and assign 2 to it, and so on. Clearly, the assigned values satisfy all the required inequalities.

C.2 The solution can be found in the article J. R. Johnson, Universal cycles for permutations, *Discrete Math.*, 309(2009), pp. 5264–5270.

C.3 The solution is similar to that of **C.1**.

We say that two sequences (a_1, a_2, \dots, a_n) and (b_1, b_2, \dots, b_n) are *equipartitioned* if for every two indices $i \neq j$ we have either $a_i = a_j$ and $b_i = b_j$, or $a_i \neq a_j$ and $b_i \neq b_j$. Denote by P_n the set of all possible partitionings of an n -term sequence.

One may check that $|P_5| = 52$, so the magician will be able to perform the trick if he finds a cyclic sequence of length 52 in which no two 5-tuples of consecutive numbers are equipartitioned. Here is one such sequence:

DDDDDCHHCCDDCCCHCHCSHHSDDSSSHSDDCHSSCHSHDHSCHSJCDC

Here the letters S, C, D, and H denote the usual card suits, and a letter J denotes a joker. Thus one may take a usual deck with 52 cards, replace a queen of spades with a joker, and arrange the obtained deck in order to be able to perform this trick.

Now we will show how to minimize a case consideration in finding such a sequence (although the result may involve more than five distinct numbers). We work with P_5 , but a similar method may be applied to any P_n with $n > 4$.

Firstly, we construct a directed graph \mathbb{P}_5 . Its vertices are the elements of P_4 , and the edges correspond to the elements of P_5 in a usual manner. Namely, for every $p \in P_5$ we define its *head* and *tail* as two partitions in P_4 equipartitioned with the first and with the last $n - 1$ elements of p , respectively. Now for every $p \in P_5$ we draw an edge from its head to its tail. For example, the partition 12324 determines the edge $1232 \rightarrow 1213$.

Graph \mathbb{P}_n is connected. Indeed, if we need to find a path from p_1 to p_2 , we may consider a $(2n - 2)$ -term sequence such that its first half is equipartitioned with p_1 , and its second half is equipartitioned with p_2 . The n -term pieces of this sequence determine the edges of a required path.

Next, this graph is also balanced. If an element of P_4 contains k distinct numbers, then every its incoming and outgoing edge corresponds to the addition of a new element which may be either equal to an existing one or distinct from all of them. Thus both in- and out-degree of this vertex are equal to $k + 1$.

Thus graph \mathbb{P}_5 admits an Eulerian tour. Every such tour defines the system of equalities and inequalities on the cyclic set of variables y_1, \dots, y_{52} in a way similar to that described in **C.1**.

Now for every equality $y_i = y_j$ we connect the variables y_i and y_j by a white edge, while for every inequality $y_i \neq y_j$ we connect y_i with y_j by a black edge. We say that this system is *contradictory* if there exists a white path whose endpoints are connected with a black edge (this means that these endpoints are equal and not equal simultaneously). If the system is not contradictory then one may obtain a required arrangement by assigning equal values to those variables which are connected with a white path.

Thus it remains to show the existence of an Eulerian tour determining a non-contradictory system.

First of all, we may notice (by an analogy with **C.1**) that in a contradictory system always exists a contradiction of the form

$$y_{i_1} = y_{i_2} = \dots = y_{i_k} \neq y_{i_1},$$

where all edges $y_{i_j} \rightarrow y_{j+1}$ face right.

Consider a sequence $W = 113112222213311$. It corresponds to a path with 11 edges in \mathbb{P}_5 .

Lemma 1. *If an Eulerian tour contains this path then it determines a non-contradictory system.*

Proof. Consider 15 variables involved in our path (without loss of generality, they are y_1, \dots, y_{15}). It is easy to see that every path facing right and connecting one of y_1, \dots, y_5 to one of y_{11}, \dots, y_{15} contains at least two black edges. Thus there is no contradiction of the abovementioned form. \square

Lemma 2. *There is an Eulerian tour in \mathbb{P}_5 containing the path determined by W .*

Proof. Delete the edges of our path from \mathbb{P}_5 and add one edge from the beginning of this path to its end. It suffices to prove that the obtained graph is balanced and connected. The former property is obvious; for the latter, it suffices to show the weak connectedness.

In other words, we need to prove that every 4-term sequence may be extended to the right in a way that the last 5 digits are distinct, and no its 5-letter subword is equipartitioned with some subword in W .

Consider a sequence (a, b, c, d) (some symbols may be equal). Let us try to augment it by a new letter e distinct from the existing ones; this works if a word (a, b, c, d, e) is not equipartitioned with a subword of W . Then we try to repeat this procedure; if it works four times then we are done. Thus, it remains to check the cases when this algorithm fails at some stage, i.e. when the resulting word is equipartitioned with some subword W' of W . The last letter of W' should be distinct from all other its letters. Thus we have only three options for W' .

- (a) Assume that $W' = 12113$. Then, instead of extending the word 1211 by 3 we may extend it as 12112345.
- (b) The case $W' = 33331$ is impossible since all the edges from the vertex 0000 are already used in W (so this vertex is deleted from the new graph).
- (c) Assume that $W' = 33312$. Then, instead of extending the word 3331 by 2 we may extend it as 33313245.

The lemma is proved. \square

The two lemmas above provide the desired result.

- C.4** Consider a complete graph on n vertices labeled by $1, 2, \dots, n$. Then we need just to find an Eulerian tour in this (undirected) graph. For known reasons, such a tour exists when n is odd, and it does not exist when n is even.
- C.5** Consider a circle partitioned into n equal arcs, and enumerate the partitioning points consecutively from 1 to n . Then a triple of numbers determines the partition of this circle into three arcs. We say that two triples *have the same difference type* if the lengths of arcs in corresponding partitions are the same (possibly after a

cyclic shift). (To find the arcs lengths one may just order the numbers and calculate their cyclic differences modulo k .)

Example: Let $n = 8$. Then the triples $\{1, 3, 7\}$ and $\{1, 5, 3\}$ have the same difference type $(2, 2, 4)$, while the triples $\{1, 2, 5\}$ and $\{1, 4, 5\}$ have distinct difference types $(1, 3, 4)$ and $(3, 1, 4)$, respectively.

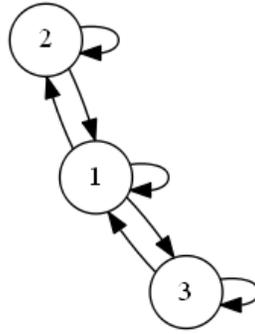
If n is not divisible by 3, then the number of difference types is $\binom{n}{3}/n = \frac{(n-1)(n-2)}{6}$.

To start, let us construct a desired arrangement for $n = 8$. There are 7 difference types:

$$(1, 1, 6), \quad (2, 2, 4), \quad (2, 3, 3), \quad (1, 2, 5), \quad (5, 2, 1), \quad (1, 3, 4), \quad (4, 3, 1).$$

We want to choose in each difference type (x, y, z) one of ordered pairs $x \rightarrow y$, $y \rightarrow z$, or $z \rightarrow x$. In the types above we make it as follows:

$$1 \rightarrow 1, \quad 2 \rightarrow 2, \quad 3 \rightarrow 3, \quad 1 \rightarrow 2, \quad 2 \rightarrow 1, \quad 1 \rightarrow 3, \quad 3 \rightarrow 1.$$



These arrows form a balanced connected directed graph. This graph admits an Eulerian cycle, and the sum of the numbers in its period is congruent to 5 modulo 8:

$$(1 \rightarrow 1 \rightarrow 2 \rightarrow 2 \rightarrow 1 \rightarrow 3 \rightarrow 3 \rightarrow 1)1 \rightarrow \dots$$

Extending this cycle periodically we get an infinite sequence (a_k) . Define the sequence (b_k) as $b_k = a_1 + \dots + a_k \pmod 8$; this sequence is periodic with period length $7 \cdot 8 = 56$.

Let us show that every triple appears in this sequence. Indeed, every triple may be represented as $(x, x+k_1, x+k_1+k_2) \pmod 8$ in a way that the numbers k_1, k_2 appear consecutively in (a_i) . Let $a_i = k_1, a_{i+1} = k_2$. Then we have $a_{i+8n} = k_1, a_{i+1+8n} = k_2$ for all n . Since $a_1 + \dots + a_8 \equiv 5 \pmod 8$, there exists n such that the number $b_{8n+i-1} \equiv a_1 + \dots + a_{i-1} + n(a_1 + \dots + a_8)$ is congruent to x modulo 8. Thus the terms $b_{8n+i-1}, b_{8n+i}, b_{8n+i+1}$ form a required triple.

Now we pass to a general construction.

Lemma. For every $n \geq 8$ not divisible by 3 one may choose an ordered pair in each difference type so that the $\frac{(n-1)(n-2)}{6}$ obtained oriented edges form a connected balanced directed graph. (Naturally, the vertices of this graph are exactly those numbers which have at least one outgoing edge.)

Proof. Consider two cases separately.

Case 1: n is even. If a difference type contains two equal numbers, we connect them with a loop. Thus we obtain loops $i \rightarrow i$ for all i from 1 to $n/2 - 1$. If all three numbers are distinct then we connect two smallest ones. The obtained graph on vertices $1, \dots, n/2 - 1$ is balanced, since the edges $i \rightarrow j$ and $j \rightarrow i$ appear simultaneously. It is connected since each of the numbers $2, \dots, n/2 - 1$ is connected with 1 in both directions.

Case 2: n is odd. The set of vertices is $\{1, 2, \dots, (n-1)/2\}$. If a type contains two equal numbers, then we connect them with a loop. Otherwise we connect two smallest numbers, except for two cases. The two exceptional triples are $(2, (n-1)/2 - 1, (n-1)/2)$ и $(2, (n-1)/2, (n-1)/2 - 1)$, in which we choose the edges $(n-1)/2 \rightarrow 2$ and $2 \rightarrow (n-1)/2$, respectively.

The obtained graph is again balanced. Its connectedness follows from the fact that every number except for $(n-1)/2$ is connected with 1, and $(n-1)/2$ is connected with 2. \square

Denote the constructed graph by L_n ; it has $\lfloor \frac{n-1}{2} \rfloor$ vertices, and it contains a loop $1 \rightarrow 1$. We need also a larger graph \mathbb{L}_n . It contains $n \lfloor \frac{n-1}{2} \rfloor$ vertices, each having the form (k, i) where $k \in \{1, 2, \dots, n\}$, and i is a vertex of L_n . For every edge $i \rightarrow j$ in L_n we introduce n edges in \mathbb{L}_n ; these edges have the form $(k, i) \rightarrow (k+i, j)$ for all admissible k .

The graph \mathbb{L}_n is balanced since L_n is such. Let us show that \mathbb{L}_n is connected. Due to balancedness, it suffices to show a weak connectedness, so we will just show that there exists a path from any vertex (k, i) to $(0, 1)$.

In L_n , the vertices i and 1 are connected with a path; this path induces a path in \mathbb{L}_n from (k, i) to some vertex of the form $(s, 1)$. But \mathbb{L}_n also contains all edges of the form $(t, 1) \rightarrow (t+1, 1)$, and one can move along such edges to reach $(0, 1)$ from $(s, 1)$.

Thus \mathbb{L}_n admits an Eulerian tour. Its length is $\binom{n}{3}$, and for every k and every edge $i \rightarrow j$ of L_n this cycle contains three consecutive vertices of the form $(k, i), (k+i, j), (k+i+j, *)$ (we do not care about the starred number). Thus, if we write down the sequence of the first coordinates of the vertices in this tour we get the sequence containing every triple of numbers from 1 to n .

D The beginning of enumeration

D.1 A graph $\mathcal{L}G$ is strongly connected precisely when for every two edges e_1, e_2 in G there exists a (directed) path starting from e_1 and arriving at e_2 .

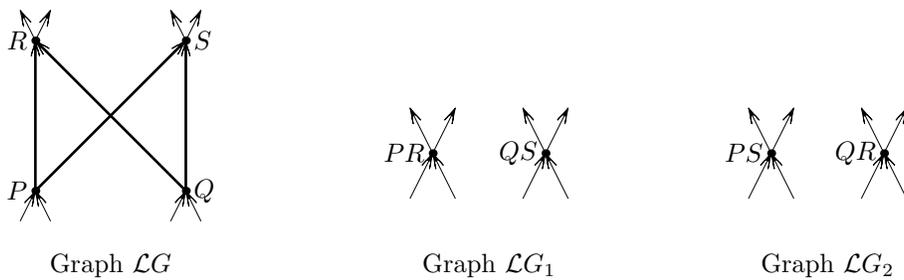
Assume that G is strongly connected, and e_1 and e_2 are two its edges. There exists a path T from the target of e_1 to the source of e_2 ; then $e_1 T e_2$ is a desired path in $\mathcal{L}G$.

Assume now that $\mathcal{L}G$ is strongly connected. If every vertex of G is a source of some edge as well as a target of some edge, then G is connected. Indeed, to find a path from v_1 to v_2 it suffices to find a path in $\mathcal{L}G$ from some edge with v_1 as a source to some edge with v_2 as a target.

So, assume that this condition fails, e.g., there is no edge from some vertex v . Since v is not isolated, there exists an edge e going to v , and there exists some other edge e' in our graph. But then it is impossible to reach e' from e in $\mathcal{L}G$. Contradiction.

D.2 The ingoing and outgoing degrees of each vertex in $\mathcal{L}G$ are also equal to 2. It has vertices P, Q, R, S , and there are edges from P and Q to R and S .

$\mathcal{L}G_1$ can be obtained from $\mathcal{L}G$ in the following fashion: edges PS, PR, QS и QR are deleted, P and R are glued into a vertex (PR) , Q and S are glued into a vertex (QS) . $\mathcal{L}G_2$ is similar: the same four edges are deleted, vertices P and S are glued into (PS) , vertices Q and R are glued into (QR) .



We will call edges PR, QS, PS and QP of $\mathcal{L}G$ the *special* ones, as well as vertices $(PR), (QS), (PS)$ and (QP) in $\mathcal{L}G_1$ and $\mathcal{L}G_2$.

By a *great 4-tuple* we mean an unordered set of four paths in $\mathcal{L}G$ such that their edge sets are disjoint and cover all edges of $\mathcal{L}G$ but the special ones. So each great 4-tuple contains two paths starting at R , two paths starting at S , two paths ending at Q , two paths ending at P .

A great 4-tuple corresponds to a 4-tuple of disjoint paths in $\mathcal{L}G_1$ ($\mathcal{L}G_2$), covering all edges, starting and ending at special vertices, but not going through them in the mean time. For simplicity we will say that a great 4-tuple is the same in $\mathcal{L}G, \mathcal{L}G_1$ and $\mathcal{L}G_2$.

Each Eulerian cycle in $\mathcal{L}G$ is split by the special edges into four pieces producing a great 4-tuple. In a similar fashion, each Eulerian cycle in $\mathcal{L}G_1$ or $\mathcal{L}G_2$ is split into a great 4-tuple by occurrences of the special vertices.

To solve the problem it suffices to show that each great 4-tuple corresponds to four Eulerian cycles in $\mathcal{L}G$, while to two Eulerian cycles in $\mathcal{L}G_1$ or $\mathcal{L}G_2$.

A great 4-tuple in $\mathcal{L}G$ can be of one of three types:

- (a) One path $R \rightarrow P$, one path $R \rightarrow Q$, one path $S \rightarrow P$, one path $S \rightarrow Q$.
- (b) Two paths $R \rightarrow P$ and two paths $S \rightarrow Q$.
- (c) Two paths $R \rightarrow Q$ and two paths $S \rightarrow P$.

Let us go through all cases.

- (a) Denote the paths of a great 4-tuple by $R \dots P$, $R \dots Q$, $S \dots P$ и $S \dots Q$. There are precisely 6 ways to put on them a cyclic order. Each can be written as

$$X_1 \dots Y_1 X_2 \dots Y_2 X_3 \dots Y_3 X_4 \dots Y_4,$$

where X_i are the starting points of the paths and Y_i the endpoints. We get four pairs of vertices $Y_i X_{i+1}$. If these pairs coincide with $\{PS, PR, QS, QR\}$, then we get an Eulerian cycle in $\mathcal{L}G$. If they coincide with $\{PR, PR, QS, QS\}$, then we get an Eulerian cycle in $\mathcal{L}G_1$, and if they coincide with $\{PS, PS, QR, QR\}$ we get an Eulerian cycle in $\mathcal{L}G_2$. We will write down these ways.

- (i) $R \dots PR \dots QS \dots PS \dots Q$ — set $\{PR, QS, QR, PS\}$, a cycle in $\mathcal{L}G$;
- (ii) $R \dots PR \dots QS \dots QS \dots P$ — set $\{PR, QS, QS, PR\}$, a cycle in $\mathcal{L}G_1$;
- (iii) $R \dots PS \dots PR \dots QS \dots Q$ — a cycle in $\mathcal{L}G$;
- (iv) $R \dots PS \dots PS \dots QR \dots Q$ — a cycle in $\mathcal{L}G_2$;
- (v) $R \dots PS \dots QR \dots QS \dots P$ — a cycle in $\mathcal{L}G$;
- (vi) $R \dots PS \dots QS \dots PR \dots Q$ — a cycle in $\mathcal{L}G$.

So we get four cycles in $\mathcal{L}G$, one cycle in $\mathcal{L}G_1$ and one cycle in $\mathcal{L}G_2$.

- (b) It will be similar, but two pairs of different paths $R \dots P$ and $S \dots Q$ will be denoted in the same way.
 - (i) $R \dots PR \dots PS \dots QS \dots Q$ — a cycle in $\mathcal{L}G$;
 - (ii) $R \dots PR \dots PS \dots QS \dots Q$ — a cycle in $\mathcal{L}G$. One mustn't forget that this is a different order, since two paths of the great 4-tuple are switched
 - (iii) $R \dots PS \dots QR \dots PS \dots Q$ — a cycle in $\mathcal{L}G_2$;
 - (iv) $R \dots PS \dots QS \dots QR \dots P$ — a cycle in $\mathcal{L}G$;
 - (v) $R \dots PS \dots QR \dots PS \dots Q$ — a cycle in $\mathcal{L}G_2$;
 - (vi) $R \dots PS \dots QS \dots QR \dots P$ — a cycle in $\mathcal{L}G$.

So we get four cycles in $\mathcal{L}G$ and two cycles in $\mathcal{L}G_2$.

- (c) Same argument as in the previous case.

D.3 Answer: $2^{2^{n-1}-n}$,

Clearly $B(2, n) = \epsilon(G(2, n))$. We will use induction to show that $\epsilon(G(2, n)) = \frac{2^{2^{n-1}}}{2^n}$.

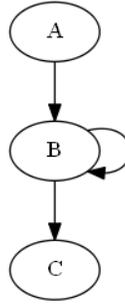
Observe that $\mathcal{L}G(2, n) = G(2, n+1)$. Indeed, vertices of $G(2, n+1)$ correspond to edges of $G(2, n)$, while edges of $G(2, n+1)$ correspond to binary words of length $n+1$, i.e. paths in $G(2, n)$ of length 2.

Lemma. *Suppose a digraph G has n vertices, each of indegree and outdegree 2. Then $\epsilon(\mathcal{L}G) = 2^{n-1}\epsilon(G)$.*

The inductive step immediately follows from the lemma: there are 2^{n-1} vertices in $G(2, n)$, so

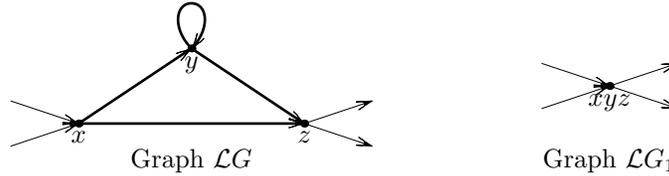
$$\epsilon(\mathcal{L}G(2, n)) = 2^{2^{n-1}-1} 2^{2^{n-1}-n} = \frac{2^{2^n}}{2^{n+1}}.$$

Proof of the Lemma. We will prove it by induction on the number of vertices. Base: $n = 1$. A graph is a vertex with two loops, it has one Eulerian cycle, precisely as its line graph.



Step $n \rightarrow n + 1$. If G has a vertex with two loops, it is not connected to anything else, so both G and $\mathcal{L}G$ have no Eulerian cycles.

Suppose G has a vertex B with a single loop. Then in a Eulerian cycle the loop $B \rightarrow B$ must come in between $A \rightarrow B$ and $B \rightarrow C$. Erase vertex B , put in edge AC and denote the resulting graph by G_1 . $\epsilon(G) = \epsilon(G_1)$. The local difference between $\mathcal{L}G$ and $\mathcal{L}G_1$ is shown on the picture below ($x = A \rightarrow B, y = B \rightarrow B, z = B \rightarrow C$).



Each Eulerian cycle in $\mathcal{L}G_1$ corresponds to two cycles in $\mathcal{L}G$: we go twice through the vertex xyz and there are two ways to do it in $\mathcal{L}G$: $x \rightarrow y \cup y \rightarrow z$ and $x \rightarrow z$. We can apply them in any order, so we get two cycles. Then

$$\epsilon(G) = \epsilon(G_1) = \frac{1}{2^{n-1}} \epsilon(\mathcal{L}G_1) = \frac{1}{2^n} \epsilon(\mathcal{L}G).$$

Suppose now that we are considering a vertex with no loops in it. Construct G_1 and G_2 as in **D2**. Each of them has $n - 1$ vertices and satisfies lemma conditions.. Each Eulerian cycle in G corresponds to a cycle in G_1 or in G_2 . As a result, $\epsilon(G) = \epsilon(G_1) + \epsilon(G_2)$,

$$\epsilon(\mathcal{L}G) = 2(\epsilon(\mathcal{L}G_1) + \epsilon(\mathcal{L}G_2)) = 2 \cdot 2^{n-1} (\epsilon(G_1) + \epsilon(G_2)) = 2^n \epsilon(G).$$

Lemma is proved.

E de Bruijn tori

General remark. Throughout this section, we regard letters of the alphabet $X_k = \{1, 2, \dots, k\}$ as residues modulo k . So it is possible to perform arithmetic operations with these letters and also obtain a letter. We will usually denote the j th cell in the i th row of a square grid by (i, j) .

E.1 For convenience, we will construct a torus of type $(k, k^{u-1}, 1, u)_k$; a required torus can be obtained via reflection across the diagonal.

Firstly, assume that $u \geq 3$. Let $c_1, c_2, c_3, \dots, c_{k^{u-1}}$ be a de Bruijn sequence of rank $u - 1$ in the alphabet $X_k = \{1, 2, \dots, k\}$; we extend it to obtain an infinite k^{u-1} -periodic sequence. Now let us fill the cell (i, ℓ) , $\ell > 0$ in a square grid with the number

$$a_{i,\ell} = i + \sum_{s=1}^{\ell} c_s$$

(recall that addition is performed modulo k). Similarly extend it to the filling of the whole square grid.

Each number appears in the period $c_1, c_2, \dots, c_{k^{u-1}}$ exactly k^{u-2} times; since $u \geq 3$, the sum $\sum_{s=1}^{k^{u-1}} c_s$ is divisible by k . So, the arrangement is indeed k^{u-1} -periodical horizontally and k -periodical vertically, thus it is a torus of required size. (One may notice that the periodicity property also holds if $u = 2$ and k is odd.)

It remains to prove that every u numbers x_0, \dots, x_{u-1} appear (in this order) consecutively in some row. Since (c_i) is a de Bruijn sequence, there exists an index ℓ such that $c_{\ell+i} = x_i - x_{i-1}$ for all $i = 1, \dots, u-1$. Since the numbers $a_{1,\ell}, \dots, a_{k,\ell}$ are pairwise distinct, there exists an index r such that $a_{r,\ell} = x_0$. Then by our construction we have

$$a_{r,\ell+i} = a_{r,\ell} + \sum_{s=1}^i c_{\ell+s} = x_0 + \sum_{s=1}^i (x_s - x_{s-1}) = x_i,$$

so we have found a desired $1 \times u$ rectangle.

Now assume that $u = 2$ and $k \geq 3$. We need to fill the rows of a $k \times k$ torus by the numbers $1, 2, \dots, k$ so that every pair of numbers appears as a pair of consecutive numbers in some row. In terms of a de Bruijn graph $G(2, k)$ introduced in the solution of **B.5**, we need to split the edges of this graph into k cyclic tours, each of length k .

If k is odd, say $k = 2t + 1$, then one may use the tours

$$(a \rightarrow (a+1) \rightarrow a \rightarrow (a+2) \rightarrow a \rightarrow \dots \rightarrow a \rightarrow (a+t) \rightarrow a \rightarrow a)$$

for $a = 1, 2, \dots, k$. (One may also mention that the model for $u \geq 3$ works in this case as well.)

If k is even, say $k = 2t$, then we may start with the tours

$$C_a = (a \rightarrow (a+1) \rightarrow a \rightarrow (a+2) \rightarrow a \rightarrow \dots \rightarrow a \rightarrow (a+t-1) \rightarrow a)$$

for all $a = 1, 2, \dots, 2t$. Each of these tours has length $2t-2$, and they cover all the edges except for those of the forms $x \rightarrow x$ and $x \rightarrow (x+t)$. Next, we augment each tour C_{2i-1} by two edges $(t+i-1) \rightarrow (i-1) \rightarrow (t+i-1)$, and we augment each tour C_{2i} by two loops $2i \rightarrow 2i$ and $(2i+1) \rightarrow (2i+1)$. One can easily check that this is possible, because these tours contain the vertices which are needed for such an augmentation.

E.2 Let $\dots, c_1, c_2, \dots, c_{k^2}, \dots$ be a de Bruijn sequence of rank 2 in the alphabet X_k (extended periodically). We put this sequence into each row with different shifts. Namely, in the i th row we shift this sequence to the right by $0 + 1 + \dots + (i-1)$ cells. Thus, the sequence in the i th row is shifted by $i-1$ with respect to the $(i-1)$ th row. Moreover, the sequence in the (k^2+1) th column is shifted (in total) by $1 + 2 + \dots + k^2$; this last sum is divisible by k^2 , thus our arrangement indeed defines a $k^2 \times k^2$ torus.

Now, for every 2×2 square, its first and second rows appear in our de Bruijn sequence. Assume that the occurrence of the second one is s terms to the right relatively to the occurrence of the first one. Then this square appears in the union of the s th and the $(s+1)$ th rows.

E.3 One may modify the method from the previous solution in order to work here as well. Again, we will construct a torus of type $(k^{u(v-1)}, k^u, v, u)_k$. For convenience, denote $R = k^{u(v-1)}$ and $S = k^u$.

We start with the de Bruijn sequence of rank u (its period length is S). We put it into the i th row shifting it to the right with respect to the previous row by some number d_i which will be defined later. (So the i th column is shifted by $d_1 + \dots + d_i$ relatively to the zeroth one.) Surely we should have $d_{i+R} = d_i$.

In order to provide a vertically R -periodic arrangement, the sum $d_1 + \dots + d_R$ should be divisible by S . Next, as in the previous problem, in order to obtain all possible $v \times u$ rectangles, we just need all the combinations of $v-1$ shifts to appear in the sequence (d_i) . Thus (d_i) should be just a de Bruijn sequence of rank $v-1$ in the alphabet X_S .

In particular, this means that the sum of the elements in the period of (d_i) is just

$$k^{u(v-2)} \cdot (1 + 2 + \dots + k^u),$$

and this number is indeed divisible by k^u for all $k, u, v \geq 2$, except for the case when $v-2 = 0$ and k^u is even.

E.4 $k = 2$ was shown in problem **A.3a**); thus we will assume that $k \geq 4$.

Step 1. Let us construct a rank 2 de Bruijn sequence $C = (c_1, \dots, c_{k^2})$ with an additional property that $c_{k^2/2} = c_{k^2}$. Consider a de Bruijn graph $G(2, k)$ and split all its edges into groups of the form $M_i = \{(\ell, \ell+i) : \ell = 1, 2, \dots, k\}$. Then let us merge all these groups into two equipotent sets so that M_1 and M_{k-1} are in distinct sets. Then we have split all the edges into two subgraphs, and both are connected and balanced.

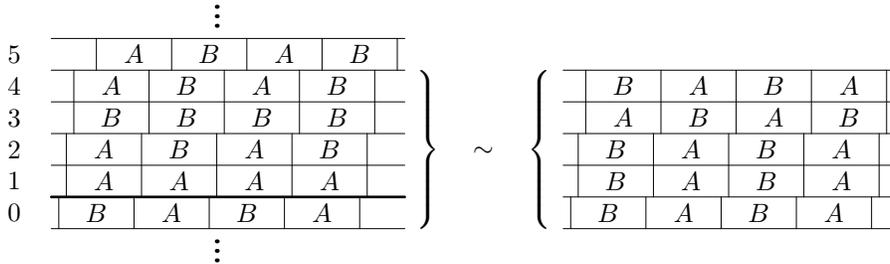
Let us take some Eulerian tours in these subgraphs and glue them at a common vertex v . We get the Eulerian tour in the whole graph, and two of the occurrences of v are half a tour apart from each other. This provides (by the methods used in **B.5**) exactly a required de Bruijn sequence.

Step 2. Now we perform almost the same procedure as in **E.2**. Consider a constructed de Bruin sequence C ; let A and B be its first and second halves. Notice that each sequence of two letters appears either in the sequence with period A or in the sequence with period B . (Here one needs to use the additional property of constructed sequence — why?)

Let us put the sequence with period C into the rows numbered from 4 to k^2 so that the relative shift of two neighboring rows takes all values from 0 to $k^2 - 1$, except for 0, 1, $k^2/2$, and $k^2/2 + 1$. The sum of all the numbers from 0 to $k^2 - 1$ is congruent to $k^2/2$ modulo k^2 . Then the k^2 th (as well as the zeroth) row is shifted relatively to the fourth one by $k^2/2 - 2$.

Next, we put the same sequence into the second row shifting it by one to the left relatively to the fourth row. Finally, we put the sequence with period A into the first row, and the sequence with period B to the third one. We shift them so that the parts A in the first and the second rows are put on the same level, and the same holds for the parts B in the third and the fourth rows (see the left picture below).

Due to the changes made in the procedure from **E.2**, we need to check that the 2×2 squares in rows from zeroth to the fourth are the same as they would be if these rows were just the usual de Bruijn sequences with the relative shifts of consecutive rows equal to 0, 1, $k^2/2$, and $k^2/2 + 1$. It is easy to see that the squares in the rows 1–2 and 3–4 are the same as they would be in two pairs of usual “de Bruijn rows” with relative shifts 0 and $k^2/2$. Similarly, the squares in the rows 0–1 and 2–3 are the same as they would be in two pairs of usual rows with relative shifts 1 and $k^2/2 + 1$.



E.5 There are several such construction. We will present one using the construction from problem **E.6**.

Assume that $k > 2$. Take a de Bruijn torus of type $(k^2, k^2, 2, 2)_k$ constructed in **E.2** (for odd k) or in **E.4** (for even k). One can check that in both constructions, the sum of letters in each row is 0 (it is almost trivial for the usual de Bruijn sequence; for the halves of the sequence used in **E.4**, one needs to involve their explicit construction). Thus one may apply **E.6** to this torus and reflect across the diagonal to get a de Bruijn torus of type $(k^4, k^2, 2, 3)_k$.

Pitifully, this method does not work for $k = 2$, since in the (essentially unique) construction of a de Bruijn torus of type $(4, 4, 2, 2)_2$ the row sums are odd. Here one may apply the method similar to those in the previous problems. Notice that the two columns of the $(4, 4, 2, 2)_2$ -torus contain all eight possible 3×1 arrangements; thus one needs only to combine them so that all possible pairings are present. One such arrangement is shown in the picture below.

1	1	0	0	1	0	1	1	1	0	0	1	1	0	1	1
0	0	1	1	0	1	1	1	0	0	1	1	0	0	1	0
0	0	1	1	0	0	0	1	0	1	1	0	0	0	0	1
0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1

E.6 For further purposes, we will prove a more general statement, where R and S are not necessarily powers of k , but are just positive integers with $RS = k^{uv}$. We act similarly to **E.1** using some additional construction.

Step 1. Now we need a sequence longer than a usual de Bruijn sequence. Namely, we need a cyclic sequence of letters in X_k with period $p_1, p_2, \dots, p_{S k^v}$ such that for every word $x_1 \dots x_v$ and for every number $\ell = 1, 2, \dots, S$

there exists an index $i \equiv \ell \pmod{S}$ such that $p_{i+1} = x_1, p_{i+2} = x_{i+2}, \dots, p_{i+v} = x_v$. So, each word of length v in the alphabet X_k would appear exactly S times in the period.

To reach the goal, we consider a different graph G' . Its vertices have the form $(w; i)$, where w is a word of length $v - 1$ in the alphabet X_k , and $i \in \{1, 2, \dots, S\}$ (the indices i will be regarded as residues modulo S). If the usual de Bruijn graph $G(v, k)$ contains an edge from w_1 to w_2 , then we draw an edge from $(w_1; i)$ to $(w_2; i + 1)$ for every $1, 2, \dots, S$. Clearly, G' is balanced and strongly connected, so there exists an Eulerian tour in this graph. If we now reconstruct a word from this tour in a usual manner, we get the desired sequence. Indeed, the required subword $x_1 \dots x_v$ in the position congruent to i modulo S corresponds exactly to the edge $(x_1 \dots x_{v-1}; i) \rightarrow (x_2 \dots x_v; i + 1)$.

Step 2. Now we are ready to construct a desired new torus. Let $a_{i,j}$ denote the letter in position (i, j) of the given torus. Consider a cell (I, J) in the new torus and let $j = J \pmod{S}$. Then we fill this cell with the number

$$A_{I,J} = p_J + \sum_{m=1}^I a_{m,j}.$$

By the conditions on the old torus, the new arrangement is vertically R -periodic. Obviously, this arrangement is also horizontally Sk^v -periodic.

Next, each row of this new torus satisfies the same property as the sequence constructed in Step 1. Indeed, the subwords of (p_j) in the positions congruent to i modulo S are just all possible words, and similar subwords of a certain row are obtained from them by componentwise addition of a fixed word.

Now it is easy to see that a constructed torus contains every possible $(u + 1) \times v$ rectangle. Let $(x_{i,j})$ be the arrangement of numbers in such a rectangle. Denote $y_{i,j} = x_{i+1,j} - x_{i,j}$. The arrangement $(y_{i,j})$ appears somewhere in the given torus, say in the positions $(\alpha + 1, \beta + 1)$ to $(\alpha + u, \beta + v)$. Then the new torus contains a desired arrangement in one of k^v positions of the form $(\alpha + 1, \beta + 1 + \mu S) - (\alpha + u + 1, \beta + v + \mu S)$ with $\mu = 0, 1, \dots, k^v - 1$, by the same reasoning as in **E.1**.

Remark. Due to the properties of all the rows, it is easily seen that the row sums of the obtained torus are all divisible by k . Thus one may apply the same procedure iteratively, switching the directions every time.

Moreover, one may see that it suffices to switch the direction every second time, provided that Sk^{v-2} . Indeed, let p_1, \dots, p_{Sk^v} be a period of some row in a constructed torus. The row of the second iteration will have the form

$$\alpha, \quad \alpha + p_1, \quad \alpha + (p_1 + p_2), \quad \dots, \quad \alpha + (p_1 + \dots + p_{Sk^v-1}).$$

The sum of all these elements is congruent modulo k to

$$-p_1 - 2p_2 - \dots - (Sk^v - 1)p_{Sk^v-1} \equiv -(p_1 + p_{k+1} + \dots + p_{Sk^v-k+1}) - 2(p_2 + p_{k+2} + \dots + p_{Sk^v-k+2}) - \dots.$$

In each bracket, every letter appears Sk^{v-2} times; this number is divisible by k , so the total sum is divisible by k as well.

E.7 Starting from the construction of **E.5**, we apply **E.6** thrice obtaining

$$(k^4, k^2, 2, 3)_k \xrightarrow{(1)} (k^4, k^5, 3, 3)_k \xrightarrow{(2)} (k^4, k^8, 4, 3)_k \xrightarrow{(3)} (k^8, k^8, 4, 4)_k;$$

surely sometimes we switch the horizontal and vertical directions. In order to show that **E.6** is applicable in each case, we need to show that the corresponding row/column sums are divisible by k in each of three steps. For step (3) it follows from the Remark after **E.6**. If $k > 2$, then the same holds for steps (1) and (2), as we have obtained the torus of type $(k^4, k^2, 2, 3)_k$ by the same procedure. In the exceptional case $k = 2$, one may check the desired condition manually (on the picture at the end of **E.5**).

It would be better to mention here that not all de Bruijn tori of type $(k^4, k^2, 2, 3)_k$ satisfy the required condition.

E.8 Firstly, let us prove the claim for even $n = 2t$ by the induction on t . The base cases $t = 1, 2$ have already been considered above.

Assume now that the torus of type $(k^{2t^2}, k^{2t^2}, 2t, 2t)$ has already been constructed, and **E.6** was applied last time to increase the vertical side of a torus. Then it suffices to apply **E.6** as

$$\begin{aligned}
(k^{2t^2}, k^{2t^2}, 2t, 2t)_k &\longrightarrow (k^{2t^2}, k^{2t(t+1)}, 2t+1, 2t)_k \\
&\longrightarrow (k^{2t^2+2t+1}, k^{2t(t+1)}, 2t+1, 2t+1)_k \\
&\longrightarrow (k^{2(t+1)^2}, k^{2t(t+1)}, 2t+1, 2t+2)_k \\
&\longrightarrow (k^{2(t+1)^2}, k^{2(t+1)^2}, 2t+2, 2t+2)_k.
\end{aligned}$$

Each time, the claim of **E.6** is applicable due to the Remark after its proof.

Assume now that n is odd but k is a perfect square, so $n = 2t + 1$ and $k = a^2$. Then we may start a similar induction. For the base case $t = 0$, it suffices to arrange the numbers $1, 2, \dots, a^2$ in the cells of a $a \times a$ square so that the sum in each column is divisible by a^2 (we need this condition in order to be able to apply **E.6**). For that, it suffices to split these numbers into a groups with equal sums, which is known to be possible.

For the induction step, assume that the torus of type $(a^{(2t+1)^2}, a^{(2t+1)^2}, 2t+1, 2t+1)_k$ has already been constructed, and **E.6** was applied last time to increase the vertical side of a torus (if it was applied at all). Then it suffices to apply **E.6** as

$$\begin{aligned}
(a^{(2t+1)^2}, a^{(2t+1)^2}, 2t+1, 2t+1)_k &\longrightarrow (a^{(2t+1)^2}, a^{(2t+1)(2t+3)}, 2t+2, 2t+1)_k \\
&\longrightarrow (a^{2t^2+8t+5}, a^{(2t+1)(2t+3)}, 2t+2, 2t+2)_k \\
&\longrightarrow (a^{(2t+3)^2}, a^{(2t+1)(2t+3)}, 2t+2, 2t+3)_k \\
&\longrightarrow (a^{(2t+3)^2}, a^{(2t+3)^2}, 2t+3, 2t+3)_k.
\end{aligned}$$

Again, the applicability of **E.6** is due to the Remark after its proof.

E.9 The case of even n is completely analogous to such case in the previous problem.

Assume now that $n = 2t + 1$ and $k = a^2$. If $n = 1$ then the statement is trivial. For $n \geq 3$, we also use the induction on t , but we need to establish the base case $t = 1$. We will obtain it with a help of **E.10**. By this problem, there exists a de Bruijn torus of type $(a^5, a^3, 2, 2)$. Moreover, the analysis of the construction in **E.10** shows that the sum of numbers in each row is divisible by k . Thus we may apply **E.6** twice to obtain

$$(a^5, a^3, 2, 2)_k \longrightarrow (a^9, a^3, 2, 3)_k \longrightarrow (a^9, a^9, 3, 3)_k,$$

as required.

The step of the induction goes exactly as in the previous problem.

E.10 As usual, we denote $k = 2st$, $R = 4st^2$, and $S = 4s^3t^2$.

Step 1. Let us find s cyclic sequences L_1, L_2, \dots, L_s , each of length $R = k^2/s$, such that every 2-letter word in alphabet X_k appears as a subword in exactly one of these sequences. This can be done exactly as in Step 1 of **E.4**, but now we need to split all the edges into s groups G_1, \dots, G_s , each with R edges, so that these groups define balanced connected subgraphs. The Eulerian tours in these subgraph will then provide the desired sequences.

We split again all the edges of $G(2, k)$ into k groups $M_i = \{(\ell, \ell + i) : \ell = 1, 2, \dots, k\}$. Firstly, we put into G_i the edges of groups M_{i-1} and M_{k-i} ; one can see that this already ensures that the resulting subgraphs will be connected. Then we distribute the other groups evenly between G_i 's. The construction is finished.

Step 2. Now we will construct a desired torus. Each column will contain just one of the sequences L_1, \dots, L_s shifted somehow. We fix a starting element of each of the sequences L_i ; after that, we may speak on the shifts of any of them relatively to any other.

Let $C = (c_1, \dots, c_{s^2})$ be a de Bruijn sequence of rank 2 in the alphabet X_s . Now we fill the columns as follows. Let I be the number of a column, and i be its residue modulo s^2 , so $I = i + s^2 \cdot j$. Then this column will contain the sequence L_{c_i} , and it will be shifted by j relatively to the previous column.

Consider the columns from zeroth to S th. We claim that every 2×2 square appears in these columns. Indeed, for every two indices i, i' the sequence L_i will follow $L_{i'}$ exactly R times, and all their relative shifts will be distinct; this yields our claim.

It remains to find the period of our arrangement. Since $S = Rs^2$, the S th column will be shifted relatively to the zeroth one by $(0 + 1 + \dots + (R - 1)) \cdot s^2$. If s is even, then this number is divisible by R , so we have obtained a required torus with periods R and S .

Assume now that s is odd. Then, pitifully, the total shift is divisible only by $R/2$. But then we may perform the same change as in **E.4**. Namely, one may see that in Step 1 we can split one of the groups G_i (say, G_2) into two balanced connected halves. Then the corresponding sequence L_2 can be also constructed in order to consist of two parts ending by the same letter. Then the same trick as in **E.4** is applicable. The details are left to the reader.

Remark: There is also a different construction for this problem.

F The continuation of Enumeration

F.1 Let us fix some edge from v ; we will assume that it is the first edge in each Eulerian tour. Consider any Eulerian cycle C . For each vertex $u \neq v$, let us mark the last edge from u in tour C . Denote the subgraph defined by the marked edges by T .

Assume that T contains an (unoriented) cycle ω . The out-degree of every vertex in T does not exceed 1, so ω is in fact an oriented cycle. Let e be the edge of ω which appears in C later than the others; let $u = t(e)$. Notice that $u \neq v$, since the out-degree of v in T is 0. Then the edge f of ω starting at u has to occur in C later than e ; otherwise, after having passed e in cycle C we would not be able to leave this vertex. This contradiction shows that T is acyclic. Therefore, if we start walking from an arbitrary vertex of G along the edges of T , we will eventually reach a vertex with no outgoing edges; such a vertex should be v . Thus, T is an oriented spanning tree rooted at v .

Thus, to every Eulerian cycle C corresponds some oriented spanning tree rooted at v ; now we will count the number of cycles corresponding to a particular tree T . This tree corresponds to those Eulerian cycles which start going from v along the fixed edge and avoid going via any edge of T as long as possible. Now we will show how to construct all such cycles.

For each vertex $u \neq v$, there are $(\text{outdeg}(u) - 1)!$ possible orderings of its outgoing edges not belonging to T (such an ordering will tell in which order the cycle should leave this vertex; the remaining edge should be the last one). For vertex v , there are again $(\text{outdeg}(v) - 1)!$ possible orderings of outgoing edges apart from the fixed one. We claim that every particular choice of all these orderings indeed determines an Eulerian cycle.

Let us start walking from v via the fixed edge; then we move according to the orderings until we get stuck. This could only happen at v ; denote the obtained cycle by C . Assume that C does not pass through some edge from a vertex u ; then it also does not pass along the edge from u in T . Considering a path from u to v in T , we find the edges e_1, e_2 lying in T such that $t(e_1) = s(e_2)$, and the cycle contains e_2 but not e_1 . This yields that C contains all the edges outgoing from $s(e_2)$ but not all edges ingoing to this vertex; this contradicts the balancedness of G .

Thus, each tree corresponds to $\prod_{u \in V(G)} (\text{outdeg}(u) - 1)!$ different Eulerian cycles, and the result follows.

Remark. As a corollary, we obtain that the number of oriented spanning trees rooted at some vertex v of a balanced strongly connected graph does not depend on the choice of v .

F.2 Answer. $B(k, n) = k!^{k^{n-1}} / k^n$.

The previous problem implies that $B(n, k)$ is $(k - 1)!^{k^{n-1}}$ times the number of oriented spanning trees with a fixed root in the de Bruijn graph $G_{k,n}$, i.e. $B(n, k)$ is $\frac{(k-1)!^{k^{n-1}}}{k^{n-1}}$ times the total number $\tau(G(k, n))$ of oriented spanning trees in $G(k, n)$. We prove by induction on n that $\tau(G_{k,n}) = k^{k^{n-1}-1}$; this immediately provides the answer.

The base $n = 1$ is clear. Notice that $G_{k,n+1} = \mathcal{L}G_{k,n}$. Therefore, plugging ones instead of all variables onto Levine's theorem we get

$$\tau(G_{k,n+1}) = \tau(G_{k,n})k^{(k-1)k^{n-1}},$$

which completes the inductive step.

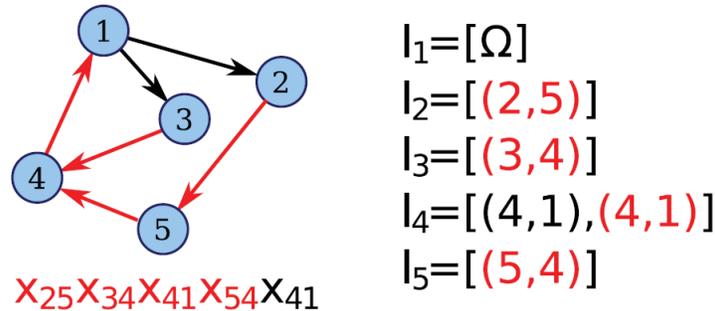
F.3 We present a proof from the article H. Bidkhori, S. Kishore. A bijective proof of a theorem of Knuth. *Combinatorics, Probability and Computing*, vol. 20, is. 01, 2011; the pictures are borrowed there as well.

Let us expand all the brackets in both sides of the desired equality; we are to prove that the multisets of the monomials in both sides are identical. We introduce the following notion.

Definition F.3 A tree array in a graph G is a set of ordered lists ℓ_v , one per vertex v of G , satisfying the following properties.

- a) The length of each list ℓ_v is $\text{indeg}(v)$. All the elements of this list are edges outgoing from v (possibly, with repetitions), with the only exception: the last element of exactly one list ℓ_{v_0} is some predefined symbol Ω .
- b) The last elements of all the lists ℓ_v with $v \neq v_0$ form an oriented spanning tree rooted at v_0 .

The picture below depicts an example of a tree array.



We put into correspondence to every tree array a monomial containing every variable x_e with an exponent equal to the number of occurrences of e in this array. One can easily see that the tree arrays are in one-to-one correspondence with the monomials in the RHS of the required equality (moreover, the arrays where the last edges of the lists form a particular tree correspond to the monomials obtained from a monomial of this tree in $\kappa^{\text{edge}}(G)$).

So, in order to prove our equality it suffices to construct a bijection of tree arrays in G and the spanning trees in \mathcal{LG} such that the monomial in $\kappa^{\text{vertex}}(\mathcal{LG})$ of a certain tree corresponds also to its tree array. Let \mathcal{A} be the set of tree arrays in G , and let \mathcal{T} be the set of oriented spanning trees in \mathcal{LG} . We will construct algorithmically mutually inverse mappings

$$\Sigma : \mathcal{A} \rightarrow \mathcal{T} \quad \text{and} \quad \Pi : \mathcal{T} \rightarrow \mathcal{A},$$

satisfying the abovementioned condition.

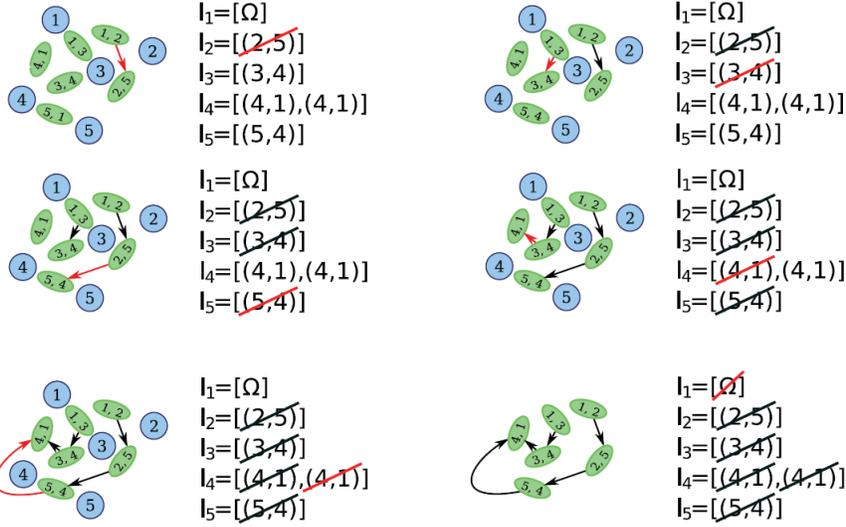
Let us fix an arbitrary enumeration of the edges of G .

Construction of Σ . Take an array $A \in \mathcal{A}$. We will construct its subgraph T edge by edge, accordingly reducing array A . We start with a subgraph T with no edges; we will define $\Sigma(A)$ as the obtained subgraph T when A is finally depleted. Denote the state of A and T after having performed the k th step by $A(k)$ and $T(k)$ respectively.

On the $(k+1)$ th move, let us choose an edge e with the smallest number such that e is not contained in $A(k)$ and its out-degree in $T(k)$ is zero. Let g be the first item in the list $\ell_{t(e)}$ of array $A(k)$. We define $A(k+1)$ by removing g from the beginning of this list. If $g = \Omega$ then we stop, otherwise we add the edge $e \rightarrow g$ to $T(k)$ forming the subgraph $T(k+1)$. The picture below depicts the stages of this algorithm working on the previous example array.

Let G contain d edges. After k steps we have k edges having nonzero out-degrees in $T(k)$ and at most $d-1-k$ distinct edges in $A(k)$. Thus we are able to choose some edge on the $(k+1)$ th step. Moreover, the list $\ell_{t(e)}$ will be nonempty, since this list decreases exactly when the in-degree of $t(e)$ decreases, so at most $\text{indeg}(t(e)) - 1$ times before this step.

We claim that T contains no oriented cycles. Indeed, if the edges $e_1 \rightarrow e_2, \dots, e_{n-1} \rightarrow e_n$ are already added to T , then it is impossible to add the edge $e_n \rightarrow e_1$ completing the cycle, since e_1 was absent in A already at the moment of introducing the edge $e_1 \rightarrow e_2$.



Now let M be the tree in G consisting of the last edges on the lists of A , and let r be its root. Consider any edge $e = (u, w)$ in M (thus this edge is in ℓ_u). Assume that at some step of the algorithm the list ℓ_v becomes empty. At this moment, T has already got all its edges ending at v ; in particular, the out-degree of e in T is nonzero at this moment. This means that e was chosen on some previous step. At that step, A already did not contain e , so at that step ℓ_u was empty. Thus, if ℓ_v is exhausted at some moment then ℓ_u had been exhausted before that.

Now consider the moment when ℓ_r empties; due to the arguments above, all the other lists should be empty at this moment as well. Thus the process will stop in exactly d steps, and the resulting subgraph $T = \Sigma(A)$ is an oriented spanning tree in $\mathcal{L}G$. It is easy to see that the monomials corresponding to A and to T coincide.

Construction of Π . Now take an oriented spanning tree $S \in \mathcal{T}$ rooted at r . We start with an empty array B , and we will increase this array while removing the edges from T . Denote the states of B and S after k th step by $B(k)$ and $S(k)$, respectively.

On the k th step, we consider all the vertices of $S(k)$ with the out-degree 1 and the in-degree 0, and we choose such a vertex e having the least number (recall that the vertices of $S(k)$ are edges of G). Let $e \rightarrow f$ be the edge of $S(k)$ from e . We remove this edge from S , and we add f to the end of list $\ell_{t(e)}$. When S becomes empty (which happens after $d - 1$ steps), we add Ω to the end of $\ell_{t(r)}$.

When the algorithm halts, the length of every list ℓ_v in B equals $\text{indeg}(v)$. Now let M be a subgraph in G formed by all last edges in the lists ℓ_v . Assume that M contains an edge $f = (u, w)$ (lying in ℓ_u). We prove that the list ℓ_v has been completed after the list ℓ_u had been completed. Indeed, when list ℓ_w is complete, vertex f of graph S should become isolated; therefore, all the edges which ended at this vertex in the original graph S were worked out before; so f appeared in list ℓ_u or the last time before this moment.

This property yields that M contains no oriented cycles. Since each vertex of M except for $t(r)$ has exactly one out-edge, M is an oriented spanning tree. Therefore, B is a tree array, and we set $B = \Pi(S)$.

It remains to show that the mappings Σ and Π are mutually inverse. Let $T = \Sigma(A)$, and let the first k steps of the algorithm constructing $\Sigma(A)$ delete from A the edges f_1, \dots, f_k and insert to T the edges $e_1 \rightarrow f_1, \dots, e_k \rightarrow f_k$ in this order. We show by the induction on k that the first k steps of the algorithm constructing $B = \Pi(T)$ insert to B the edges f_1, \dots, f_k and delete from T the edges $e_1 \rightarrow f_1, \dots, e_k \rightarrow f_k$ in the same order.

The base $k = 0$ is trivial. For the step, consider the $(k + 1)$ th step of the Π -algorithm. By the induction hypothesis, the edge $e_{k+1} \rightarrow f_{k+1}$ exists in subgraph $T(k)$. Moreover, $T(k)$ cannot contain an edge of the form $e \rightarrow e_{k+1}$, otherwise this edge would have been added to T on some step of Σ with number $\ell > k + 1$; but before this ℓ th step array $A(\ell - 1)$ did not contain edge e_{k+1} — a contradiction. Thus e_{k+1} has required in- and out-degrees in $T(k)$.

On the other hand, if $T(k)$ contains some edge $e \rightarrow e'$ such that the in-degree of e in $T(k)$ is zero, then the number of e is greater than that of e_{k+1} ; otherwise we would add the edge $e \rightarrow e'$ to T on the $(k+1)$ th step of Σ instead of $e_{k+1} \rightarrow f_{k+1}$. Therefore, on the $(k+1)$ th step of Π we indeed should delete edge $e_{k+1} \rightarrow f_{k+1}$ from T and add edge f_{k+1} to B .

So, we have proved that $\Pi(\Sigma(A)) = A$ for all $A \in \mathcal{A}$. The proof of the relation $\Sigma(\Pi(T)) = T$ for all $T \in \mathcal{T}$ is analogous.

Remark. The original Levine's proof of his theorem was algebraic, and it involved some technique using determinants.

G de Bruijn sequences via recurrences

G.1 The proof of this statement involves some involved algebraic technique. If you are not acquainted with this technique, you may either postpone reading this solution for several years, or read some algebraic literature before. We use several classical facts without proof. It is known that for every positive integer n there exists a degree n polynomial f which is irreducible over the 2-element field F_2 . Next, the residue classes modulo this polynomial f form a field K with 2^n elements. For every nonzero $u \in K$ the equality $u^{2^n-1} = 1$ holds; moreover, it is known that there exists a nonzero $\xi \in K$ such that $\xi^t \neq 1$ for all $0 < t < 2^n - 1$. Thus all nonzero elements of K are just the powers of ξ .

Now consider a polynomial g irreducible over F_2 such that $g(\xi) = 0$. Then g divides the polynomial $x^{2^n} - x$ which has no multiple roots (since its roots are just all elements of K). Hence, g has n distinct roots in K . We have $\deg g = n$ since $|F_2(u)| = 2^n$. So we may write $g = x^{k_1-1} + \dots + x^{k_s-1} + x^n$, where $k_1 < k_2 < \dots < k_s$. Now we define a template putting X exactly at the positions with numbers k_1, k_2, \dots, k_s .

Next, let $\xi = \xi_1, \xi_2, \dots, \xi_n$ be the roots of g . The following system of linear equations

$$\begin{cases} x_1 + x_2 + \dots + x_n = 0 \\ \xi_1 x_1 + \xi_2 x_2 + \dots + \xi_n x_n = 0 \\ \vdots \\ \xi_1^{n-2} x_1 + \xi_2^{n-2} x_2 + \dots + \xi_n^{n-2} x_n = 0 \\ \xi_1^{n-1} x_1 + \xi_2^{n-1} x_2 + \dots + \xi_n^{n-1} x_n = 1 \end{cases}$$

has a unique solution, since its determinant is nonzero (it is simply the Vandermonde determinant). It is easy to check now that the sequence determined by our template can be also defined as

$$a_k = x_1 \xi_1^k + \dots + x_n \xi_n^k.$$

For every $n > 1$ we have $k_1 = 1$ since g is irreducible. One may see then that the sequence (a_k) is purely periodic, since each piece of this sequence of length n determines uniquely both the previous and the next its pieces. Let the period have the length t . The equalities $a_t = a_0, a_{t+1} = a_1, \dots, a_{t+n-1} = a_{n-1}$ together with the uniqueness of the solution of the system yield $x_1 \xi_1^t = x_1, \dots, x_n \xi_n^t = x_n$. Since one of the x_i 's is nonzero, we get $\xi_i^t = 1$. Therefore, $t \geq 2^n - 1$, since the extensions $F_2(\xi_i)$ and $F_2(u)$ are isomorphic. On the other hand, we have $t \leq 2^n - 1$ since the piece of n zeroes cannot occur in our sequence, and the first repetition of the piece of n consecutive terms yields the periodicity.



Universal cycles for permutations

J. Robert Johnson

School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK

Received 24 March 2006; received in revised form 17 July 2007; accepted 2 November 2007

Available online 20 February 2008

Abstract

A universal cycle for permutations is a word of length $n!$ such that each of the $n!$ possible relative orders of n distinct integers occurs as a cyclic interval of the word. We show how to construct such a universal cycle in which only $n + 1$ distinct integers are used. This is best possible and proves a conjecture of Chung, Diaconis and Graham.

© 2007 Elsevier B.V. All rights reserved.

Keywords: Universal cycles; Combinatorial generation; Permutations

1. Introduction

A *de Bruijn cycle* of order n is a word in $\{0, 1\}^{2^n}$ in which each n -tuple in $\{0, 1\}^n$ appears exactly once as a cyclic interval (see [2]). The idea of a universal cycle generalizes the notion of a de Bruijn cycle.

Suppose that \mathcal{F} is a family of combinatorial objects with $|\mathcal{F}| = N$, each of which is represented (not necessarily in a unique way) by an n -tuple over some alphabet A . A *universal cycle* (or *ucycle*) for \mathcal{F} is a word $u_1u_2 \dots u_N$ with each $F \in \mathcal{F}$ represented by exactly one $u_{i+1}u_{i+2} \dots u_{i+n}$ where, here and throughout, index addition is interpreted modulo N . With this terminology a de Bruijn cycle is a ucycle for words of length n over $\{0, 1\}$ with a word represented by itself. The definition of ucycle was introduced by Chung, Diaconis and Graham in [1]. Their paper, and the references therein, forms an good overview of the topic of universal cycles. The cases considered by them include \mathcal{F} being the set of permutations of an n -set, r -subsets of an n -set, and partitions of an n -set.

In this paper we will be concerned with ucycles for permutations: our family \mathcal{F} will be S_n , which we will regard as the set of all n -tuples of distinct elements of $[n] = \{1, 2, \dots, n\}$. It is not immediately obvious how we should represent permutations with words. The most natural thing to do would be to take $A = [n]$ and represent a permutation by itself, but it is easily verified that (except when $n \leq 2$) it is not possible to have a ucycle in this case. Indeed, if every cyclic interval of a word is to represent a permutation then our word must repeat with period n , and so only n distinct permutations can be represented. Another possibility which we mention in passing would be to represent the permutation $a_1a_2 \dots a_n$ by $a_1a_2 \dots a_{n-1}$. It is clear that the permutation is determined by this. It was shown by Jackson [3] (using similar techniques to those used for de Bruijn cycles) that these ucycles exist for all n . Recently an efficient algorithm for constructing such ucycles was given by Williams [4]. He introduced the term *shorthand universal cycles for permutations* to describe them. Alternatively, Chung, Diaconis and Graham in [1] consider ucycles

E-mail address: r.johnson@qmul.ac.uk.

for permutations using a larger alphabet where each permutation is represented by any n -tuple in which the elements have the same relative order. Our aim is to prove their conjecture that such cycles always exist when the alphabet is of size $n + 1$, the smallest possible. In contrast to the situation with shorthand universal cycles, the techniques used for de Bruijn cycles do not seem to help with this so a different approach is needed.

To describe the problem more formally we need the notion of order-isomorphism. If $a = a_1a_2 \dots a_n$ and $b = b_1b_2 \dots b_n$ are n -tuples of distinct integers, we say that a and b are *order-isomorphic* if

$$a_i < a_j \Leftrightarrow b_i < b_j$$

for all $1 \leq i, j \leq n$. Note that no two distinct permutations in S_n are order-isomorphic, and that any n -tuple of distinct integers is order-isomorphic to exactly one permutation in S_n . Hence, the set of n -tuples of distinct integers is partitioned into $n!$ order-isomorphism classes which correspond to the elements of S_n .

We say that a word $u_1u_2 \dots u_n!$ over an alphabet $A \subset \mathbb{Z}$ is a *ucycle* for S_n if there is exactly one $u_{i+1}u_{i+2} \dots u_{i+n}$ order-isomorphic to each permutation in S_n . For example 012032 is a ucycle for S_3 . Let $M(n)$ be the smallest integer m for which there is a ucycle for S_n with $|A| = m$. Note that if $|A| = n$ then each permutation is represented by itself and so, as we noted earlier, no ucycle is possible (unless $n \leq 2$). We deduce that $M(n) \geq n + 1$ for all $n \geq 3$. Chung, Diaconis and Graham in [1] give the upper bound $M(n) \leq 6n$ and conjecture that $M(n) = n + 1$ for all $n \geq 3$. Our main result is that this conjecture is true.

Theorem 1. *For all $n \geq 3$ there exists a word of length $n!$ over the alphabet $\{0, 1, 2, \dots, n\}$ such that each element of S_n is order-isomorphic to exactly one of the $n!$ cyclic intervals of length n .*

We prove this by constructing such a word inductively. The details of our construction are in the next section. Having shown that such a word exists, it is natural to ask how many there are. In the final section we give some bounds on this.

Our construction works for $n \geq 5$. For smaller values of n it is a relatively simple matter to find such words by hand. For completeness examples are 012032 for $n = 3$, and 012301423042103421302143 for $n = 4$.

2. A construction of a universal cycle

We will show how to construct a word of length $n!$ over the alphabet $\{0, 1, 2, \dots, n\}$ such that for each $a \in S_n$ there is a cyclic interval which is order-isomorphic to a .

Before describing the construction we make a few preliminary definitions.

As is standard for universal cycle problems we let $G_n = (V, E)$, the *transition graph*, be the directed graph with

$$V = \{(a_1a_2 \dots a_n) : a_i \in \{0, 1, 2, \dots, n\}, \text{ and } a_i \neq a_j \text{ for all } i \neq j\}$$

$$E = \{(a_1a_2 \dots a_n)(b_1b_2 \dots b_n) : a_{i+1} = b_i \text{ for all } 1 \leq i \leq n - 1\}.$$

Notice that every vertex of G_n has out-degree and in-degree both equal to 2.

The vertices on a directed cycle in G_n plainly correspond to the n -tuples which occur as cyclic intervals of some word. Our task, therefore, is to find a directed cycle in G_n of length $n!$ such that for each $a \in S_n$ there is some vertex of our cycle which is order-isomorphic to a . This is in contrast to many universal cycle problems where we seek a Hamilton cycle in the transition graph.

We define the map on the integers:

$$s_x(i) = \begin{cases} i & \text{if } i < x \\ i + 1 & \text{if } i \geq x. \end{cases}$$

We also, with a slight abuse of notation, write s_x for the map constructed by applying this map coordinatewise to an n -tuple. That is,

$$s_x(a_1a_2 \dots a_n) = s_x(a_1)s_x(a_2) \dots s_x(a_n).$$

The point of this definition is that if $a = a_1a_2 \dots a_n \in S_n$ is a permutation of $[n]$ and $x \in [n + 1]$ then $s_x(a)$ is the unique n -tuple of elements of $[n + 1] \setminus \{x\}$ which is order-isomorphic to a . Note that, as will become clear, this is

the definition we need even though our final construction will produce a ucycle for permutations of $[n]$ using alphabet $\{0, 1, 2, \dots, n\}$.

We also define a map r on n -tuples which permutes the elements of the n -tuple cyclically. That is,

$$r(a_1a_2 \dots a_n) = a_2a_3 \dots a_{n-1}a_na_1.$$

Note that $(a, r(a))$ is an edge of G_n and that $r^n(a) = a$.

As indicated above, we prove **Theorem 1** by constructing a cycle of length $n!$ in G_n such that for each $a \in S_n$ the cycle contains a vertex which is order-isomorphic to a . Our approach is to find a collection of short cycles in G_n which between them contain one vertex from each order-isomorphism class and to join them up. The joining up of the short cycles requires a slightly involved induction step which is where the main work lies.

Proof of Theorem 1. *Step 1:* Finding short cycles in G_n .

The first step is to find a collection of short cycles (each of length n) in G_n which between them contain exactly one element from each order-isomorphism class of S_n . These cycles will use only n elements from the alphabet and we will think of each cycle as being “labelled” with the remaining unused element. Suppose that for each $a = a_1a_2 \dots a_{n-1} \in S_{n-1}$ we choose a label $l(a)$ from $[n]$. Let $0a$ be the n -tuple $0a_1a_2 \dots a_{n-1}$. We have the following cycle in G_n :

$$s_{l(a)}(0a), r(s_{l(a)}(0a)), r^2(s_{l(a)}(0a)), \dots, r^{n-1}(s_{l(a)}(0a)).$$

We denote this cycle by $\mathcal{C}(a, l(a))$. As an example, $\mathcal{C}(42135, 2)$ is the following cycle in G_6 :

$$053146 \rightarrow 531460 \rightarrow 314605 \rightarrow 146053 \rightarrow 460531 \rightarrow 605314 \rightarrow 053416,$$

where arrows denote directed edges of G_6 .

Note that for any choice of labels (that is any map l) the cycles $\mathcal{C}(a, l(a))$ and $\mathcal{C}(b, l(b))$ are disjoint when $a, b \in S_n$ are distinct. Consequently, whatever the choice of labels, the collection of cycles

$$\bigcup_{a \in S_{n-1}} \mathcal{C}(a, l(a))$$

is a disjoint union. It is easy to see that the vertices on these cycles contain between them exactly one n -tuple order-isomorphic to each permutation in S_n .

We must now show how, given a suitable labelling, we can join up these short cycles.

Step 2: Joining two of these cycles

Suppose that $\mathcal{C}_1 = \mathcal{C}(a, x)$ and $\mathcal{C}_2 = \mathcal{C}(b, y)$ are two of the cycles in G_n described above. What conditions on a, b and their labels x, y will allow us to join these cycles?

We may assume that $x \leq y$. Suppose further that $1 \leq x \leq y - 2 \leq n - 1$, and that a and b satisfy the following:

$$b_i = \begin{cases} a_i & \text{if } 1 \leq a_i \leq x - 1 \\ a_i + 1 & \text{if } x \leq a_i \leq y - 2 \\ x & \text{if } a_i = y - 1 \\ a_i & \text{if } y \leq a_i \leq n - 1. \end{cases}$$

If this happens we will say that the pair of cycles $\mathcal{C}(a, x), \mathcal{C}(b, y)$ are *linkable*.

In this case $s_x(0a)$ and $s_y(0b)$ agree at all but one position; they differ only at the t for which $a_t = y - 1$ and $b_t = x$. It follows that there is a directed edge in G_n from

$$r^t(s_x(0a)) = s_x(a_t \dots a_{n-1}0a_1 \dots a_{t-1})$$

to

$$r^{t+1}(s_y(0b)) = s_y(b_{t+1} \dots b_{n-1}0b_1 \dots b_t).$$

Similarly, there is a directed edge in G_n from

$$r^t(s_y(0b)) = s_x(b_t \dots b_{n-1}0b_1 \dots b_{t-1})$$

to

$$r^{t+1}(s_x(0a)) = s_y(a_{t+1} \dots a_{n-1}0a_1 \dots a_t).$$

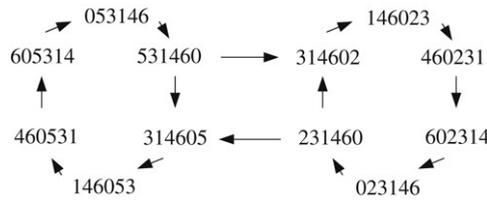


Fig. 1. The cycles $\mathcal{C}(42135, 2)$ and $\mathcal{C}(23145, 5)$ are linkable.

If we add these edges to $\mathcal{C}_1 \cup \mathcal{C}_2$ and remove the edges

$$r^t(s_x(0a))r^{t+1}(s_x(0a))$$

and

$$r^t(s_y(0b))r^{t+1}(s_y(0b)),$$

then we produce a single cycle of length $2n$ whose vertices are precisely the vertices in $\mathcal{C}_1 \cup \mathcal{C}_2$.

We remark that if $x = y - 1$ then the other conditions imply that $a = b$ and so although we can perform a similar linking operation it is not useful. If $x = y$ then b is not well defined.

As an example of the linking operation consider the linkable pair of 6-cycles $\mathcal{C}(42135, 2)$ and $\mathcal{C}(23145, 5)$ in G_6 . If we add the edges $531460 \rightarrow 314602$ and $231460 \rightarrow 314605$, and remove the edges $531460 \rightarrow 314605$ and $231460 \rightarrow 314602$ then a single cycle of length 12 in G_6 is produced. These cycles and the linking operation are shown in Fig. 1.

Step 3: Joining all of these cycles

We now show that this linking operation can be used repeatedly to join a collection of disjoint short cycles, one for each $a \in S_n$, together.

Let $H_n = (V, E)$ be the (undirected) graph with,

$$V = \{(a, x) : a \in S_{n-1}, x \in [n]\}$$

$$E = \{(a, x)(b, y) : \mathcal{C}(a, x), \mathcal{C}(b, y) \text{ are linkable}\}.$$

If we can find a subtree T_n of H_n of order $(n - 1)!$ which contains exactly one vertex (a, x) for each $a \in S_{n-1}$ then we will be able to construct the required cycle. Take any vertex $(a, l(a))$ of T_n and consider the cycle $\mathcal{C}(a, l(a))$ associated with it. Consider also the cycles associated with all the neighbours in T_n of $(a, l(a))$. The linking operation described above can be used to join the cycles associated with these neighbours to $\mathcal{C}(a, l(a))$. This is because the definition of adjacency in H_n guarantees that we can join each of these cycles individually. Also, the fact that every vertex in G_n has out-degree 2 means that the joining happens at different places along the cycle. That is if $(b, l(b))$ and $(c, l(c))$ are distinct neighbours of $(a, l(a))$ then the edge of $\mathcal{C}(a, l(a))$ which must be deleted to join $\mathcal{C}(b, l(b))$ to it is not the same as the one which must be deleted to join $\mathcal{C}(c, l(c))$ to it. We conclude that we can join all of the relevant cycles to the cycle associated with $(a, l(a))$. The connectivity of T_n now implies that we can join all of the cycles associated with vertices of T_n into one cycle. This is plainly a cycle with the required properties.

The next step is to find such a subtree in H_n .

Step 4: Constructing a Suitable Tree

We will prove, by induction on n , the stronger statement that for all $n \geq 5$, there is a subtree T_n of H_n of order $(n - 1)!$ which satisfies:

1. for all $a \in S_{n-1}$ there exists a unique $x \in [n]$ such that $(a, x) \in V(T_n)$,
2. $(12 \dots (n - 1), 1) \in V(T_n)$,
3. $(23 \dots (k - 1)1(k)(k + 1) \dots (n - 1), k) \in V(T_n)$ for all $3 \leq k \leq n$,
4. $(32145 \dots (n - 1), 2) \in V(T_n)$,
5. $(243156 \dots (n - 1), 3) \in V(T_n)$,
6. $v(31245 \dots (n - 1))$ is a leaf in T_n ,
7. $v(24135 \dots (n - 1))$ is a leaf in T_n .

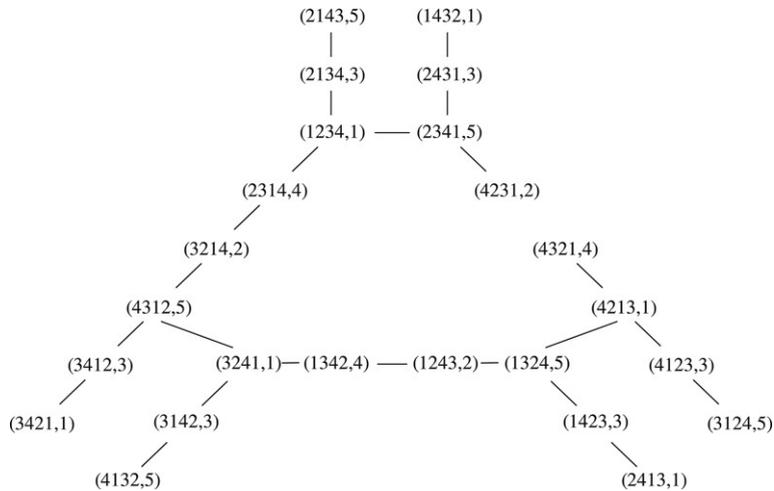


Fig. 2. A suitable choice for T_5 .

Where, for a tree satisfying property 1, we denote the unique vertex in $V(T_n)$ of the form (a, x) by $v(a)$.

For $n = 5$ a suitable tree can be found. One such is given in Fig. 2.

Suppose that $n \geq 5$ and that we have a subtree T_n of the graph H_n which satisfies the above conditions. We will use this to build a suitable subtree of H_{n+1} .

A key observation for our construction is that the map from $V(H_n)$ to $V(H_{n+1})$ obtained by replacing each vertex $(a_1 a_2 \dots a_{n-1}, x) \in V(H_n)$ by $(1(a_1 + 1)(a_2 + 1) \dots (a_{n-1} + 1), x + 1) \in V(H_{n+1})$ preserves adjacency. It follows that subgraphs of H_n are mapped into isomorphic copies in H_{n+1} by this map. Further, applying a fixed permutation to the coordinates of the n -tuple associated with each vertex of H_{n+1} gives an automorphism of H_{n+1} and so subgraphs of H_{n+1} are mapped into isomorphic copies.

We take n copies of T_n . These copies will be modified to form the building blocks for our subtree of H_{n+1} as follows.

In the first copy we replace each vertex $(a_1 a_2 \dots a_{n-1}, x)$ by

$$(1(a_3 + 1)(a_1 + 1)(a_4 + 1)(a_2 + 1)(a_5 + 1)(a_6 + 1) \dots (a_{n-1} + 1), x + 1).$$

By the observation above this gives an isomorphic copy of T_n in H_{n+1} . We denote this tree by $T_{n+1}^{(0)}$.

In the next copy we replace each vertex $(a_1 a_2 \dots a_{n-1}, x)$ by

$$((a_3 + 1)1(a_2 + 1)(a_1 + 1)(a_4 + 1)(a_5 + 1) \dots (a_{n-1} + 1), x + 1).$$

We denote this tree by $T_{n+1}^{(1)}$.

For all $2 \leq k \leq n - 1$, we take a new copy of T_n and modify it as follows. We replace each vertex $(a_1, a_2 \dots a_{n-1}, x)$ by

$$((a_k + 1)(a_1 + 1)(a_2 + 1) \dots (a_{k-1} + 1)1(a_{k+1} + 1) \dots (a_{n-1} + 1), x + 1).$$

We denote these trees by $T_{n+1}^{(2)}, T_{n+1}^{(3)}, \dots, T_{n+1}^{(n-1)}$.

As we mentioned this results in n subtrees of H_{n+1} . They are clearly disjoint because the position in which 1 appears in the first coordinate of each vertex is distinct for distinct trees. Let F_{n+1} be the n component subforest of H_{n+1} formed by taking the union of the trees $T_{n+1}^{(k)}$ for $0 \leq k \leq n - 1$.

It is also easy to see that for every $a \in S_n$ there is a vertex in F_{n+1} of the form (a, x) for some $x \in [n + 1]$. It remains to show that the n components can be joined up to form a single tree with the required properties.

Notice that it is a consequence of the construction of the $T_{n+1}^{(k)}$ that if $v(l_1 l_2 \dots l_{n-1})$ is a leaf in T_n then the following vertices are all leaves in F_{n+1} :

- $v(1(l_3 + 1)(l_1 + 1)(l_4 + 1)(l_2 + 1)(l_5 + 1)(l_6 + 1) \dots (l_{n-1} + 1))$
- $v((l_3 + 1)1(l_2 + 1)(l_1 + 1)(l_4 + 1)(l_5 + 1) \dots (l_{n-1} + 1))$
- $v((l_k + 1)(l_1 + 1)(l_2 + 1) \dots (l_{k-1} + 1)1(l_{k+1} + 1) \dots (l_{n-1} + 1))$ for $2 \leq k \leq n - 1$.

We claim that $v(12 \dots n)$ is a leaf in $T_{n+1}^{(0)}$, and hence a leaf in F_{n+1} . This follows from the fact that $v(24135 \dots (n-1))$ is a leaf in T_n and the remark above. We delete this vertex from F_{n+1} to form a new forest.

The construction of the $T_{n+1}^{(k-1)}$ and the fact that $(23 \dots (k-1)1(k)(k+1) \dots (n-1), k) \in V(T_n)$ for all $3 \leq k \leq n$ means that $(23 \dots k1(k+1)(k+2) \dots n, k+1) \in V(F_{n+1})$ for all $3 \leq k \leq n$. Further, the construction of the $T_{n+1}^{(1)}$ and the fact that $(32145 \dots (n-1), 2) \in V(T_n)$ means that $(2134 \dots n, 3) \in V(F_{n+1})$.

We add to F_{n+1} a new vertex $(123 \dots n, 1)$ (this replaces the deleted vertex from $T_{n+1}^{(0)}$) and edges from this new vertex to $(23 \dots k1(k+1)(k+2) \dots n, k+1)$ for all $2 \leq k \leq n$. The previous observation shows that all of these vertices are in F_{n+1} , and it is easy to check, using the definition of linkability, that the added edges are in H_{n+1} . This new forest has only two components.

Similarly, the inductive hypothesis that $v(31245 \dots (n-1))$ is a leaf in T_n gives that $v(342156 \dots n)$ is a leaf in F_{n+1} (using the case $k = 3$ of the observation on leaves). We delete this leaf from the forest, replace it with a new vertex $(342156 \dots n, 1)$, and add edges from this new vertex to $(341256 \dots n, 3)$ and $(143256 \dots n, 4)$. The construction of $T_{n+1}^{(2)}$ and the fact that $(32145 \dots (n-1), 2) \in V(T_n)$ ensures that the first of these vertices is in F_{n+1} . The construction of $T_{n+1}^{(0)}$ and the fact that $(243156 \dots (n-1), 3) \in V(T_n)$ ensures that the second of these vertices is in our modified $T_{n+1}^{(0)}$.

These modifications to F_{n+1} produce a forest of one component—that is a tree. Denote this tree by T_{n+1} . We will be done if we can show that T_{n+1} satisfies the properties demanded.

Plainly, T_{n+1} contains exactly one vertex of the form (a, x) for each $a \in S_n$. By construction $(12 \dots n, 1)$, and $(23 \dots t1(t+1)(t+2) \dots n, t+1)$ are vertices of T_{n+1} for all $2 \leq t \leq n$. Hence the first three properties are satisfied.

The construction of $T_{n+1}^{(2)}$ and the fact that $(123 \dots (n-1), 1) \in V(T_n)$ ensures that $(32145 \dots n, 2)$ is a vertex of T_{n+1} . The construction of $T_{n+1}^{(3)}$ and the fact that $(32145 \dots (n-1), 2) \in V(T_n)$ ensures that $(243156 \dots n, 3)$ is a vertex of T_{n+1} . Hence properties 4 and 5 are satisfied.

Finally, the construction of $T_{n+1}^{(1)}$ and the fact that $v(31245 \dots (n-1))$ is a leaf in T_n ensures that $v(31245 \dots n)$ is a leaf in F_{n+1} . The modifications which F_{n+1} undergoes do not change this and so it is a leaf in T_{n+1} . The construction of $T_{n+1}^{(2)}$ and the fact that $v(31245 \dots (n-1))$ is a leaf in T_n ensures that $v(241356 \dots n)$ is a leaf in F_{n+1} . Again, the modifications to F_{n+1} do not change this and so this vertex is still a leaf in T_{n+1} . Hence properties 6 and 7 are satisfied.

We conclude that the tree T_{n+1} has the required properties. This completes the construction. \square

3. Bounds on the number of universal cycles

Having constructed a ucycle for S_n over the alphabet $\{0, 1, \dots, n\}$ it is natural to ask how many such ucycles exist. We will regard words which differ only by a cyclic permutation as the same so we normalize our universal cycles by insisting that the first n entries give a word order-isomorphic to $12 \dots n$. We denote by $U(n)$ the number of words of length $n!$ over the alphabet $\{0, 1, 2, \dots, n\}$ which contain exactly one cyclic interval order-isomorphic to each permutation in S_n and for which the first n entries form a word which is order-isomorphic to $12 \dots n$. There is a natural upper bound which is essentially exponential in $n!$ based on the fact that if we are writing down the word one letter at a time we have 2 choices for each letter. We can also show that there is enough choice in the construction of the previous section to prove a lower bound which is exponential in $(n-1)!$. It is slightly surprising that our construction gives a lower bound which is this large. However, the upper and lower bounds are still far apart and we have no idea where the true answer lies.

Theorem 2.

$$420^{\frac{(n-1)!}{24}} \leq U(n) \leq (n+1)2^{n!-n}.$$

Proof. Suppose we write down our universal cycle one letter at a time. We must start by writing down a word of length n which is order-isomorphic to $12 \dots n$; there are $n+1$ ways of doing this. For each of the next $n! - n$ entries we must not choose any of the previous $(n-1)$ entries (all of which are distinct) and so we have 2 choices for each entry. This gives the required upper bound.

Now for the lower bound. We will give a lower bound on the number of subtrees of H_n which satisfies the conditions of step 4 of the proof of Theorem 1. It can be checked that if a universal cycle comes from a subtree of H_n in the way

described then the tree is determined by the universal cycle. It follows that the number of such trees is a lower bound for $U(n)$.

Notice that if we have t_n such subtrees of H_n then we have at least t_n^n such subtrees of H_{n+1} . This is because in our construction we took n copies of T_n to build T_{n+1} from and each different set of choices yields a different tree. We conclude that the number of subtrees of H_n satisfying the conditions is at least

$$t_5^{5 \times 6 \times \dots \times n-1} = t_5^{\frac{(n-1)!}{24}}.$$

Finally, we bound t_5 . We modify the given T_5 by adding edges from (1432, 1) to (2143, 5), from (3421, 1) to (4132, 5) and from (4231, 2) to (4321, 4). This graph is such that any of its spanning trees satisfies the properties for our T_5 . It can be checked that this graph has 420 spanning trees. This gives the lower bound. \square

Acknowledgements

This work was inspired by the workshop on Generalizations of de Bruijn Cycles and Gray Codes held at Banff in December 2004. I thank the organizers and participants of the workshop for a stimulating and enjoyable week.

References

- [1] F. Chung, P. Diaconis, R. Graham, Universal cycles for combinatorial structures, *Discrete Math.* 110 (1993) 43–59.
- [2] N.G. de Bruijn, A combinatorial problem, *Nederl. Akad. Wetensch., Proc.* 49 (1946) 758–764.
- [3] B.W. Jackson, Universal cycles for k -subsets and k -permutations, *Discrete Math.* 117 (1993) 141–150.
- [4] A.M. Williams, Shorthand universal cycles for permutations, in: *ACM–SIAM Symposium on Discrete Algorithms 2008, 2007* (submitted for publication).

Вокруг теоремы Понселе

Е.Диомидов, А.Заславский, В.Калашников, П.Кожевников, Г.Челноков

В наиболее простой форме теорема Понселе утверждает следующее.

Теорема Понселе. Пусть даны две окружности, одна из которых лежит внутри другой. Из точки A_0 большей окружности Ω проведем касательную к меньшей ω и найдем вторую точку A_1 пересечения этой касательной с большей окружностью. По точке A_1 аналогично построим точку A_2 и т.д. Тогда, если $A_0 = A_n$ для какой-то точки A_0 , это будет выполнено и для любой другой точки большой окружности

Говоря неформально, вписанно-описанный многоугольник¹ можно "вращать" между двумя окружностями (при этом его форма, вообще говоря, меняется). Будем называть такой "вращающийся" многоугольник *многоугольником Понселе*.

Целью данного проекта является доказательство теоремы Понселе и изучение свойств многоугольников Понселе, а также знакомство с обобщениями теоремы Понселе и некоторыми другими похожими теоремами.

1 Теорема Понселе для $n = 3, 4$

1. Пусть O, I — центры описанной и вписанной окружностей треугольника, R, r — их радиусы. Докажите **формулу Эйлера**

$$OI^2 = R^2 - 2Rr.$$

2. Докажите теорему Понселе для $n = 3$.

С каждым треугольником связан ряд так называемых замечательных точек или центров. Когда треугольник "вращается" между описанной и вписанной окружностями, эти точки движутся по каким-то кривым. В следующих задачах требуется найти соответствующие траектории.

3. Какую траекторию описывает

а) точка пересечения медиан M ;

б) ортоцентр H ;

в) точка Жергонна G (точка пересечения отрезков, соединяющих вершины треугольника и точки касания противоположных сторон с вписанной окружностью)

г) точка Лемуана L , изогонально сопряженная M .

треугольника Понселе?

4. Пусть A', B', C' — точки касания сторон треугольника Понселе с вписанной окружностью. Найдите траекторию центра тяжести M_0 треугольника $A'B'C'$.

5.* Дан треугольник Понселе и неподвижная точка P . Найдите траекторию точки, изогонально сопряженной P .

6. Докажите, что для фиксированной точки X на Ω , ее прямая Симсона относительно треугольника Понселе проходит через фиксированную точку Y (причем, прямая ℓ , проходящая через Y перпендикулярно XU , касается ω).

7. Полуописанной окружностью треугольника ABC называется окружность, касающаяся сторон AC, BC и описанной окружности треугольника

а) Найдите траекторию центра полуописанной окружности.

¹будем употреблять этот термин, хотя на самом деле в теореме Понселе возникает не многоугольник а замкнутая ломаная, возможно, самопересекающаяся

б) Докажите, что полувписанная окружность треугольника Понселе все время касается, помимо Ω , еще одной окружности.

с) Докажите аналогичное утверждение про окружности, проходящие через две вершины треугольника Понселе и касающиеся ω .

8*. Пусть дан треугольник ABC и точка X . Прямые AX , BX , CX пересекают BC , CA , AB соответственно в точках A' , B' , C' . Тогда точки пересечения прямых $A'B'$ и AB , $B'C'$ и BC , $C'A'$ и CA лежат на одной прямой, которая называется *трилинейной полярной* X относительно ABC .

а) Докажите, что трилинейная полярная фиксированной точки X на Ω относительно треугольника Понселе проходит через фиксированную точку Y .

б) Найдите ГМТ $Y(X)$

9. Окружность с центром I лежит внутри другой окружности. Найдите геометрическое место центров описанных окружностей треугольников IAB , где AB — хорда внешней окружности, касающаяся внутренней.

10. Даны две окружности, одна из которых лежит внутри другой. Найдите геометрическое место центров вписанных окружностей треугольников ABC , где AC и BC — хорды внешней окружности, касающиеся внутренней.

11. Две окружности радиуса 1 пересекаются в двух точках, расстояние между которыми также равно 1. Из точки C одной окружности проведены ко второй касательные CA и CB , вторично пересекающие первую окружность в точках B' и A' . Найдите расстояние AA' .

12. Дана окружность и точка P внутри нее. Рассмотрим пары перпендикулярных лучей с началом P , пересекающих окружность в точках A и B .

а) Найдите геометрическое место середин отрезков AB .

б) Найдите геометрическое место точек пересечения касательных к окружности в точках A и B .

13. Докажите теорему Понселе для $n = 4$.

14. Пусть две окружности с центрами O , I и радиусами R , r удовлетворяют теореме Понселе для $n = 4$. Выведите соотношение, связывающее величины R , r и $d = OI$.

15.

а) Докажите, что диагонали всех вписанно-описанных четырехугольников с данными вписанной и описанной окружностями пересекаются в одной точке P , лежащей на прямой OI .

б) Вывести соотношение, связывающее OP , R и d .

16. Докажите, что прямые, соединяющие точки касания противоположных сторон вписанно-описанного четырехугольника с вписанной окружностью, являются биссектрисами углов между его диагоналями.

17. Найдите траекторию центра тяжести M четырехугольника.

18*. Докажите, что в четырехугольнике Понселе

а) произведение тангенсов углов, образованных диагоналями с прямой OI ;

б) произведение длин диагоналей постоянно.

2 Теорема Понселе с алгебраической точки зрения

При $n > 4$ теорему Понселе также можно доказать геометрически. Но дальнейшее изучение многоугольников Понселе чисто геометрическими методами представляется затруднительным. Более эффективными оказываются средства алгебраической геометрии. Для начала покажем, как с помощью этих средств получить доказательство теоремы Понселе.

Введем на плоскости систему координат, начало которой совпадает с центром описанной окружности, а ось абсцисс - с линией центров. Пусть R, r — радиусы соответственно описанной и вписанной окружностей, d - расстояние между их центрами, так что центр вписанной окружности имеет координаты $(d, 0)$. Координаты точек большой окружности можно задать формулами $x = R(1 - t^2)/(1 + t^2), y = R \cdot 2t/(1 + t^2)$, причем соответствие между точками окружности и значениями t будет взаимнооднозначным, если считать, что точке $(-R, 0)$ соответствует $t = \infty$. Такой способ задания кривой называется ее рациональной параметризацией. Пусть t_0, t_1, \dots, t_{n-1} — значения параметра t , соответствующие вершинам многоугольника.

19.

а) Выведите соотношение, связывающее t_0 и t_1 .

б) Выведите соотношение, связывающее t_0 и t_2 .

с*) Докажите, что t_0 и t_n связаны соотношением $P_n(t_0, t_n) = 0$, где $P_n(x, y)$ — некоторый симметричный многочлен от двух переменных, степень которого по каждой переменной равна 2.

20. Докажите теорему Понселе.

Обобщенная теорема Понселе. Пусть внутри окружности Ω лежат окружности $\omega_1, \dots, \omega_n$, причем все эти окружности соосны, т.е. имеют общую радикальную ось. Если существует вписанный в Ω многоугольник $A_1 \dots A_n$ такой, что $A_1 A_2$ касается ω_1 , $A_2 A_3$ касается $\omega_2, \dots, A_n A_1$ касается ω_n , то существует бесконечно много таких многоугольников.

21.

а) Докажите обобщенную теорему Понселе.

б) Докажите "совсем обобщенную" теорему Понселе, в которой вместо соосных окружностей берутся коники, проходящие через четыре данных точки.

Из обобщенной теоремы Понселе следует, что, если $A_1 \dots A_n$ — многоугольник Понселе, вписанный в окружность Ω и описанный около окружности ω , то его диагонали $A_i A_{i+k}$ при фиксированном k касаются некоторой окружности, соосной с Ω и ω .

22. Пусть для многоугольника Понселе радиусы описанной и вписанной окружностей равны R и r , а расстояние между их центрами d . Найдите радиус окружности, касающейся диагоналей $A_i A_{i+2}$ и расстояние от ее центра до центра описанной окружности.

23. Выведите формулы, связывающие R, r и d для

а) шестиугольника;

б) восьмиугольника;

с) пятиугольника Понселе.

24. (С.Маркелов) Пусть R, r и d являются радиусами описанной и вписанной окружностей и расстоянием между их центрами для n -угольника Понселе. Докажите, что d, r и R также являются радиусами описанной и вписанной окружностей и расстоянием между их центрами для некоторого многоугольника Понселе, причем число его сторон равно либо n , либо $2n$, либо $n/2$.

25. Найдите траекторию

- а) центра тяжести вершин;
- б) центра тяжести точек касания вписанной окружности со сторонами многоугольника Понселе.

26. Даны центры описанной и вписанной окружностей и центр тяжести вершин вписанного описанного n -угольника. Можно ли восстановить этот n -угольник с помощью циркуля и линейки при

- а) $n = 3$?
- б) $n = 4$?

27.

а) Пусть t_1, \dots, t_n — значения параметра, соответствующие вершинам A_1, \dots, A_n n -угольника Понселе; $\sigma_1 = t_1 + \dots + t_n$, $\sigma_2 = t_1 t_2 + t_1 t_3 + \dots + t_{n-1} t_n, \dots, \sigma_n = t_1 \dots t_n$ — симметрические многочлены Виета от t_1, \dots, t_n . Докажите, что все четные многочлены Виета постоянны, а нечетные пропорциональны друг другу.

б) Пусть d_1, \dots, d_n — длины касательных из вершин A_1, \dots, A_n n -угольника Понселе к его вписанной окружности; $\sigma_1 = d_1 + \dots + d_n$, $\sigma_2 = d_1 d_2 + d_1 d_3 + \dots + d_{n-1} d_n, \dots, \sigma_n = d_1 \dots d_n$ — симметрические многочлены Виета от d_1, \dots, d_n . Докажите, что все четные многочлены Виета постоянны, а нечетные пропорциональны друг другу.

28*. Даны две окружности, одна из которых лежит внутри другой. Рассматриваются ломаные $A_1 A_2 \dots A_{n+1}$, вершины которых лежат на внешней окружности, а звенья касаются внутренней. Найдите геометрическое место центров тяжести точек касания.

29*. Определим прямую Симсона точки X относительно вписанного n -угольника по индукции как прямую, на которой лежат основания перпендикуляров из X на все прямые Симсона $(n - 1)$ -угольников, полученных выкидыванием каждой из вершин. Докажите, что для фиксированной точки X на Ω ее прямые Симсона относительно многоугольника Понселе проходят через фиксированную точку.

30. Пусть треугольник ABC вписан в окружность Ω радиуса 1, а прямые AB, BC, CA касаются окружностей $\omega_1, \omega_2, \omega_3$, причем все эти окружности соосны. а расстояния от центров $\omega_1, \omega_2, \omega_3$ до центра Ω равны d_1, d_2, d_3 . Выведите соотношение между d_1, d_2, d_3 .

3 Другие теоремы замыкания

Теорема Понселе является одним из примеров так называемых теорем замыкания. Приведем еще несколько примеров таких теорем.

Поризм Штейнера. Даны две окружности: α и лежащая внутри нее β . Рассмотрим цепочку окружностей $\omega_1, \omega_2, \dots$, касающихся α внутренним и β внешним образом, таких, что ω_{i+1} касается ω_i . Если при некотором выборе окружности ω_1 окружность ω_n ее касается, то это выполнено и при любой другой окружности ω_1 .

Теорема о зигзаге. Даны две окружности: α и β . Возьмем произвольную точку A_0 на α и найдем на β такую точку B_0 , что $A_0 B_0 = 1$. Затем найдем на α отличную от A_0 точку A_1 такую, что $A_1 B_0 = 1$ и т.д. Если точка A_n совпадает с A_0 , то это же верно и для любой другой точки A_0 .

Отметим, что теорема о зигзаге верна даже для окружностей, не лежащих в одной плоскости.

Теорема Эмха. Даны три окружности: α , лежащая внутри нее β и лежащая внутри β γ . Рассмотрим цепочку окружностей $\omega_1, \omega_2, \dots$, касающихся α внутренним и γ внешним образом, таких, что ω_{i+1} и ω_i пересекаются в точке, лежащей на β . Если при некотором

выборе окружности ω_1 окружность ω_n ее касается, то это выполнено и при любой другой окружности ω_1 .

Теорема о ломаной Брокара. Даны окружность ω , точка P внутри нее и угол ϕ . Для произвольной точки X_0 на ω построим такую точку X_1 , что $\angle PX_0X_1 = \phi$. Аналогично по точке X_1 построим точку X_2 и т.д. Если для некоторой точки X_0 $X_n = X_0$, то это верно и для любой другой точки X_0 .

Теорема Протасова. Пусть S_0, S_1, S_2 — три сферы в пространстве, центры которых не лежат на одной прямой. Рассмотрим семейство Σ сфер, касающихся S_1 и S_2 (сферы из Σ касаются каждой из сфер S_1, S_2 одинаковым образом — внутренним или внешним) и перпендикулярных S_0 . Пусть ω — окружность в пространстве, не лежащая ни на какой сфере из Σ и не проходящая через точки, принадлежащие более, чем двум сферам из Σ . Для произвольной точки X_0 на ω возьмем проходящую через нее сферу $s_1 \in \Sigma$ и найдем вторую точку X_1 пересечения s_1 с ω . Возьмем отличную от s_1 сферу $s_2 \in \Sigma$, проходящую через X_1 и найдем вторую точку X_2 ее пересечения с ω и т.д. Если для некоторой точки X_0 $X_n = X_0$, то это верно и для любой другой точки X_0 .

31. Докажите эти теоремы алгебраически.

Любая окружность на плоскости задается уравнением вида $x^2 + y^2 + ax + by + c = 0$. Поставим в соответствие такой окружности точку пространства с координатами (a, b, c) .

32. Является ли это соответствие взаимнооднозначным?

33. Какие пары точек соответствуют двум касающимся окружностям?

34. Какие утверждения получаются при этом соответствии из теорем Штейнера и Эмха?

35. Выведите

а) Теорему Эмха и теорему о ломаной Брокара из теоремы Понселе.

б) Теорему Понселе, поризм Штейнера и теорему о зигзаге из теоремы Эмха.

36. Докажите теорему Протасова.

37. Выведите из теоремы Протасова теорему о зигзаге, теоремы Понселе и Эмха, поризм Штейнера.

Литература

1. Заславский А.А., Челноков Г.Р. Теорема Понселе в евклидовой и алгебраической геометрии. Математическое образование. 2001. N 4(19).

2. Заславский А., Косов Д., Музафаров М. Траектории замечательных точек треугольника Понселе. Квант. 2003. N 2.

3. Акопян А.В., Заславский А.А. Геометрические свойства кривых второго порядка. М.: МЦНМО, 2007.

4. V.Yu. Protasov. Generalized closing theorems. Elem.Math. 66 (2011) p.98–117.

Вокруг теоремы Понселе Решения.

1 Теорема Понселе для $n = 3, 4$

1. Проведем прямую через I и вершину C треугольника ABC и найдем вторую точку C' пересечения этой прямой с описанной около ABC окружностью (рис.1).

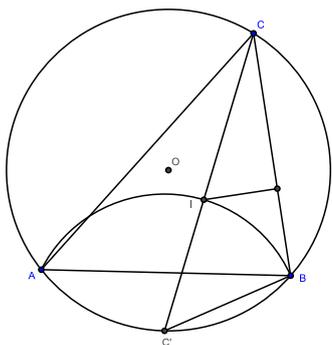


Рис.1

Так как $C'A = C'B$, $\angle AIB = \pi - (\angle A + \angle B)/2 = (\pi + \angle C)/2$ и $\angle AC'B = \pi - \angle C$, C' — центр окружности, описанной около треугольника AIB . Значит, $IC' = C'B = 2R \sin \frac{\angle C}{2}$. С другой стороны, $IC = r / \sin \frac{\angle C}{2}$, следовательно

$$R^2 - OI^2 = CI \cdot C'I = 2Rr.$$

2. Пусть дан треугольник ABC . Из произвольной точки C' на его описанной окружности проведем касательные к вписанной окружности треугольника и найдем вторые точки A' , B' их пересечения с описанной окружностью. Надо показать, что прямая $A'B'$ также касается вписанной окружности.

Предположим противное. Например, пусть $A'B'$ не пересекает вписанной окружности треугольника ABC . Будем увеличивать угол $A'C'B'$, так чтобы прямая $C'I$ оставалась его биссектрисой. Тогда расстояние от I до прямых $C'A'$ и $C'B'$ будет увеличиваться, а до прямой $A'B'$ — уменьшаться, и в какой-то момент окружность с центром I и радиусом $r' > r$ окажется вписанной в треугольник $A'B'C'$. Но из формулы Эйлера следует, что радиусы вписанных окружностей треугольников ABC и $A'B'C'$ равны — противоречие. Случай, когда $A'B'$ пересекает вписанную окружность, рассматривается аналогично.

3. Проще всего воспользоваться **теоремой Фейербаха**, утверждающей, что окружность Эйлера, проходящая через середины A_0, B_0, C_0 треугольника ABC , касается его вписанной окружности. Из нее следует, что центр этой окружности, совпадающий с серединой отрезка OH , лежит на окружности с центром I и радиусом $R/2 - r$. Значит, точки M и N лежат на образах этой окружности при гомотетиях с центром O и коэффициентами $2/3$ и 2 , соответственно.

Точка Жергонна также движется по окружности, причем эта окружность соосна с описанной и вписанной окружностями треугольника. Однако, простое геометрическое доказательство этого факта пока получить не удалось.

Точка Лемуана движется по эллипсу, малая ось которого лежит на прямой OI . Простое геометрическое доказательство этого факта также неизвестно.

4. Пусть A'', B'', C'' — вторые точки пересечения высот треугольника $A'B'C'$ с вписанной окружностью ABC . Тогда $A''A', B''B', C''C'$ — биссектрисы углов $A''B''C''$, т.е. ортоцентр H' треугольника $A'B'C'$ совпадает с центром вписанной окружности $A''B''C''$. Кроме того, нетрудно проверить, что стороны $A''B''C''$ параллельны соответствующим сторонам ABC , и значит эти треугольники гомотетичны. При этой гомотетии O переходит в I , а I — в H' , следовательно, H' лежит на прямой OI и $IH'/OI = r/R$. Поэтому при вращении треугольника H' , а значит и делящий отрезок $H'I$ в отношении $2 : 1$ центр тяжести $A'B'C'$ остается неподвижным.

5. **Ответ.** Пусть P' — точка, инверсная P относительно описанной окружности треугольника. Рассмотрим поворотную гомотетию с центром P' , переводящую P в I , и найдем образ Q точки I при этой гомотетии. Искомая траектория — окружность с центром Q (рис.2). Это можно доказать, используя комплексные числа. Геометрическое доказательство неизвестно.

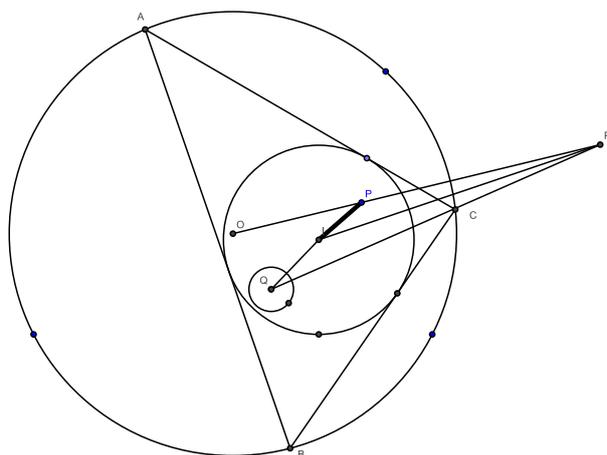


Рис.2

6. **Указание.** Прямая Симсона делит пополам отрезок между соответствующей точкой и ортоцентром H треугольника. Параллельная ей прямая, проходящая через H , вторично пересекает окружность, по которой движется H , в фиксированной точке (рис.3).

Пусть $Q_{AB} = AB \cap T_A T_B$, $Q_{BC} = BC \cap T_B T_C$. Заметим, что $Q_{AB} Q_{BC}$ — полярная T относительно Γ . Так как $T \in IO$, получаем, что $Q_{AB} Q_{BC} \perp IO$.

Пусть M_{AB}, M_{BC} — середины дуг AB, BC ; P_{AB} — точка пересечения $T_A T_B$ с касательной к Γ в точке M_{AB} . Аналогично определим P_{BC} .

Радикальная ось $l(\omega_A, \omega_B)$ проходит через M_{AB} и точку пересечения касательных к Γ в точках T_A и T_B . Поэтому P_{AB} — полюс $l(\omega_A, \omega_B)$ относительно Γ . Аналогично P_{BC} — полюс радикальной оси $l(\omega_B, \omega_C)$ относительно Γ . Теперь $P_{AB} P_{BC}$ — полярная радикального центра L относительно Γ . Чтобы убедиться, что $L \in IO$, осталось показать, что $P_A P_C \parallel Q_A Q_C$.

Пусть X_{AB}, X_{BC} — точки касания ω_B с AB и BC . Заметим, что T_B, X_{AB}, M_{AB} лежат на одной прямой, T_B, X_{BC}, M_{BC} также лежат на одной прямой, и $\frac{T_B X_{BC}}{T_B M_{BC}} = \frac{T_B X_{AB}}{T_B M_{AB}}$, так как гомотетия с центром T_B переводит ω_B в Γ .

Получаем $\frac{T_B Q_{BC}}{T_B P_{BC}} = \frac{T_B X_{BC}}{T_B M_{BC}} = \frac{T_B X_{AB}}{T_B M_{AB}} = \frac{T_B Q_{AB}}{T_B P_{AB}}$, что завершает доказательство.

Рассмотрев симметричную относительно OI конфигурацию, получаем, что $\vec{OL} = \frac{2Rr}{R^2 - d^2 - r^2} \vec{OI}$, где $d = OI$.

б) Из предыдущего пункта получаем, что все полувыписанные окружности касаются, помимо окружности с центром O еще одной окружности с центром в другом фокусе эллипса.

в) **Указание.** Геометрическим местом центров таких окружностей является эллипс с фокусами O и I .

8. **Указание.** Трилинейная полярная точки описанной окружности проходит через точку Лемуана L и вторично пересекает эллипс, по которому движется L в фиксированной точке (рис.4).

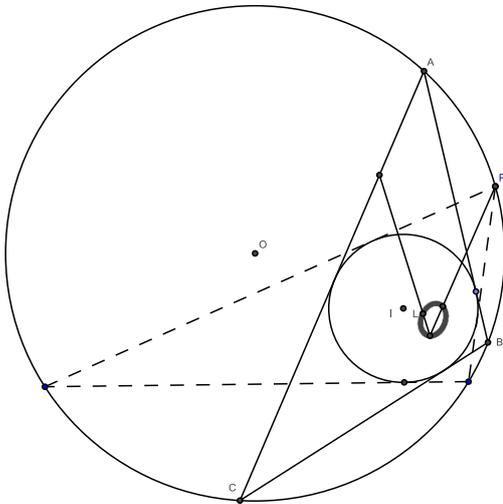


Рис.4

9. Пусть R, r — радиусы большей и меньшей окружностей, O — центр большей окружности, O' — центр описанной окружности треугольника ABI . Из условия следует, что O и O' лежат на серединном перпендикуляре к плоскости AB .

Дважды применим теорему косинусов — к треугольникам $AO'O$ и $OO'I$:

$$R^2 = O'A^2 + O'O^2 - 2O'A \cdot O'O \cos \angle AO'O$$

$$OI^2 = O'I^2 + O'O^2 - 2O'I \cdot O'O \cos \angle IO'O.$$

Вычитая из первого равенства второе, получим:

$$R^2 - OI^2 = 2O'O(O'A \cos \angle AO'O - O'I \cos \angle IO'O) = 2O'O \cdot r.$$

Следовательно, искомое ГМТ — окружность с центром O и радиусом $(R^2 - OI^2)/2r$.

Другое решение. Зафиксируем внешнюю окружность Γ (с центром O и радиусом R), и центр I внутренней окружности γ (ее радиус r может меняться). Пусть $A, B, C \in \Gamma$ таковы, что AB и BC касаются γ . Пусть S и R — центры описанных окружностей треугольников AIB , BIC соответственно. Мы имеем $OS \perp AB$, $OR \perp BC$ и $SR \perp IB$ (так как SR — серединный перпендикуляр к IB). Поскольку $\angle(AB, BI) = \angle(IB, BC)$, получаем, что $\angle(OS, SR) = \angle(SR, RO)$, hence $OS = OR$.

Пусть $X, Y \in \Gamma$ и XY касается γ так, что $\angle(\vec{IX}, \vec{IY}) < \pi$. Определим отображение $g_r : \Gamma \rightarrow \Gamma$ так, что $g_r(X) = Y$. Пусть $S_r(X)$ — центр описанной окружности треугольника $XI g_r(X)$, а $OS_r(X) = \rho_r(X)$. Заметим, что $\rho_r(X)$ непрерывно зависит от (X, r) .

Докажем, что $\rho_r(X) = \rho_r(g_r(X))$. Отсюда будет следовать, что $\rho_r(X)$ не зависит от X .

Назовем r *регулярным* если орбита $\{X, g_r(X), g_r^2(X), \dots\}$ плотна в Γ . Для каждого регулярного r получаем, что $\rho_r(X)$ не зависит от X . Если r_0 не регулярно (случай траектории Понселе), представим $\rho_{r_0}(X) = \lim_{r \rightarrow r_0} \rho_r(X)$, где r регулярны. Тогда $\rho_r(X)$ не зависит от X при всех r .

Рассмотрев симметричную относительно OI конфигурацию, получим, что $\rho_r(X) = \frac{R^2 - d^2}{2r}$, где $d = OI$.

10. Пусть O, D — центры внешней и внутренней окружностей; R, r — их радиусы; A', B', C' — середины дуг BC, CA, AB ; I — центр вписанной окружности треугольника ABC . Тогда в треугольнике $A'B'C'$ I будет ортоцентром, а значит, $\vec{OI} = \vec{OA'} + \vec{OB'} + \vec{OC'}$. Следовательно, вектор $C'I$ лежит на прямой CD , а его длина равна $2R \sin \angle OA'B' = 2Rr/CD$. С другой стороны, $C'D = (R^2 - OD^2)/CD$, так что отношение $C'I/C'D$ не зависит от точки C . Но тогда и отношение DI/DC' не зависит от C , т.е. точка I лежит на окружности, гомотетичной внешней относительно D .

Другое решение. Зафиксируем внешнюю окружность Γ (с центром O и радиусом R), и центр I внутренней окружности γ (ее радиус r может меняться). Пусть $A, B, C \in \Gamma$ таковы, что AB, AC, BD касаются γ . Пусть AI и BI вторично пересекают Γ в точках A' и B' соответственно. Пусть S и R — центры вписанных окружностей треугольников ABC, ABD соответственно. Мы имеем $B'R/B'I = B'A/B'I = \lambda = A'B/A'I = A'S/A'I$. Значит S и R лежат на образе Γ при гомотетии с центром I и коэффициентом $1 - \lambda$.

Рассмотрев частый случай, найдем λ .

Теперь решение аналогично предыдущей задаче.

11. Пусть O — центр окружности, на которой лежит точка C , O' — центр другой окружности. Так как $OO' = \sqrt{3}$, прямая $A'B'$ касается второй окружности в точке C' . Следовательно, $\angle A'O'A = \angle AO'C' + \frac{1}{2} \angle C'O'B = 2\angle ABC' + \angle C'AB = \angle CB'A + \frac{1}{2} \angle CA'B'$, $\angle O'A'O = \angle O'A'B' + \angle B'A'O = \frac{\pi}{2} - \angle C'O'A + \frac{\pi}{2} - \angle BCA = \pi - \angle BCA - \frac{1}{2} \angle CA'B' = \angle CB'A + \frac{1}{2} \angle CA'B'$. Так как $O'A = OA'$, $AO'A'O$ — равнобокая трапеция, и $AA' = OO' = \sqrt{3}$.

12. Пусть C — четвертая вершина прямоугольника $PACB$. Так как $OP^2 + OC^2 = OA^2 + OB^2$, C описывает окружность с центром O . Значит, середина отрезка AB описывает окружность, центром которой является середина OP , и инверсная к ней точка пересечения касательных также описывает окружность.

13. **Указание.** Докажите, что отрезки, соединяющие точки касания противоположных сторон четырехугольника с вписанной окружностью, взаимно перпендикулярны, и воспользуйтесь предыдущей задачей.

14. **Ответ.**

$$\frac{1}{r^2} = \frac{1}{(R+d)^2} + \frac{1}{(R-d)^2}.$$

15. **Ответ.**

$$\frac{R+OP}{R-OP} = \frac{(R+d)^2}{(R-d)^2}.$$

16. Из формулы предыдущей задачи нетрудно получить, что P — предельная точка пучка, порожденного описанной и вписанной окружностями четырехугольника. Поэтому для любой точки X описанной окружности отношение расстояния XP к касательной из X к вписанной окружности будет одним и тем же. Утверждение задачи следует из этого факта и того, что прямые, соединяющие точки касания противоположных сторон описанного четырехугольника с вписанной окружностью, проходят через точку пересечения диагоналей.

17. Точка M — середина отрезка между серединами диагоналей четырехугольника. Используя тот факт, что прямая, соединяющая середины диагоналей описанного четырехугольника, проходит через центр вписанной окружности, нетрудно вывести, что траектория M — окружность.

18.

а) Пусть U, V — середины диагоналей. Так как U, V лежат на окружности с диаметром OP , а прямая UV проходит через I , получаем

$$\operatorname{tg}\angle UPO \operatorname{tg}\angle VPO = \frac{UO \cdot VO}{UP \cdot VP} = \frac{S_{OUV}}{S_{PUV}} = \frac{OI}{IP} = \sqrt{\frac{R^2}{R^2 - OP^2}}.$$

б) **Указание.** Длины диагоналей равны $2\sqrt{R^2 - OP^2 \sin^2 \angle UPO}$ и $2\sqrt{R^2 - OP^2 \sin^2 \angle VPO}$. Отсюда с учетом предыдущего пункта получаем, что произведение диагоналей равно $4R\sqrt{R^2 - OP^2}$.

2 Теорема Понселе с алгебраической точки зрения

19.

а) Напишем уравнение прямой A_0A_1 и используем, что расстояние от точки $(d, 0)$ до этой прямой равно r . В результате получим

$$((R + d)^2 - r^2)t_0^2t_1^2 - r^2(t_0^2 + t_1^2) + 2(R^2 - d^2)t_0t_1 + ((R - d)^2 - r^2) = 0$$

б) **Указание.** Обозначим многочлен из предыдущего пункта через P_1 . Исключив t_1 из системы $P_1(t_0, t_1) = 0$, $P_1(t_1, t_2) = 0$, получим многочлен от t_0, t_2 , степень которого по каждой переменной равна 4. Разделив его на $(t_0 - t_2)^2$, получим искомое соотношение.

с) Действуя аналогично предыдущему пункту, по индукции получим искомое утверждение.

20. Пусть, начав из некоторой точки t_0 , мы на n -ном шаге вернулись в нее. Это означает, что выполнена следующая система уравнений: $P_n(t_0, t_n) = 0$, $t_0 = t_n$. Подставив второе уравнение в первое, получаем уравнение степени, не выше 4 от одной переменной, t_0 является его корнем. Однако очевидно, что также его корнями являются также t_1, t_2, \dots и т. д. Однако если у полиномиального уравнения корней больше, чем его степень, то оно тождественно равно нулю, и все числа являются его корнями, что при $n \geq 5$ доказывает теорему Понселе.

21. **Указание.** Пусть хорды A_0A_1 и A_1A_2 касаются двух окружностей пучка. Написав соответствующие уравнения для параметров и исключив из них t_1 , получим многочлен от t_0, t_2 , степень которого по каждой переменной равна 4. Этот многочлен разлагается в произведение двух множителей, каждый из которых соответствует некоторой окружности пучка. Следовательно, A_0A_2 касается одной из двух окружностей, в зависимости от того, как выбирались исходные касательные. Дальнейшие рассуждения аналогичны предыдущей задаче.

22. Введем обозначения $x_i = r_i/(R + d_i)$, $y_i = r_i/(R - d_i)$, где r_1, r_2 — радиусы окружностей, касающихся сторон и диагоналей, d_1, d_2 — расстояния от их центров до центра описанной окружности. Рассмотрев многоугольники, симметричные относительно линии центров, нетрудно получить соотношения

$$x_1 = (x_2^2 + y_2^2 - 1)/(1 - x_2^2 + y_2^2), \quad y_1 = (x_2^2 + y_2^2 - 1)/(1 + x_2^2 - y_2^2) \quad (1).$$

решив эту систему относительно x_2, y_2 , получим:

$$x_2 = \sqrt{(x_1(1 + y_1)/(x_1 + y_1))}, \quad y_2 = \sqrt{(y_1(1 + x_1)/(x_1 + y_1))} \quad (2)$$

23.

а) Для $n = 3$ имеем формулу Эйлера: $1/r = 1/(R + d) + 1/(R - d)$, т.е. $x + y = 1$ или в параметрической форме $x = \sin^2 t$, $y = \cos^2 t$, $0 < t < \pi/4$. Для $n = 6$ из (2) получаем $x = \sin t \cdot \sqrt{1 + \cos^2 t}$, $y = \cos t \cdot \sqrt{1 + \sin^2 t}$.

б) $x = \sqrt{\frac{\sin t \cdot (1 + \cos t)}{(\sin t + \cos t)}}, \quad y = \sqrt{\frac{\cos t \cdot (1 + \sin t)}{(\sin t + \cos t)}}.$

с) Определив величины x_i, y_i и рассуждая, как при выводе формулы (1), получим:

$$x_2 = (x_1^2 + y_1^2 - 1)/(1 - x_1^2 + y_1^2), \quad y_2 = (x_1^2 + y_1^2 - 1)/(1 + x_1^2 - y_1^2)$$

$$x_1 = (1 - x_2^2 - y_2^2)/(1 - x_2^2 + y_2^2), \quad y_1 = (1 - x_2^2 - y_2^2)/(1 + x_2^2 - y_2^2)$$

Решив вторую пару уравнений относительно x_2, y_2 , приравняв два выражения для x_2 , возведя в квадрат и избавившись от знаменателя, получим (индекс 1 можно отбросить)

$$x(1-y)(1-x^2+y^2)^2 - (x+y)(x^2+y^2-1)^2 = 0$$

Непосредственная проверка показывает, что это уравнение обращается в тождество при $x = -1, y = 0, x + y = 1$. Разделив на соответствующие множители, получим искомое соотношение:

$$(x+y-1)(x+y+1)^2 = 4xy(x+y)$$

24. При замене R на d и наоборот определенная выше величина x остается неизменной, а y меняет знак. Легко видеть, что, если пара (x, y) удовлетворяет условию замыкания на n -м шаге, то $(x, -y)$ удовлетворяет условию замыкания на $2n$ -м, т.е. через какое-то число шагов k , являющееся делителем $2n$, ломаная замыкается. В силу симметричности этого утверждения k может равняться только $n/2, n$ или $2n$.

25.

а) Пусть внешняя окружность рационально параметризована и t_0, t_1, t_{-1}, \dots – значения параметров, соответствующих вершинам многоугольника. Тогда из уравнения, связывающего t_0 и t_i по теореме Виета найдем $t_i + t_{-i}$ и $t_i * t_{-i}$. Затем выразим через t_0 суммы координат соответствующих вершин и, просуммировав по i , найдем координаты центра тяжести. Они будут иметь вид $x = P(t_0)/Q(t_0), y = R(t_0)/S(t_0)$.

Утверждение 1. $S = Q$ и $\deg Q = 2n$. В самом деле, знаменатель рациональной функции определяется ее полюсами, центр тяжести уходит на бесконечность только если одна из точек n -угольника попала в одну из 2 бесконечных точек окружности. То есть Q и S имеют корни именно в этих $2n$ точках.

Теперь, выбрав параметризацию, добьемся, чтобы при t_0 , стремящемся к бесконечности центр тяжести на бесконечность не уезжал. Если картинка действительная, то и выбирать нечего – любая параметризация с действительными коэффициентами подходит. Отсюда степени P и R не больше степени Q . Теперь посмотрим, в скольких точках наша кривая может пересекаться с произвольной прямой. Подставив в уравнение прямой рациональные функции степени $2n$ получим уравнение степени $2n$ на t_0 , у него $2n$ корней, но каждой точке кривой соответствуют n значений параметра, значит точек на кривой две. (вариант рассуждения: функции степени $2n$ с совпадающими знаменателями параметризуют кривую степени $2n$, но кривая взята с кратностью n (мы нашу окружность на нее n раз намотали), посему степень 2) Итак, наша кривая с каждой прямой пересекается по 2 точкам, то есть она 2 порядка. Теперь посмотрим, где она пересекает бесконечно удаленную. Если $n - 1$ точка стремятся к конечному пределу, а одна – к бесконечному, то центр тяжести едет на бесконечность в том же направлении. Итак, наша коника пересекает бесконечно удаленную прямую в тех же 2 точках, в которых ее пересекает любая окружность, а значит и она – окружность.

б) Если центр тяжести точек касания движется, то его траектория должна пересекать бесконечно удаленную прямую. Очевидно, это может происходить только тогда, когда на бесконечность уходит одна из точек касания. Но в бесконечно удаленных точках вписанная и описанная окружности пересекаются, следовательно, для того чтобы точка касания, например стороны A_1A_2 с вписанной окружностью, ушла на бесконечность, в ту же точку должен уходить один из концов этой стороны, например A_1 , а значит, и точка касания с вписанной окружностью стороны A_1A_n . При этом обе точки касания движутся на бесконечность в противоположных направлениях, и поведение центра тяжести определяется поведением середины соединяющего их отрезка.

Воспользуемся теперь тем, что середина отрезка, соединяющего точки касания двух прямых с окружностью, является образом при инверсии относительно этой окружности точки пересечения этих прямых. Введя стандартную параметризацию описанной окружности и используя хорошо известные формулы для инверсии, нетрудно убедиться, что когда точка A_1 стремится к бесконечности, ее инверсный образ стремится к некоторому конечному пределу. Таким образом, центр тяжести точек касания не уходит на бесконечность и, следовательно, остается неподвижным.

26.

а) Нет. Пусть t_a, t_b, t_c — значения параметра, соответствующие вершинам A, B, C треугольника. Координаты центра тяжести являются функциями параметра t_a , и условие попадания центра тяжести в данную точку дает уравнение относительно t_a . Поскольку t_b, t_c также являются корнями этого уравнения, его степень равна 3. Но кубическое уравнение с помощью циркуля и линейки решить нельзя.

б) Да. Центр тяжести M лежит на окружности, противоположными точками которой являются I и середина отрезка OP . Поэтому, перпендикуляр из M к прямой MI пересекает OI в середине OP , т.е. мы можем найти точку пересечения диагоналей P и определить радиусы описанной и вписанной окружностей. Далее, прямая MI пересекает окружность с диаметром OP в серединах диагоналей, что позволяет восстановить вершины четырехугольника.

27.

а) Очевидно, что, например, t_0 и t_1 связаны соответствием, которое алгебраично, симметрично и взаимнодвузначно. Поэтому все многочлены Виета можно выразить через t_0 . Так как все эти функции обращаются в бесконечность в одних и тех же точках, любые две из них связаны линейным соотношением, т.е. каждый из многочленов Виета является линейной функцией σ_1 . При этом четные многочлены являются четными функциями, а нечетные — нечетными, откуда и следует утверждение задачи.

28. Легко видеть, что верна следующая

Лемма. Даны три соосных окружности. Из произвольной точки C на одной из них проведены касательные CA, CB к двум другим. Точка D делит отрезок AB в фиксированном отношении. Тогда ГМТ D — окружность, соосная с данными.

Теперь утверждение задачи доказывается по индукции.

29.

30. Очевидно, что соотношение между d_1, d_2, d_3 является симметричным и имеет степень 2 по каждой переменной. Поэтому его можно записать в виде $P(\sigma_1, \sigma_2, \sigma_3) = 0$, где P — многочлен второй степени, а $\sigma_1, \sigma_2, \sigma_3$ — многочлены Виета от d_1, d_2, d_3 . Далее, если одна из трех коник совпадает с внешней, то две другие совпадают друг с другом, поэтому при $d_3 = 0$ $P = (d_1 - d_2)^2$, т.е., с учетом симметричности $P = \sigma_3(a\sigma_3 + b\sigma_2 + c\sigma_1 + d) + \sigma_1^2 - 4\sigma_2$. Если подставить сюда $d_1 = d_2 = d_3 = t$, то получим уравнение относительно t 6 степени. Два из его корней равны нулю, а 4 остальных можно найти, исключая r из следующей системы: $t^2 = 1 - 2r$ (формула Эйлера для треугольника) $l^2 - 1 = (l - t)^2 - r^2$ (условие соосности), где l — абсцисса точки пересечения линии центров и радикальной оси.

В результате получаем

$$P = (\sigma_3 - \sigma_1)^2 + 8l\sigma_3 - 4\sigma_2$$

Литература

1. Заславский А.А., Челноков Г.Р. Теорема Понселе в евклидовой и алгебраической геометрии. Математическое образование. 2001. N 4(19).

2. Заславский А., Косов Д., Музафаров М. Траектории замечательных точек треугольника Понселе. Квант. 2003. N 2.
3. Акопян А.В., Заславский А.А. Геометрические свойства кривых второго порядка. М.: МЦНМО, 2011.
4. V.Yu. Protasov. Generalized closing theorems. Elem.Math. 66 (2011) p.98–117.

On the Poncelet theorem

G.Chelnokov, E.Diomidov, V.Kalashnikov, P.Kozhevnikov, A.Zaslavsky

The simplest formulation of the Poncelet theorem is next.

Poncelet theorem. Let two circles be given, and one of them lies inside the second one. A tangent from an arbitrary point A_0 of the external circle Ω to the internal circle ω meets Ω for the second time at point A_1 . Similarly from point A_1 construct point A_2 etc. Then if $A_0 = A_n$ for some point A_0 , this will be true for any other point of Ω .

Not formally an inscribed and circumscribed polygon¹ can be "rotated" between two circles (its form can change during this rotation). We will call such "rotating" polygon a *Poncelet polygon*.

This project purposes to prove the Poncelet theorem and to examine some properties of Poncelet polygons. Also we consider the generalizations of Poncelet theorem and some similar theorems.

1 Poncelet theorem for $n = 3, 4$

1. Let O, I be the circumcenter and the incenter of the triangle, and R, r be the radii of the circumcircle and the incircle respectively. Prove **the Euler formula**

$$OI^2 = R^2 - 2Rr.$$

2. Prove the Poncelet theorem for $n = 3$.

A set of remarkable points or centers is associated with any triangle. When we "rotate" a triangle between its circumcircle and incircle, these points move on some curves. In the next problems we have to find the corresponding trajectories.

3. Find the trajectory of

a) the centroid M ;

b) the orthocenter H ;

c*) the Gergonne point G (the common point of the segments between the vertices of the triangle and the touching points of the opposite sides with the incircle)

d*) the Lemoine point L , isogonally conjugated to M of the Poncelet triangle?

4. Let A', B', C' be the touching points of the incircle with the sides. Find the trajectory of the centroid M_0 of triangle $A'B'C'$.

5*. Let a Poncelet triangle and a fixed point P be given. Find the trajectory of the point isogonally conjugated to P .

6. Let X be a fixed point of Ω . Prove that its Simson line passes through a fixed point Y (and line ℓ , passing through Y and perpendicular to XY , touches ω).

7. A circle touching sides AC, BC and the circumcircle of triangle ABC is called *semi-inscribed* circle of this triangle.

a) Find the trajectory of the center of the semi-inscribed circle.

b) Prove that the semi-inscribed circle of the Poncelet triangle touches some circle distinct from Ω .

c) Prove the same assertion for the circle, passing through two vertices of the Poncelet triangle and touching ω .

¹we will use this term in place of closed broken line, which may be self-intersecting

8* Let triangle ABC and point X be given. Lines AX , BX , CX meet BC , CA , AB respectively at points A' , B' , C' . Then the common points of lines $A'B'$ and AB , $B'C'$ and BC , $C'A'$ and CA are collinear on the line which is called a *trypolar* of X wrt ABC .

a) Prove that the trypolar of a fixed point X of Ω wrt the Poncelet triangle passes through a fixed point Y .

b) Find a locus of points $Y(X)$.

9. A circle with center I lies inside an other circle. Find the locus of the circumcenters of triangles IAB , where AB is an arbitrary chord of the external circle touching the internal one.

10. Let two circles be given and one of them lies inside the second one. Find the locus of the incenters of triangles ABC , where AC and BC are two chords of the external circle touching the internal one.

11. Two circles with radii 1 meet at two point, and the distance between these points also is equal to 1. C is an arbitrary point on one of these circles, the tangents CA and CB to the second circle meet the first circle for the second time at points B' and A' . Find the distance AA' .

12. Let a circle and a point P inside it be given. Two perpendicular rays with origin P meet the circle at points A and B .

a) Find the locus of the midpoints of segments AB .

b) Find the locus of the common points of the tangents to the circle at points A and B .

13. Prove the Poncelet theorem for $n = 4$.

14. Let two circles with centers O , I and radii R , r satisfy the Poncelet theorem for $n = 4$. Find the relation between R , r and $d = OI$.

15.

a) Prove that the diagonals of the Poncelet quadrilateral meet on the same point P , lying on OI .

b) Find the relation between OP , R and d .

16. Prove that the lines joining the touching points of the opposite sides of the Poncelet quadrilateral with the incircle are the bisectors of the angles formed by its diagonals.

17. Find the trajectory of the centroid M of the Poncelet quadrilateral.

18* Prove that

a) the product of the tangents of the angles between line OI and the diagonals;

b) the product of the lengths of the diagonals of the Poncelet quadrilateral is constant.

2 An algebraic view on the Poncelet theorem

When $n > 4$ the Poncelet theorem also can be proved synthetically. By the examination of the properties of the Poncelet polygons using only geometric methods is difficult. The methods of algebraic geometry are more effective. Firstly prove the Poncelet theorem using these methods.

Consider center O of Ω as an origin of a coordinates system and line OI as an abscissa axis. Let R, r — be the radii of the circles, and d be the distance between its centers, i.e. I has the coordinates $(d, 0)$. Define the coordinates of the points of Ω as $x = R(1 - t^2)/(1 + t^2), y = R \cdot 2t/(1 + t^2)$, this concordance between the points of Ω and the significances of t will be one-one, if point $(-R, 0)$ correspond to $t = \infty$. Such defining of a curve is called its rational parametrization. Let t_0, t_1, \dots, t_{n-1} be the significances of t , corresponding to the vertices of the polygon.

19.

- a) Find the relation between t_0 and t_1 .
- b) Find the relation between t_0 and t_2 .
- c*) Prove that t_0 and t_n satisfy to the relation $P_n(t_0, t_n) = 0$, where $P_n(x, y)$ is some symmetric polynomial, having degree 2 on each variable.

20. Prove the Poncelet theorem.

The general Poncelet theorem. Let circles $\omega_1, \dots, \omega_n$ lie inside circle Ω , and let all these circles be coaxial, i.e they have a common radical axis. If there exists a polygon $A_1 \dots A_n$ inscribed into Ω and such that A_1A_2 touches ω_1, A_2A_3 touches ω_2, \dots, A_nA_1 touches ω_n , then there exists an infinite set of such polygons.

21.

- a) Prove the general Poncelet theorem.
- b) Prove "the generallest" Poncelet theorem, in which the coaxial circles are replaced by the conics passing through four fixed points.

>From the general Poncelet theorem we obtain that if $A_1 \dots A_n$ is the Poncelet polygon inscribed into circle Ω and circumscribed around circle ω , then its diagonals A_iA_{i+k} for any fixed k touche the same circle coaxial with Ω and ω .

22. Let R and r be the radii of the circumcircle and the incircle of the Poncelet polygon, and d be the distance between its centers. Find the radius of the circle touching the diagonals A_iA_{i+2} and the distance from the center of this circle to the circumcenter.

23. Find the relations between R, r and d for the Poncelet

- a) hexagon;
- b) octagon;
- c) pentagon.

24. (S.Markelov) Let R, r and d be the radii of the circumcircle and the incircle of the Poncelet n -gon and the distance between its centers. Prove that d, r and R are also the radii of the circumcircle an the incircle and th distance between its centers for some Poncelet polygon, having $n, 2n$, or $n/2$ sides.

25. Find the trajectory

- a) the centroid of the vertices;
- b) the centroid of the touching points of the incircle with the sides of the Poncelet polygon.

26. Let an incenter, a circumcenter and a centroid of an inscribed and circumscribed n -gon be given. Can this n -gon be restored by a compass and a ruler if

- a) $n = 3$?
 b) $n = 4$?
 27.

a) Let t_1, \dots, t_n be the values of the parameter corresponding to the vertices A_1, \dots, A_n of a Poncelet n -gon; let $\sigma_1 = t_1 + \dots + t_n$, $\sigma_2 = t_1 t_2 + t_1 t_3 + \dots + t_{n-1} t_n, \dots, \sigma_n = t_1 \dots t_n$ be the Vieta polynomials from t_1, \dots, t_n . Prove that all even Vieta polynomials are constant and all odd polynomials are proportional to σ_1 .

b) Let d_1, \dots, d_n be the lengths of the tangents from the vertices A_1, \dots, A_n of a Poncelet n -gon to its incircle; let $\sigma_1 = d_1 + \dots + d_n$, $\sigma_2 = d_1 d_2 + d_1 d_3 + \dots + d_{n-1} d_n, \dots, \sigma_n = d_1 \dots d_n$ be the Vieta polynomials from d_1, \dots, d_n . Prove that all even Vieta polynomials are constant and all odd polynomials are proportional to σ_1 .

28*: Let two circles be given one of them lying inside the other. Consider a broken line $A_1 A_2 \dots A_{n+1}$, with the vertices lying on the external circle, and the links touching the internal one. Find the locus of the centroids of the touching points.

29*: Define the Simson line of point X wrt a cyclic n -gon using the induction as the line containing the projections of X to the Simson lines of X wrt $(n-1)$ -gons, obtaining by deleting of each vertex. Prove that the Simson line of a fixed point of Ω wrt the Poncelet polygon passes through a fixed point.

30. Let triangle ABC be inscribed into circle Ω with radius 1, and let lines AB, BC, CA touch circles $\omega_1, \omega_2, \omega_3$, in such a way that all these circles are coaxial. Find the relation between the distances d_1, d_2, d_3 from the centers of $\omega_1, \omega_2, \omega_3$ to the center of Ω .

3 The other closing theorems

The Poncelet theorem is the example of a closing theorem. Take some other examples of such theorems.

The Steiner porism. Let two circles be given: α and lying inside it β . Consider a chain of circles $\omega_1, \omega_2, \dots$, touching α internally, touching β externally, and such that ω_{i+1} touches ω_i . If for some circle ω_1 circle ω_n touches ω_1 , then this is true for any ω_1 .

The zigzag theorem. Let two circles α and β be given. Take an arbitrary point A_0 on α and find such point B_0 on β that $A_0 B_0 = 1$. Now find point A_1 on α distinct from A_0 and such that $A_1 B_0 = 1$ etc. If A_n coincides with A_0 , then this is true for any other point A_0 .

Note that the zigzag theorem is correct even for two circles not lying in the same plane.

The Emch theorem. Let three circles be given: α, β lying inside α and γ lying inside β . Consider a chain of circles $\omega_1, \omega_2, \dots$, touching α internally, touching γ externally, and such that ω_{i+1} and ω_i meet at the point lying on β . If for some ω_1 circle ω_n touches ω_1 , then this is true for any ω_1 .

The Brocard broken line theorem. Let a circle ω , a point P inside it and an angle ϕ be given. For an arbitrary point X_0 of ω construct such point X_1 , that $\angle P X_0 X_1 = \phi$. Similarly for point X_1 construct X_2 etc. If for some X_0 $X_n = X_0$, then this is true for any X_0 .

The Protasov theorem. Let S_0, S_1, S_2 be three spheres with non-collinear centers. Consider a family Σ of spheres touching S_1 and S_2 (the spheres of Σ touch each of spheres S_1, S_2 by the same way — internally or externally) and perpendicular to S_0 . Let ω — be a circle in the space, which do not lie on any sphere from Σ and do not pass through the common points of many than two spheres of Σ . For an arbitrary point X_0 on ω take a sphere $s_1 \in \Sigma$ passing through it and find the second common point X_1 of s_1 and ω . Take a sphere $s_2 \in \Sigma$ distinct

from s_1 and passing through X_1 and find its second common point X_2 with ω etc. If for some X_0 $X_n = X_0$, then this is true for any X_0 .

31. Prove these theorems algebraically.

An arbitrary circle on the plane can be given by an equation $x^2 + y^2 + ax + by + c = 0$. Correspond to such circle a point in the space with coordinates (a, b, c) .

32. Is this a one-one correspondence?

33. Which pairs of points correspond to touching circles?

34. Which assertions correspond to the Steiner and Emch theorems?

35. Obtain

a) the Emch theorem and the Brocard broken line theorem from the Poncelet theorem;

b) the Poncelet theorem, the zigzag theorem and the Steiner porism from the Emch theorem.

36. Find the Protasov theorem

37. Obtain the zigzag theorem, the Poncelet theorem, the Emch theorem and the Steiner porism from the Protasov theorem.

On the Poncelet theorem Solutions.

1 Poncelet theorem for $n = 3, 4$

1. Let the line joining I with vertex C of triangle ABC meet for the second time the circumcircle of ABC at point C' (fig.1).

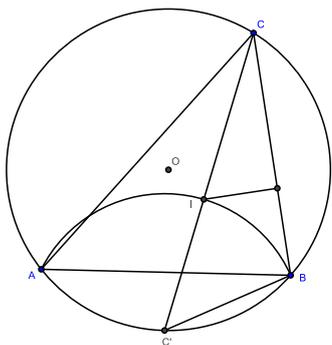


Fig.1

Since $C'A = C'B$, $\angle AIB = \pi - (\angle A + \angle B)/2 = (\pi + \angle C)/2$ and $\angle AC'B = \pi - \angle C$, we obtain that C' is the circumcenter of triangle AIB . Thus $IC' = C'B = 2R \sin \frac{\angle C}{2}$. On the other hand $IC = r / \sin \frac{\angle C}{2}$, therefore

$$R^2 - OI^2 = CI \cdot C'I = 2Rr.$$

2. Let a triangle ABC be given. Take the tangents from an arbitrary point C' of its circumcircle to its incircle and find their common points A', B' with the circumcircle distinct from C' . We have to prove that line $A'B'$ also touches the incircle.

Suppose the opposite. For example let $A'B'$ do not intersect the incircle of ABC . Increase angle $A'C'B'$ in such a way that line $C'I$ stays its bisector. Then the distances from I to lines $C'A'$ and $C'B'$ will increase, and the distance from I to $A'B'$ will decrease, thus sometimes a circle with center I and radius $r' > r$ will be the incircle of triangle $A'B'C'$. But by Euler formula the inradii of triangles ABC and $A'B'C'$ are equal — contradiction. The case when $A'B'$ intersect the incircle can be considered similarly.

3. By the **Feuerbach theorem**, the Euler circle passing through the midpoints A_0, B_0, C_0 of the sides of triangle ABC touches its incircle. From this the center of this circle coinciding with the midpoint of OH lie on the circle with center I and radius $R/2 - r$. Thus the trajectories of points M and H are homothetic to this circle with center O and coefficients $2/3$ and 2 respectively.

The trajectory of the Gergonne point is a circle coaxial with the circumcircle and the incircle. Synthetic proof of this fact is unknown.

The trajectory of the Lemoine point is an ellipse with the minor axis lying on OI . Synthetic proof of this fact is also unknown.

4. Let A'', B'', C'' be the second common points of the altitudes of $A'B'C'$ with the incircle of ABC . Then $A''A', B''B', C''C'$ are the bisectors of triangle $A''B''C''$, i.e. the orthocenter H' of triangle $A'B'C'$ coincides with the incenter of $A''B''C''$. Also it is easy to see that the sidelines of $A''B''C''$ are parallel to the corresponding sidelines of ABC , thus these triangles are homothetic. This homothety maps O and I to I to H' respectively, therefore H' lies on OI and $IH'/OI = r/R$. When the triangle rotates H' and the centroid of $A'B'C'$ dividing $H'I$ in ratio $2 : 1$ are immobile.

5. **Answer.** Let P' be the point inverse to P wrt the circumcircle. Consider a rotational homothety with center P' , transforming P to I and find the image Q of I . The desired trajectory is a circle with center Q (fig.2). This can be proved using the complex numbers. Synthetic proof is unknown.

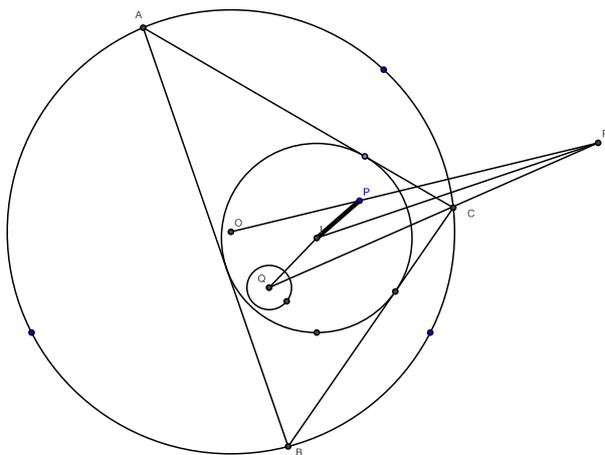


Fig.2

6. **Hint.** The Simson line bisects the segment between the corresponding point and the orthocenter H треугольника. The parallel line passing through H , meets for the second time the trajectory of H at a fixed point (fig.3).

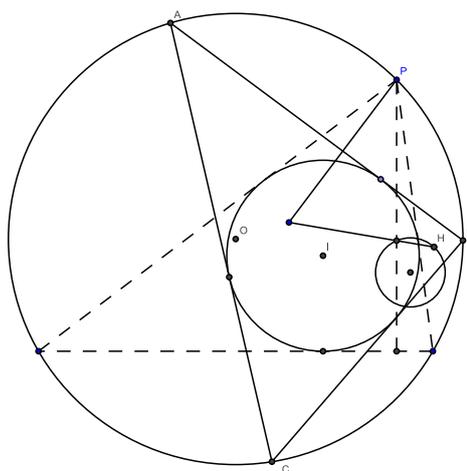


Fig.3

7.

a) Prove general assertion.

Let two circles one lying inside the other be given. From an arbitrary point X of the external circle draw the tangents to the internal one and inscribe to the obtained angle a circle touching the external circle. Then the locus of the centers of such circles is an ellipse having the center of the external circle as a focus.

Proof. Let O, I be the centers of the given circles, and let Y be a touching point. Then all chords XY meet OI at the same point — the homothety center H of the given circles. Since the center Z of the semi-inscribed circle is the common point of lines OY and IX , its trajectory is an ellipse. To prove that O is its focus consider a polar map wrt the circle with center O . It transforms I, H to a parallel lines i, h , also it transforms X, Y to the tangents x, y meeting at some point P of line h . Let U, V be the common point of x and y with i , and let Q be the vertex of parallelogram $PUQV$. Then Q lies on the line symmetric h about i . Since PQ is the fourth harmonic line to x, y, h , it meet the perpendicular from O to h at the fixed point — the pole of h . Using the homothety with the center in this point we obtain that all lines QU, QV (i.e. the polars of points Z) touches the same circle.

Alternative solution. It is sufficient to prove that all semiinscribed circles have common radical center L . Suppose this is true, and all semiinscribed circles have power equal to p wrt L . Then they all touch the image of Γ under inversion with center L and radius $\sqrt{|p|}$ followed by the symmetry in L , for $p < 0$.

Let us fix the outer circle Γ (let O be its center, and R be its radius), and the center I of the inner circle γ (let r be its radius, further r could vary). Let $Z, A, B, C, D \in \Gamma$ so that ZA, AB, BC, CD touch γ . Let $\omega_A, \omega_B, \omega_C$ be semiinscribed circles of triangles ZAB, ABC, BCD opposite to A, B, C , and touching Γ at T_A, T_B, T_C , respectively. We will prove that the radical center L of $\omega_A, \omega_B, \omega_C$ belongs to IO (we use the proof of Stoyan Boyev, he applied it for the case of three semiinscribed circles of a triangle). By the jump argument it is sufficient to conclude that all the circles from the family of semiinscribed circles have common radical center L .

Firstly, we will consider the homothety h taking the γ to Γ . According to the Monge's theorem we can easily find that lines AT_A, BT_B and CT_C are concurrent and their intersection point T is the center of homothety h . Hence T, I and O are collinear points.

Let $Q_{AB} = AB \cap T_A T_B, Q_{BC} = BC \cap T_B T_C$. Note that $Q_{AB} Q_{BC}$ is the polar line of point T wrt Γ . Since $T \in IO$, we have $Q_{AB} Q_{BC} \perp IO$.

Let M_{AB}, M_{BC} be the midpoints of arcs AB, BC (take arcs opposite to I). Let P_{AB} is the common point of $T_A T_B$ and the tangent to Γ at M_{AB} . P_{BC} defined similarly.

The radical axis $l(\omega_A, \omega_B)$ passes through M_{AB} and the common point of tangents to Γ through T_A and T_B . Hence P_{AB} is the pole of $l(\omega_A, \omega_B)$ wrt Γ . Similarly, and P_{BC} is the pole of the radical axis $l(\omega_B, \omega_C)$ wrt Γ . Thus $P_{AB} P_{BC}$ is the polar of the radical center L wrt Γ . To prove that $L \in IO$ it remains to prove that $P_A P_C \parallel Q_A Q_C$.

Let X_{AB}, X_{BC} be touching points of ω_B with AB and BC . Note that T_B, X_{AB}, M_{AB} are collinear, T_B, X_{BC}, M_{BC} are collinear, and $\frac{T_B X_{BC}}{T_B M_{BC}} = \frac{T_B X_{AB}}{T_B M_{AB}}$ from homothety with center T_B taking ω_B to Γ . We have $\frac{T_B Q_{BC}}{T_B P_{BC}} = \frac{T_B X_{BC}}{T_B M_{BC}} = \frac{T_B X_{AB}}{T_B M_{AB}} = \frac{T_B Q_{AB}}{T_B P_{AB}}$, and this completes the proof.

Considering a particular case with symmetry in OI , we obtain $\vec{OL} = \frac{2Rr}{R^2 - d^2 - r^2} \vec{OI}$, where $d = OI$.

b) From previous result we obtain that all semi-inscribed circles touche the circle with center O and another circle with the center in the remaining focus of the ellipse.

c) **Hint.** The locus of the centers of such circles is an ellipse with foci O and I .

8. **Hint.** The tryptolar passes through the Lemoine point L and meets for the second time the trajectory of L at a fixed point (fig.4).

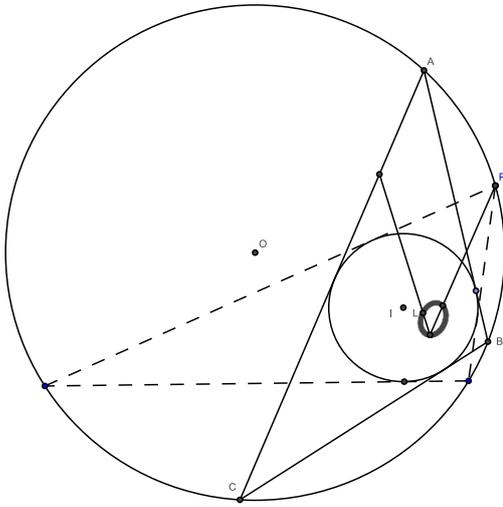


Fig.4

9. Let R, r be the radii of the given circles, let O be the center of the external circle, and O' be the circumcenter of triangle ABI . We have that O and O' lie on the perpendicular bisector to segment AB .

Use the cosines theorem to triangles $AO'O$ and $OO'I$:

$$R^2 = O'A^2 + O'O^2 - 2O'A \cdot O'O \cos \angle AO'O$$

$$OI^2 = O'I^2 + O'O^2 - 2O'I \cdot O'O \cos \angle IO'O.$$

Subtracting the second equality from the first one we obtain:

$$R^2 - OI^2 = 2O'O(O'A \cos \angle AO'O - O'I \cos \angle IO'O) = 2O'O \cdot r.$$

Therefore the desired locus is the circle with center O and radius $(R^2 - OI^2)/2r$.

Alternative solution. Let us fix the outer circle Γ (let O be its center, and R be its radius), and the center I of the inner circle γ (let r be its radius, further r could vary). Let $A, B, C \in \Gamma$ so that AB and BC touch γ . Let S and R be circumcenters of triangles AIB, BIC , respectively. We have $OS \perp AB, OR \perp BC$, and $SR \perp IB$ (since SR is the perpendicular bisector of IB). Since $\angle(AB, BI) = \angle(IB, BC)$, we have $\angle(OS, SR) = \angle(SR, RO)$, hence $OS = OR$.

Let $X, Y \in \Gamma$, and XY touches γ so that $\angle(\vec{IX}, \vec{IY}) < \pi$. Define the map $g_r : \Gamma \rightarrow \Gamma$ such that $g_r(X) = Y$. Let $S_r(X)$ be the circumcenter of triangle $XI g_r(X)$, and $OS_r(X) = \rho_r(X)$. Note that $\rho_r(X)$ is continuous over (X, r) .

We have proved that $\rho_r(X) = \rho_r(g_r(X))$ (we made a jump). From this jump we will derive that $\rho_r(X)$ is independent of X .

Let us call r *regular* if the orbit $\{X, g_r(X), g_r^2(X), \dots\}$ is dense in Γ . For each regular r we obtain that $\rho_r(X)$ is independent of X . If r_0 is not regular (there are closed Poincaré trajectories), then take a limit $\rho_{r_0}(X) = \lim_{r \rightarrow r_0} \rho_r(X)$ over regular r . Thus we get that $\rho_r(X)$ is independent of X for all r .

Considering a particular case with symmetry in OI , one can easily obtain $\rho_r(X) = \frac{R^2-d^2}{2r}$, where $d = OI$.

10. Let O, D be the centers of the given circles, and let R, r be their radii; let A', B', C' be the midpoints of arcs BC, CA, AB , and I be the incenter of ABC . Then I is the orthocenter of triangle $A'B'C'$, thus $\vec{OI} = \vec{OA'} + \vec{OB'} + \vec{OC'}$. Therefore vector $C'I$ lies on CD , and its length is equal to $2R \sin \angle OA'B' = 2Rr/CD$. On the other hand $C'D = (R^2 - OD^2)/CD$, i.e. the ratio $C'I/C'D$ do not depend on C . Thus DI/DC' also do not depend on C , i.e. I lies on the circle homothetic to the given external circle with center D .

Alternative solution. Let us fix the outer circle Γ (let O be its center, and R be its radius), and the center I of the inner circle γ (let r be its radius, further r could vary). Let $A, B, C \in \Gamma$ so that AB, AC, BD touch γ . Let AI and BI intersect Γ for the second time at A' and B' , respectively. Let S and R be incenters triangles ABC, ABD , respectively. We have $B'R/B'I = B'A/B'I = \lambda = A'B/A'I = A'S/A'I$. Hence S and R lie on the image of Γ under homothety with center I and ratio $1 - \lambda$.

Considering special case one can calculate λ .

We have made a jump. From this solution follows similarly to Problem 9.

11. Let O be the center of the circle containing point C , and O' be the center of the remaining circle. Since $OO' = \sqrt{3}$, we obtain that $A'B'$ touches the second circle at some point C' . Therefore $\angle A'O'A = \angle AO'C' + \frac{1}{2}\angle C'O'B = 2\angle ABC' + \angle C'AB = \angle CB'A' + \frac{1}{2}\angle CA'B'$, $\angle O'A'O = \angle O'A'B' + \angle B'A'O = \frac{\pi}{2} - \angle C'O'A' + \frac{\pi}{2} - \angle BCA = \pi - \angle BCA - \frac{1}{2}\angle CA'B' = \angle CB'A' + \frac{1}{2}\angle CA'B'$. Since $O'A = OA'$, we obtain that $AO'A'O$ is an isosceles trapezoid, and $AA' = OO' = \sqrt{3}$.

12. Let C be the fourth vertex of rectangle $PACB$. Since $OP^2 + OC^2 = OA^2 + OB^2$, C lies on the circle with center O . Thus the midpoint of AB lies on the circle having the center at the midpoint of OP , and the inverse common point of the tangents also lies on a circle.

13. **Hint.** Prove that the segments joining the touching points of the incircle with the opposite sides are perpendicular and use the previous problem.

14. **Answer.**

$$\frac{1}{r^2} = \frac{1}{(R+d)^2} + \frac{1}{(R-d)^2}.$$

15. **Answer.**

$$\frac{R+OP}{R-OP} = \frac{(R+d)^2}{(R-d)^2}.$$

16. Using the formula of the previous problem we obtain that P is the limit point of the pencil containing the incircle and the circumcircle. Thus for any point X of the circumcircle the ratio of distance XP and the length of the tangent from X to the incircle is the same. From this fact using that the lines joining the opposite touching points pass through P we obtain the assertion of the problem.

17. Point M is the midpoint of the segment between the midpoints of the diagonals. Since the midpoints of the diagonals and the incenter are collinear it is easy to see that the trajectory of M is a circle.

18.

a) Let U, V be the midpoints of the diagonals. Since U, V lie on the circle with diameter OP , and line UV passes through I , we have

$$\operatorname{tg}\angle UPO \operatorname{tg}\angle VPO = \frac{UO \cdot VO}{UP \cdot VP} = \frac{S_{OUV}}{S_{PUV}} = \frac{OI}{IP} = \sqrt{\frac{R^2}{R^2 - OP^2}}.$$

b) **Hint.** The lengths of the diagonals are $2\sqrt{R^2 - OP^2 \sin^2 \angle UPO}$ and $2\sqrt{R^2 - OP^2 \sin^2 \angle VPO}$. From this and previous equality we obtain that the product of the diagonals is equal to $4R\sqrt{R^2 - OP^2}$.

2 An algebraic view on the Poncelet theorem

19.

a) Write an equation of line A_0A_1 and use that the distance from point $(d, 0)$ to this line is equal to r . We obtain

$$((R + d)^2 - r^2)t_0^2t_1^2 - r^2(t_0^2 + t_1^2) + 2(R^2 - d^2)t_0t_1 + ((R - d)^2 - r^2) = 0$$

b) **Hint.** Denote the above polynomial as P_1 . Excluding t_1 from the system $P_1(t_0, t_1) = 0$, $P_1(t_1, t_2) = 0$, we obtain the polynomial from t_0, t_2 , having degree 4 on each variable. Dividing it to $(t_0 - t_2)^2$, we obtain the desired relation.

c) The desired assertion can be obtained by induction similarly as the previous result.

20. Let starting from some point t_0 we return to it through n steps. Then we have: $P_n(t_0, t_n) = 0$, $t_0 = t_n$. Substituting the second equation to the first one we obtain the equation of degree 4 such that t_0 is its root. It is evident that t_1, t_2, \dots are also its roots. Since the number of roots of this equation is greater than its degree we obtain that it is an identity when $n \geq 5$. That proves the Poncelet theorem.

21. **Hint.** Let chords A_0A_1 and A_1A_2 touche two circles of the given pencil. Writing the corresponding equations and excluding t_1 we obtain a polynomial from t_0, t_2 having degree 4 on each variable. This polynomial can be decomposed to two multipliers each of them corresponding to some circle of the pencil. Therefore A_0A_2 touches one of these two circle depending on the choice of the tangents. Now we can reason similarly to the previous problem.

22. Denote $x_i = r_i/(R + d_i)$, $y_i = r_i/(R - d_i)$, where r_1, r_2 are the radii of the circles touching the sides and the diagonals respectively, and d_1, d_2 are the distances from their centers to the circumcenter. Considering the symmetric polygons we obtain

$$x_1 = (x_2^2 + y_2^2 - 1)/(1 - x_2^2 + y_2^2), \quad y_1 = (x_2^2 + y_2^2 - 1)/(1 + x_2^2 - y_2^2) \quad (1).$$

resolving this system wrt x_2, y_2 we obtain:

$$x_2 = \sqrt{(x_1(1 + y_1)/(x_1 + y_1))}, \quad y_2 = \sqrt{(y_1(1 + x_1)/(x_1 + y_1))} \quad (2)$$

23.

a) For $n = 3$ we have the Euler formula: $1/r = 1/(R + d) + 1/(R - d)$ i.e. $x + y = 1$ or $x = \sin^2 t$, $y = \cos^2 t$, $0 < t < \pi/4$. For $n = 6$ from (2) we obtain $x = \sin t \cdot \sqrt{1 + \cos^2 t}$, $y = \cos t \cdot \sqrt{1 + \sin^2 t}$.

b) $x = \sqrt{\frac{\sin t \cdot (1 + \cos t)}{(\sin t + \cos t)}}, y = \sqrt{\frac{\cos t \cdot (1 + \sin t)}{(\sin t + \cos t)}}.$

c) Define x_i, y_i and reason similarly to the conclusion of (1) we obtain:

$$\begin{aligned} x_2 &= (x_1^2 + y_1^2 - 1)/(1 - x_1^2 + y_1^2), & y_2 &= (x_1^2 + y_1^2 - 1)/(1 + x_1^2 - y_1^2) \\ x_1 &= (1 - x_2^2 - y_2^2)/(1 - x_2^2 + y_2^2), & y_1 &= (1 - x_2^2 - y_2^2)/(1 + x_2^2 - y_2^2) \end{aligned}$$

Resolving the second system wrt x_2, y_2 and comparing two expressions for x_2 we obtain (index 1 is ejected)

$$x(1 - y)(1 - x^2 + y^2)^2 - (x + y)(x^2 + y^2 - 1)^2 = 0$$

It is easy to see that this equation is identity when $x = -1, y = 0, x + y = 1$. Dividing to corresponding multipliers we obtain:

$$(x + y - 1)(x + y + 1)^2 = 4xy(x + y)$$

24. When we change R to d and vice versa defined above x do not change, and y change the sign. Since (x, y) satisfy the closing condition for the n -th step, we obtain that $(x, -y)$ satisfy the closing condition for the $2n$ -th step, i.e. the broken line close through k steps where k is some divisor of $2n$. Since this assertion is symmetric k may be equal only to $n/2$, n or $2n$.

25.

a) Let the external circle is rationally parametrized and t_0, t_1, t_{-1}, \dots are the parameters corresponding to the vertices of the polygon. Using the Vieta theorem from the relation between t_0 and t_i find $t_i + t_{-i}$ and $t_i * t_{-i}$. Now express through t_0 the sums of the coordinates of the corresponding vertices and summing for all i , find the coordinates of the centroid. Let they be $x = P(t_0)/Q(t_0)$, $y = R(t_0)/S(t_0)$.

Lemma 1. $S = Q$ and $\deg Q = 2n$. In fact, the denominator of a rational function is defined by its poles. The centroid is an infinite point iff one of the vertices of the n -gon coincide with one if two infinite points of the circle. Thus the roots of Q and S coincide with these $2n$ points.

Now choose parametrize the circle in such a way that the centroid does not tend to infinity when t_0 tends to infinity. Then the degrees of P and R are not greater than the degree of Q . Now count the common points of our curve with an arbitrary line. Substituting the rational functions with degrees $2n$ to the equation of the line we obtain an equation with degree $2n$ wrt t_0 , it has $2n$ roots but each point of the curve corresponds to n significances of the parameters, thus there exists two points on the curve.

So our curve meets any line at 2 points, thus its degree is 2. Now consider its infinite points. If $n - 1$ points of the circle tend to the finite point, and one point tends to the infinite point, then the enroid tends to the same infinite point. Therefore our conic meet the infinite line at 2 points lying on any circle, i.e. it is also a circle.

b) Suppose that the centroid is not a fixed point. Then its trajectory intersect the infinite line. This can happen only if one of touching points is infinite. But the circumcircle and the incircle meet at the infinite points. Therefore if for example the touching point of side A_1A_2 with the incircle is infinite then some endpoint of this side for example A_1 also is infinite. Thus the touching point of side A_1A_n is infinite. When A_1 tends to an infinite point two touching points move on the opposite directions and the trajectory of the centroid is defined by the midpoint of the corresponding segment.

Now use that the midpoint of the segment between two touching points is inverse to the common point of the corresponding tangents. It is easy to see that when A_1 tends to infinity, the inverse point tends to some finite point. Thus the centroid does not intersect the infinite line, therefore it is a fixed point.

26.

a) No. Let t_a, t_b, t_c be the significances of the parameter corresponding to the vertices A, B, C of the triangle. Expressing the coordinates of the centroid through t_a we obtain an equation wrt t_a . Since t_b, t_c are also the roots of this equation, its degree is equal to 3. But a cubic equation can not be solving by a compass and a ruler.

b) Yes. The centroid M lies on the circle having I and the midpoint of OP as opposite points. Thus the perpendicular from M to line MI meets OI at the midpoint of OP , i.e. we can find the common point P of the diagonals and calculate the radii of the circumcircle and the incircle. Now line MI meets the circle with diameter OP at the midpoints of the diagonals, which allows to restore the vertices of the quadrilateral.

27.

a) The relation between t_0 and t_1 is symmetric and has degree 2 wrt each variable. Thus we can express all Vieta polynomials through t_0 . All these functions have the same poles, therefore

each of them is a linear function of σ_1 . Since the odd polynomials are odd functions, and the even polynomials are even functions we obtain the desired assertion.

28. It is easy to prove next

Lemma. Let three coaxial circles be given. From an arbitrary point C on one of them take the tangents CA, CB to two remaining circles. Let point D divide segment AB in some fixed ratio. Then the locus of points D is the circle coaxial with the given circles.

Now the desired assertion can be obtained by induction.

29.

30. It is evident that the relation between d_1, d_2, d_3 is symmetric and has degree 2 on each variable. Thus we can write it as $P(\sigma_1, \sigma_2, \sigma_3) = 0$, where P is a polynomial with degree 2, and $\sigma_1, \sigma_2, \sigma_3$ are the Vieta polynomials from d_1, d_2, d_3 . If one of conics coincide with the external one then two remaining conics coincide i.e if $d_3 = 0$ then $P = (d_1 - d_2)^2$, therefore $P = \sigma_3(a\sigma_3 + b\sigma_2 + c\sigma_1 + d) + \sigma_1^2 - 4\sigma_2$. Substituting $d_1 = d_2 = d_3 = t$, we obtain an equation wrt t with degree 6. Two of its roots are equal to zero. Find 4 remaining roots excluding r from the system: $t^2 = 1 - 2r$ (Euler formula) $l^2 - 1 = (l - t)^2 - r^2$ (the condition of coaxility), where l is the abscissa of the common point of the center line and the radical axis.

As result we obtain

$$P = (\sigma_3 - \sigma_1)^2 + 8l\sigma_3 - 4\sigma_2$$

References

1. A.Akopyan, A.Zaslavsky. Geometry of Conics. American Mathematical Society, New York, 2007.
2. V.Yu.Protasov. Generalized closing theorems. Elem.Math. 66 (2011) p.98–117.

Инциденции точек и прямых.

Ф. Нилов, А. Полянский, Н. Полянский



Рис. 1: Пал Эрдёш

Жил-был дедушка Эрдёш. Придумывал он много задачек. Так вот однажды он загадал такую загадку.

Пусть на плоскости живет некоторое конечное множество прямых \mathcal{L} и некоторое конечное множество точек P . Тогда через $I(\mathcal{L}, P)$ будем обозначать количество инциденций между этими множествами, то есть число таких пар (l, p) , $l \in \mathcal{L}$, $p \in P$, что $p \in l$.

Обозначим за $I(n, m)$ максимальное значение $I(\mathcal{L}, P)$ среди всех таких пар (\mathcal{L}, P) , что $|\mathcal{L}| = n$, $|P| = m$, здесь и далее через $|A|$ обозначаем количество элементов в множестве A .

Вопрос: Получить точную оценку сверху для $I(n, m)$.

П. Эрдёш предположил: существует такая константа C , что

$$I(n, n) \leq C \left(n^{4/3} \right).$$

Очевидно, что эта оценка лучше тривиальной $I(n, n) \leq n^2$.

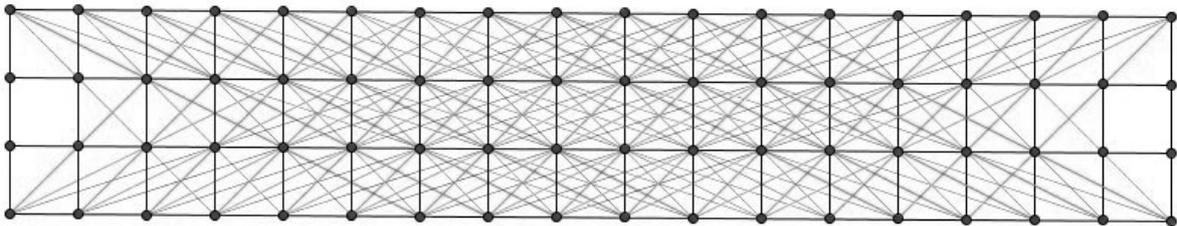


Рис. 2: Точки и прямые с большим числом инциденций

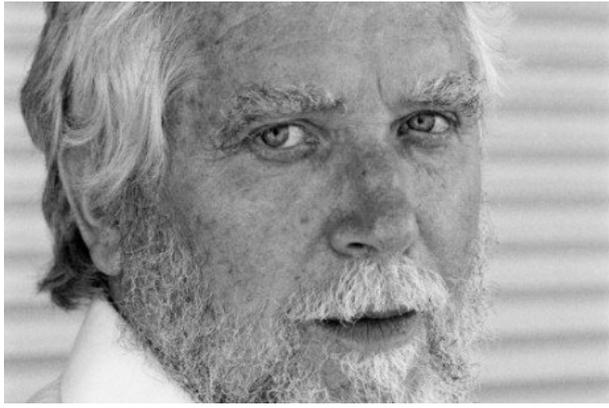


Рис. 3: Эндре Семереди



Рис. 4: Уильям Т. Троттер

В 1983 году два математика, Семереди и Троттер, доказали последнюю оценку. Этот факт известен как **теорема Семереди-Троттера**.

Наша основная цель — доказать эту теорему двумя способами. Попутно мы решим много интересных задач в геометрии и комбинаторике.

1 Комбинаторная часть

1.1 Введение. Комбинаторная геометрия

1.1. На плоскости расположено конечное количество точек. Докажите, что найдётся такая прямая, что в каждой из полуплоскостей, на которые она делит плоскость, будет не больше половины от всех точек (полуплоскость не содержит свою границу).

1.2. Пусть на плоскости дано $2n$ точек. Докажите, что их можно разделить на пары так, что отрезки, соответствующие парам, не будут пересекаться.

1.3. Дано n точек на плоскости, никакие три из которых не лежат на одной прямой. Между некоторыми из точек проведены отрезки. Назовём набор отрезков между точками *связным*, если между любыми двумя точками найдётся путь по отрезкам из этого набора. Построен такой связный набор Γ , что сумма длин отрезков в Γ не больше, чем в любом другом связном наборе. Докажите, что отрезки из Γ пересекаются только концами.

1.4. Пусть на плоскости даны n точек и n непараллельных прямых. Докажите, что можно пронумеровать точки и прямые числами от 1 до n так, чтобы отрезки перпендикуляров, опущенных из соответствующих точек на соответствующие прямые не пересекались.

1.5. Дан невыпуклый многоугольник $A_1A_2 \dots A_n$. Если несмежные вершины A_i и A_j многоугольника таковы, что он лежит целиком по одну сторону от прямой A_iA_j , то можно взять одну из двух ломаных, на которые точки A_i и A_j его разбивают, и отразить симметрично относительно центра отрезка A_iA_j . Докажите, что рано или поздно многоугольник станет выпуклым.

1.2 Инциденции множеств

1.6. Пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ – произвольная совокупность трёхэлементных подмножеств n -элементного множества, причём $|M_i \cap M_j| \neq 1$ для любых i, j . Найдите максимальное значение s , при котором это возможно.

1.7. Пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ – произвольная совокупность, состоящая из четырёхэлементных подмножеств n -элементного множества, причём $|M_i \cap M_j| \neq 2$ для любых i, j . Докажите, что максимальное s , при котором это возможно, лежит в пределах от $\lfloor n/4 \rfloor^2$ до $n(n-1)/4$.

Определение. Пусть $\mathcal{L} = \{l_1, \dots, l_n\}$ – произвольная совокупность подмножеств m -элементного множества $P = \{p_1, \dots, p_m\}$. Назовём пару (l_i, p_k) *инцидентом*, если $p_k \in l_i$. Тогда через $I(\mathcal{L}, P)$ будем обозначать число инцидентов, образованных элементами из \mathcal{L} и P , а через $I(n, m)$ максимальное значение $I(\mathcal{L}, P)$ по всем таким множествам \mathcal{L} и P , что $|\mathcal{L}| = n, |P| = m$.

Один из важных вопросов всего проекта состоит в том, чтобы оценить число инцидентов в случае, когда даны какие-то условия на множества. Если нет никаких условий на множества, то можем получить лишь тривиальную оценку $I(\mathcal{L}, P) \leq mn$.

Есть следующий способ воспринимать инциденты:

Рассмотрим пустую табличку, состоящую из n строчек и m столбцов. Строки будут соответствовать элементам множества $\{l_1, \dots, l_n\}$, а столбцы – элементы $\{p_1, \dots, p_m\}$. Тогда мы будем ставить на позицию, находящуюся на пересечении i -ой строчки, и j -го столбца, звездочку тогда и только тогда, когда $p_j \in l_i$. Вопрос о числе инцидентов можно теперь поставить так: сколько звездочек стоит в таблице?

Если вам это будет удобно, то переводите задачи на язык табличек (см. задачу **1.11.**).

В оставшихся задачах этого параграфа мы считаем, что $n, m, r \in \mathbb{N}$, $\mathcal{L} = \{l_1, \dots, l_n\}$ – произвольная совокупность подмножеств m -элементного множества $P = \{p_1, \dots, p_m\}$, причем $|l_i \cap l_j| \leq r$ для любых $i \neq j$.

1.8. Пусть $r = 1$. Докажите, что

а) $I(\mathcal{L}, P) \leq n^2 + m, I(\mathcal{L}, P) \leq m^2 + n$.

б) $I(\mathcal{L}, P) \leq \sqrt{m(n^2 - n)} + m, I(n, m) \leq \sqrt{n(m^2 - m)} + n$.

1.9. Докажите, что

$$I(\mathcal{L}, P) \leq \sqrt{mr(n^2 - n)} + m.$$

1.10. Пусть $r = 1$.

(a) Найдите $\max I(\mathcal{L}, P)$ при $n \leq 3$.

(b) Найдите $\max I(\mathcal{L}, P)$ при $m \geq C_n^2$. При каких условиях достигается этот максимум?

1.11. Квадрат 13×13 разбит на единичные квадратики. Центры некоторых из них отмечены так, что нет прямоугольника с вершинами в отмеченных точках и сторонами, параллельными сторонам квадрата. Найдите наибольшее возможное число отмеченных точек.

1.12. 100 (a) мышей вместе грызут 1000 (b) кусков сыра. Каждая мышь может попробовать несколько кусков сыра, сделав в каждом из них по одной дырке. Любые две мыши имеют дырки не более чем в 10 (c) общих кусках сыра. Докажите, что число дырок не больше $11000(b + a\sqrt{bc})$. Докажите, что число дырок не больше $10500 \left(\frac{b + \sqrt{b^2 + 4bca(a-1)}}{2} \right)$.

1.3 Теорема о сэндвиче.

1.13. Докажите, что если на плоскости даны красные и синие точки в общем положении, то найдётся прямая, которая будет делить плоскость на две такие полуплоскости, что в каждой из них будет находиться не более половины красных и не более половины синих точек.

1.14. Докажите, что если в пространстве \mathbb{R}^3 даны красные, синие и зелёные точки в общем положении, то найдётся плоскость, которая будет делить \mathbb{R}^3 на два такие полупространства, что в каждом из них будет находиться не более половины точек каждого цвета.

1.15. Пусть на плоскости дано $2m$ точек общего положения, из них m красных и m синих. Докажите, что их можно разделить на пары так, что точки в каждой паре разного цвета и отрезки, соответствующие парам, не будут пересекаться.

Будем обозначать прямую через $\mathbb{R} = \mathbb{R}^1$, плоскость — через \mathbb{R}^2 , а трёхмерное пространство — через \mathbb{R}^3 . Проще всего воспринимать эти объекты следующим образом: \mathbb{R} — это множество всевозможных вещественных (действительных) чисел, \mathbb{R}^2 — это множество всех пар $\mathbf{x} = (x_1, x_2)$ чисел $x_1, x_2 \in \mathbb{R}$, а \mathbb{R}^3 — множество всех троек $\mathbf{x} = (x_1, x_2, x_3)$, где $x_1, x_2, x_3 \in \mathbb{R}$. Аналогично определяется и \mathbb{R}^n . Элементами \mathbb{R}^n являются векторы (точки) $\mathbf{x} = (x_1, \dots, x_n)$, где $x_i \in \mathbb{R}$, $i = 1, \dots, n$ (x_i — координаты).

Пусть a_1, a_2, \dots, a_d — некоторые действительные числа, не равные одновременно нулю, а a_0 — произвольное действительное число. Назовём *гиперплоскостью* в пространстве \mathbb{R}^d множество таких точек \mathbf{x} , что
$$\sum_{i=1}^d a_i x_i = a_0,$$
 где (x_1, x_2, \dots, x_n) — координаты \mathbf{x} .

Контрольный вопрос. Что такое гиперплоскость в \mathbb{R}^2 и \mathbb{R}^3 ?

Теорема о сэндвиче. Множества $A_1, \dots, A_d \in \mathbb{R}^d$ — конечные. Тогда существует такая гиперплоскость l , что в каждом из полупространств, образованных данной гиперплоскостью, будет не более $\lfloor A_i/2 \rfloor$ точек из A_i (некоторые точки могли лежать в гиперплоскости).

Если в случае $d = 3$ заменить множества A_1, A_2, A_3 на хлеб, сыр и ветчину, то будет существовать такой разрез ножом (плоскость), что в каждом из полученных полупространств будет одинаковое количество каждого из ингредиентов.

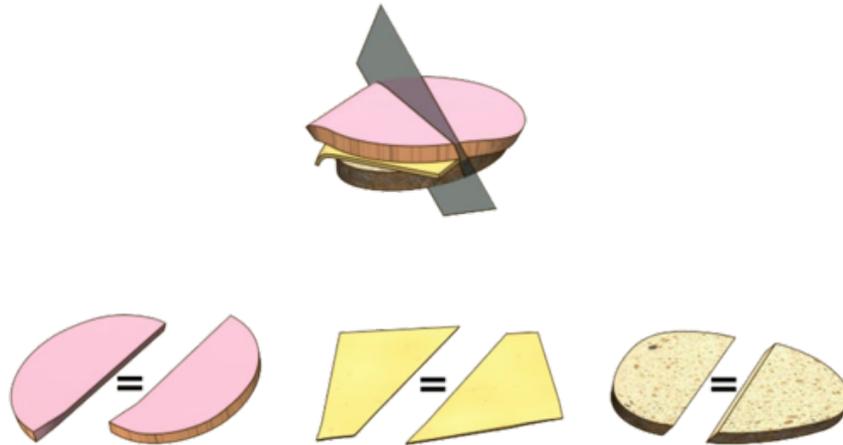


Рис. 5: Разрез сэндвича

1.16. Пусть в пространстве дано $3n$ точек общего положения, из них n красных, n синих и n зелёных. Докажите, что их можно разделить на тройки так, что точки в каждой тройке разного цвета и треугольники, соответствующие тройкам, не будут пересекаться.

1.17.* Два вора украли ожерелье с двумя концами, состоящее из платиновой цепочки, на которую нанизаны драгоценные камни d видов. Они не знают ценности каждого камня, поэтому хотят поделить камни каждого вида поровну (известно, что камней каждого вида четное количество). Чтобы потерять как можно меньше платины, воры хотят сделать наименьшее число разрезов. Могут ли они поделить ожерелье с помощью

- а) $(d - 1)$ разрезов?
- б) d разрезов?

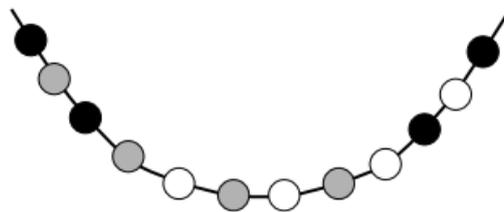


Рис. 6: Для данного ожерелья достаточно 3 разрезов

2 Конструктивная геометрия

Мы будем говорить, что n точек и n прямых на плоскости образуют *конфигурацию* n_d из точек и прямых, если на любой данной прямой лежит ровно d данных точек и через любую данную точку проходит ровно d данных прямых. Т.е. число инцидентий будет равно nd .

2.1. Постройте пример конфигурации 9_3 .

(*Подсказка:* используйте известную геометрическую теорему)

2.2. Постройте пример конфигурации 9_3 , отличной от той, что возникла в 2.1.

2.3. Постройте пример конфигурации 10_3 .

(*Подсказка:* используйте известную геометрическую теорему)

2.4. Постройте пример конфигурации 10_3 , отличной от той, что возникла в 2.3.

2.5.* Докажите, что найдется такая константа C , что для любого N найдутся такие $n > N$ прямых и $n > N$ точек, что число инцидентий задаваемое этими наборами прямых и точек на плоскости больше, чем $Cn^{4/3}$.

Подсказка (после промежуточного финиша). Обратите внимание на картинку на первой странице.

3 Алгебраические мотивы в геометрии

Под записью $g(x) = O(f(x))$ будем подразумевать, что существует такая постоянная $C > 0$, что $|g(x)| \leq C f(x)$ выполняется при любом x .

Дан многочлен $f(x, y)$. Множеством нулей Z_f многочлена $f(x, y)$ называется множество всех точек (x, y) , для которых $f(x, y) = 0$. Назовем степенью многочлена число равное наибольшему значению $i + j$ среди всех мономов вида $x^i y^j$ с ненулевым коэффициентом. Степень многочлена $f(x, y)$ будем обозначать через $\deg f$.

3.1. Дан многочлен $f(x, y)$ степени d и произвольная прямая l . Докажите, что либо прямая l пересекает множество Z_f не более, чем по d точкам, либо прямая l целиком содержится в множестве Z_f .

3.2. Дан многочлен $f(x, y)$ степени d . Докажите, что число прямых которые содержатся в множестве Z_f не превосходит d .

3.3. Покажите, что количество мономов степени не выше d от двух переменных равно $\binom{d+2}{2} = \frac{(d+1)(d+2)}{2}$.

Многочлен $f(x, y)$ будем называть r -**делящим** (где $r > 1$) для данного конечного множества точек $A \subset \mathbb{R}^2$ (где $|A| = n$), если в каждой компоненте связности множества $\mathbb{R}^2 \setminus Z_f$ будет содержаться не более n/r точек из A .

3.4. Докажите, что для данного множества $A \subset \mathbb{R}^2$ (где $|A| = n$) существует многочлен степени $[r]$, который будет r -делящим.

Определение. Пусть d — произвольное натуральное число, а $D = \binom{d+2}{2} - 1$. *Отображением Веронезе степени d* назовем отображение $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^D$, заданное следующей формулой:

$$\varphi(x, y) := (x^i y^j)_{(i, j) | 1 \leq i + j \leq d} \in \mathbb{R}^D.$$

(Каждой координате в \mathbb{R}^D соответствует пара (i, j) , для которой выполняется неравенство $1 \leq i + j \leq d$.)

Заметим, что с помощью применения отображения Веронезе степени 2 можно показать, что для любых пяти точек, среди которых нет четырех, лежащих на одной прямой, существует единственная коника, проходящая через эти точки (коникой называется множество нулей многочлена от двух переменных степени 2). Для этого необходимо провести гиперплоскость через образы данных пяти точек (в нашем случае $D=5$ и можно показать, что через пять образов точек можно провести единственную гиперплоскость) при отображении Веронезе и рассмотреть конику, уравнение которой имеет те же коэффициенты, что и данная гиперплоскость.

3.5. Даны конечные множества A_1, \dots, A_m . Докажите, что существует многочлен степени не выше k , где $\binom{k+2}{2} - 1 \geq m$, который будет 2-делящим многочленом для каждого из данных множеств.

3.6. Докажите, что для данного множества $A \subset \mathbb{R}^2$ (где $|A| = n$) существует многочлен степени не выше $c\sqrt{r}$, который будет r -делящим (например, можно показать, что $c < 7$)

4 Первое доказательство теоремы Семереди-Троттера

4.1. Докажите, что $I(m, n) = I(n, m)$.

Далее будем считать, что $|L| = |P| = n$. Построим r -делящий многочлен $f(x, y)$ для данного множества точек P .

Обозначим через $L_0 \subset L$ множество прямых $l \in L$, $Z_l \subset Z_f$, а через $P_0 \subset P$ множество точек $p \in P \cap Z_f$. Пусть многочлен f поделил плоскость на s частей: точки в i -ой части будем обозначать через P_i , а прямые который пересекают i -ую часть через L_i .

4.2. Докажите, что существуют такие константы c_1, c_2, c_3 , что

а) $I(L_0, P_0) \leq c_1 n \sqrt{r}$;

б) $I(L \setminus L_0, P_0) \leq c_2 n \sqrt{r}$;

в) $\sum_{i=1}^s I(L_i, P_i) \leq c_3 n^2 / r$.

4.3. Выбрав нужное r , докажите теорему Семереди-Троттера.

4.4. Докажите теорему Семереди-Троттера в общем случае:

Теорема Семереди-Троттера. $I(n, m) = O((nm)^{2/3} + n + m)$.

Для этого нужно получить оценки, аналогичные тем, что были получены в задаче 4.2.

5 Применение теоремы Семереди-Троттера

5.1. а) Докажите, что число прямых, каждая из которых содержит по крайней мере k различных точек m -элементного множества P , равно $O(m^2/k^3 + m/k)$.

б) Докажите, что такие прямые задают $O(m^2/k^2 + m)$ инциденций с данным множеством точек P .

5.2. (*Теорема Бека*) Пусть P — множество точек на плоскости, а L — множество прямых, образованных по крайней мере двумя точками из P . Тогда найдутся такие константы $c_1, c_2 > 0$, что выполняется одно из двух условий:

1. Найдется прямая из L , которая содержит по крайней мере $c_1|P|$ точек.
2. $|L| \geq c_2|P|^2$.

5.3. Пусть $A \subset \mathbb{R}$ — конечное множество. Тогда существует $c > 0$ такое, что

$$\max\{|A + A|; |A \cdot A|\} \geq c|A|^{5/4}.$$

Здесь

$$A + A = \{a_1 + a_2 : a_1 \in A, a_2 \in A\}, A \cdot A = \{a_1 \cdot a_2 : a_1 \in A, a_2 \in A\}.$$

Инциденции точек и прямых.

Фёдор Нилов, Александр Полянский, Никита Полянский,
при участии Михаила Харитонов и Игоря Шнурникова



Рис. 1: Пал Эрдёш

Жил-был дедушка Эрдёш. Придумывал он много задачек. Так вот однажды он загадал следующую загадку.

Пусть на плоскости живет некоторое конечное множество прямых \mathcal{L} и некоторое конечное множество точек P . Тогда через $I(\mathcal{L}, P)$ будем обозначать количество инциденций между этими множествами, то есть число таких пар (l, p) , $l \in \mathcal{L}$, $p \in P$, что $p \in l$.

Обозначим за $I(n, m)$ максимальное значение $I(\mathcal{L}, P)$ среди всех таких пар (\mathcal{L}, P) , что $|\mathcal{L}| = n$, $|P| = m$, здесь и далее через $|A|$ обозначаем количество элементов в множестве A .

Вопрос: Получить точную оценку сверху для $I(n, m)$.

П. Эрдёш предположил: существует такая константа C , что

$$I(n, n) \leq C \left(n^{4/3} \right).$$

Очевидно, что эта оценка лучше тривиальной $I(n, n) \leq n^2$.

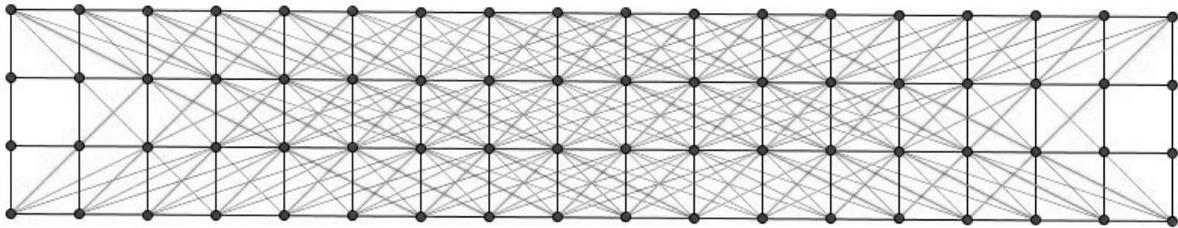


Рис. 2: Точки и прямые с большим числом инциденций

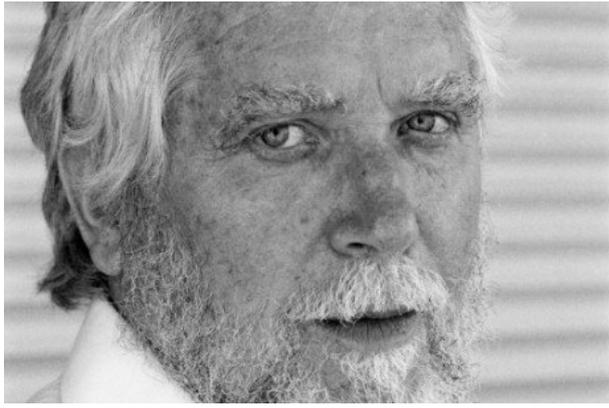


Рис. 3: Эндре Семереди



Рис. 4: Уильям Т. Троттер

В 1983 году два математика, Семереди и Троттер, доказали последнюю оценку. Этот факт известен как **теорема Семереди-Троттера**.

Наша основная цель — доказать эту теорему двумя способами. Попутно мы решим много интересных задач в геометрии и комбинаторике.

1 Комбинаторная часть

1.1 Введение. Комбинаторная геометрия

1.1. На плоскости расположено конечное количество точек. Докажите, что найдётся такая прямая, что в каждой из полуплоскостей, на которые она делит плоскость, будет не больше половины от всех точек (полуплоскость не содержит свою границу).

Доказательство. Пусть $\{a_1, a_2, \dots, a_n\}$ – данный в условии набор точек, L – произвольная полуплоскость, граница которой не параллельна ни одному отрезку, соединяющему точки набора. Пусть L_i – полуплоскость, полученная параллельным переносом полуплоскости L , и граница которой проходит через точку a_i . Заметим, что для каждого целого числа j от 0 до n найдётся полуплоскость L_{i_j} , содержащая ровно j точек из набора $\{a_1, a_2, \dots, a_n\}$. Тогда граница полуплоскости $L_{i_{\lfloor n/2 \rfloor}}$ и есть искомая прямая. \square

1.2. Пусть на плоскости дано $2n$ точек. Докажите, что их можно разделить на пары так, что отрезки, соответствующие парам, не будут пересекаться.

Доказательство. От противного. Предположим, что разбить точки на пары требуемым способом нельзя. Заметим, что способов разделить $2n$ точек на пары – конечное число. Значит, среди этих разбиений найдётся такое, что сумма длин отрезков, соответствующих парам, не больше, чем при любом другом разбиении. Рассмотрим это разбиение. По предположению найдётся два пересекающихся отрезка, пусть это будут AB и CD . Тогда сумма длин отрезков AC и BD меньше, чем AB и CD . Получили противоречие с минимальностью суммы длин отрезков в рассмотренном разделении на пары. \square

1.3. Дано n точек на плоскости, никакие три из которых не лежат на одной прямой. Между некоторыми из точек проведены отрезки. Назовём набор отрезков между точками *связным*, если между любыми двумя точками найдётся путь по отрезкам из этого набора. Построен такой связный набор Γ , что сумма длин отрезков в Γ не больше, чем в любом другом связном наборе. Докажите, что отрезки из Γ пересекаются только концами.

Доказательство. От противного. Пусть отрезки AC и BD пересекаются. По неравенству треугольника сумма отрезков AB и CD , как и сумма отрезков AD и BC , меньше суммы отрезков AC и BD . Пусть Ω – множество всех отрезков Γ кроме AC и BD . Рассмотрим набор отрезков $\Gamma_1 = \Omega \cup \{AB, CD\}$. Если Γ_1 – не связен, то в Ω нет путей между точками A, B с одной стороны и C, D с другой. Рассмотрим набор отрезков $\Gamma_2 = \Omega \cup \{AD, BC\}$. Если Γ_2 – не связен, то в Ω нет путей между точками A, D с одной стороны и C, B с другой. Значит, если и набор отрезков Γ_1 , и набор отрезков Γ_2 – не связны, то в наборе Γ нет пути между точками A и B . Получено противоречие со связностью Γ . Без ограничения Γ_1 – связный. Но сумма длин отрезков в Γ_1 меньше, чем в Γ . Противоречие. \square

1.4. Пусть на плоскости даны n точек и n непараллельных прямых. Докажите, что можно пронумеровать точки и прямые числами от 1 до n так, чтобы отрезки перпендикуляров, опущенных из соответствующих точек на соответствующие прямые не пересекались.

Доказательство. Рассмотрим такую нумерацию, при которой сумма длин перпендикуляров минимальна. Если таких нумераций несколько, то выберем любую из них. За F_i обозначим i -ю точку, за l_i – i -ю прямую. Пусть для некоторых i и j перпендикуляры из точек F_i и F_j пересеклись в некоторой точке E . Пусть A и B – основания перпендикуляров из точек F_i и F_j на прямые l_i и l_j соответственно. Проведём перпендикуляры из точек F_i и F_j на l_j и l_i с основаниями C и D соответственно. Таким, образом,

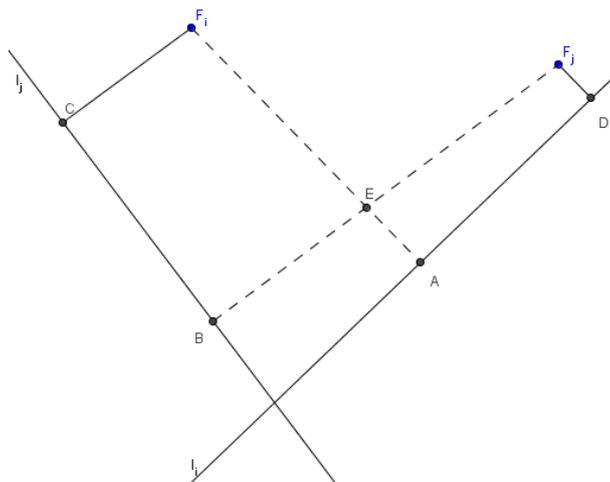


Рис. 5:

имеем

$$\begin{aligned} F_i A + F_j B &= F_i E + EA + F_j E + BE = (EA + F_j E) + (F_i E + BE) \geq \\ &\geq F_j A + F_i B \geq F_j D + F_i C. \end{aligned}$$

Значит, сумма длин перпендикуляров в выбранной нумерации не минимальна. Противоречие. \square

1.5. Дан невыпуклый многоугольник $A_1 A_2 \dots A_n$. Если несмежные вершины A_i и A_j многоугольника таковы, что он лежит целиком по одну сторону от прямой $A_i A_j$, то можно взять одну из двух ломаных, на которые точки A_i и A_j его разбивают, и отразить симметрично относительно центра отрезка $A_i A_j$. Докажите, что рано или поздно многоугольник станет выпуклым.

Доказательство. Пусть для $i = 1, 2, \dots, n$, γ_i – меньший из углов, под которыми пересекаются $A_i A_{i+1}$ и ось абсцисс (в случае равенства углов γ_i равно 90 градусов). γ_n – угол при $A_n A_1$. Рассмотрим теперь множество пар вида (“длина отрезка”, “угол с осью абсцисс”) $\Omega = \{(|A_1 A_2|, \gamma_1), (|A_2 A_3|, \gamma_2), \dots, (|A_n A_1|, \gamma_n)\}$. После каждой операции из условия задача будем пересчитывать множество Ω для нового многоугольника. Заметим, что все такие множества будут отличаться только порядком элементов. Значит, нашими операциями можно получить конечное число многоугольников. Заметим, что при каждой операции площадь многоугольника увеличивается. Значит, наступит момент, когда операцию из условия задачи проделать нельзя. В этот момент и будет получен выпуклый многоугольник. \square

1.2 Инциденции множеств

1.6. Пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ – произвольная совокупность трёхэлементных подмножеств n -элементного множества, причём $|M_i \cap M_j| \neq 1$ для любых i, j . Найдите максимальное значение s , при котором это возможно.

Доказательство. Рассмотрим A и B – 2 пересекающихся множества из нашей совокупности. Пусть $F = A \cap B$, $G = A \cup B$. Пусть $A = \{a, b, c\}$. Без ограничения общности $B = \{b, c, d\}$, $F = \{b, c\}$. Посмотрим, какие множества могут пересекать G .

Случай 1: $\nexists C \in \mathcal{M} : C \supset F$.

Пусть $C \cap (A \cup B) \neq \emptyset$. Т.к. $C \not\supset F$, имеем $\{a, d\} \subset C$. Следовательно, либо $C = \{a, b, d\}$, либо $\{a, c, d\}$.

Заметим, что четверка $A, B, \{a, b, d\}, \{a, c, d\}$ может являться подмножеством \mathcal{M} . Более того, больше никакое множество не из этой четверки не пересекается с $A \cup B$. Назовём такое объединение элементов четверки *булочкой*.

Случай 2: В \mathcal{M} есть ровно $k > 0$ множеств, содержащих F .

Пусть эти множества: C_1, C_2, \dots, C_k . Считаем $A_i = \{a_i, b, c\}$.

Пусть найдётся $D \in \mathcal{M}$, $D \not\supset F$ такое, что

$$D \cap (A \cup B \cup A_1 \cup A_2 \cup \dots \cup A_k) \neq \emptyset.$$

Без ограничения общности $D \cap A \neq \emptyset$. Опять же, без ограничения общности $D \cap A = \{a, b\}$, пусть $D = \{a, b, x\}$. Но, т.к. $D \cap B \neq \emptyset$, $D \cap A_1 \neq \emptyset$ и $x \neq c$, мы имеем $x = d$ and $x = a_1$ одновременно. Противоречие. Значит, такого D не существует.

Заметим, что набор $A, B, A_1, A_2, \dots, A_k$ может являться подмножеством \mathcal{M} . Назовём объединение элементов такого набора *цветочком* с $(k + 2)$ лепестками.

Таким образом, наше n -элементное множество распадается на попарно непересекающиеся булочки и цветочки.

Заметим, что в булочке ровно 4 элемента, в цветочке с k лепестками – $k + 2$ элемента.

Получаем, что $s \leq n - 2t$, где t – количество цветочков.

Отсюда следует, что **при** $n \equiv 0, 1, 2 \pmod{4}$ **максимальное** $s = 4 \cdot \lfloor \frac{n}{4} \rfloor$, достигается при разбиении множества на $\lfloor \frac{n}{4} \rfloor$ булочек (ещё могут остаться 1 или 2 элемента, которые ни в одно множество не входят). **При** $n \equiv 3 \pmod{4}$ **достигается** $s = n - 2$, если все элементы включить в один большой цветочек. \square

1.7. Пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ — произвольная совокупность, состоящая из четырёхэлементных подмножеств n -элементного множества, причём $|M_i \cap M_j| \neq 2$ для любых i, j . Докажите, что максимальное s , при котором это возможно, лежит в пределах от $\lfloor n/4 \rfloor^2$ до $n(n-1)/4$.

Доказательство. 1) Верхняя оценка. Рассмотрим произвольный элемент A нашего n -элементного множества. Пусть \mathcal{F}_A — подсовокупность множеств \mathcal{M} , содержащих A . Рассмотрим совокупность трёхэлементных множеств \mathcal{F}'_A , полученную из \mathcal{F}_A удалением элемента A из каждого множества из \mathcal{F}_A . Любые два множества из \mathcal{F}'_A либо не пересекаются, либо пересекаются по двум элементам. Следовательно, к ним можно применить задачу 18, решённую выше. Получаем, что в \mathcal{F}'_A не более $(n-1)$ -го множества. Количество множеств в \mathcal{F}_A равно количеству множеств \mathcal{F}'_A . Следовательно, в \mathcal{F}_A не более $(n-1)$ -го множества. Для любого элемента исходного n -элементного множества соответствующая подсовокупность содержит не более $(n-1)$ -го множества, в каждом множестве ровно 4 элемента, следовательно, $s \leq \frac{n(n-1)}{4}$.

2) Нижняя оценка. Пронумеруем элементы числами от 1 до n . Рассмотрим множества вида $\{4k+1, 4k+2, 4k+3, 4t\}$, где $k = 0, 1, \dots, \lfloor \frac{n}{4} \rfloor - 1$, $t = 1, 2, \dots, \lfloor \frac{n}{4} \rfloor$. Таких множеств ровно $\lfloor \frac{n}{4} \rfloor^2$. Несложно проверить, что их совокупность удовлетворяет условию задачи.

3) Вывод. Мы получили, что максимальное s лежит в пределах от $\lfloor \frac{n}{4} \rfloor^2$ до $\frac{n(n-1)}{4}$. \square

Определение. Пусть $\mathcal{L} = \{l_1, \dots, l_n\}$ — произвольная совокупность подмножеств m -элементного множества $P = \{p_1, \dots, p_m\}$. Назовём пару (l_i, p_k) *инцидентом*, если $p_k \in l_i$. Тогда через $I(\mathcal{L}, P)$ будем обозначать число инцидентов, образованных элементами из \mathcal{L} и P , а через $I(n, m)$ максимальное значение $I(\mathcal{L}, P)$ по всем таким множествам \mathcal{L} и P , что $|\mathcal{L}| = n, |P| = m$.

Один из важных вопросов всего проекта состоит в том, чтобы оценить число инцидентов в случае, когда даны какие-то условия на множества. Если нет никаких условий на множества, то можем получить лишь тривиальную оценку $I(\mathcal{L}, P) \leq mn$.

Есть следующий способ воспринимать инциденты:

Рассмотрим пустую табличку, состоящую из n строчек и m столбцов. Строки будут соответствовать элементам множества $\{l_1, \dots, l_n\}$, а столбцы — элементы $\{p_1, \dots, p_m\}$. Тогда мы будем ставить на позицию,

находящуюся на пересечении i -ой строчки, и j -го столбца, звездочку тогда и только тогда, когда $p_j \in l_i$. Вопрос о числе инцидентов можно теперь поставить так: сколько звездочек стоит в таблице?

Если вам это будет удобно, то переводите задачи на язык табличек (см. задачу 1.11.).

В оставшихся задачах этого параграфа мы считаем, что $n, m, r \in \mathbb{N}$, $\mathcal{L} = \{l_1, \dots, l_n\}$ – произвольная совокупность подмножеств m -элементного множества $P = \{p_1, \dots, p_m\}$, причем $|l_i \cap l_j| \leq r$ для любых $i \neq j$.

1.8. Пусть $r = 1$. Докажите, что

а) $I(\mathcal{L}, P) \leq n^2 + m$, $I(\mathcal{L}, P) \leq m^2 + n$.

б) $I(\mathcal{L}, P) \leq \sqrt{m(n^2 - n)} + m$, $I(n, m) \leq \sqrt{n(m^2 - m)} + n$.

Доказательство. а) Покажем, что $I(\mathcal{L}, P) \leq m^2 + n$. Мы можем разделить множество \mathcal{L} на две группы: первое подмножество \mathcal{L}_1 будет состоять из тех элементов \mathcal{L} , которые инциденты не более чем одному элементу P , и пусть $\mathcal{L}_2 = \mathcal{L} \setminus \mathcal{L}_1$. Тогда очевидно, что $I(\mathcal{L}_1, P) \leq |\mathcal{L}_1| \leq n$. Оценим $I(\mathcal{L}_2, P)$. Заметим, что всякий элемент p из P может иметь не более чем $m - 1$ инцидентный из \mathcal{L}_2 , поскольку в противном случае найдутся такие два элемента из \mathcal{L}_2 , которые будут содержать по крайней мере 2 общих элемента из P (p и какой-то еще). А потому $I(\mathcal{L}_2, P) \leq m(m - 1) \leq m^2$.

Другое неравенство следует из принципа двойственности, из которого легко вывести, что $I(n, m) = I(m, n)$.

б) Воспользуемся вышеупомянутой аналогией с матрицей. Пусть r_i , $1 \leq i \leq n$, означает число звезд в i -й строке. Также пусть $r_i \geq r_j$ для $i \leq j$ и определим число k следующим образом: $r_k \geq 2$ и $r_i = 1$ for $i > k$. Тогда заметим

$$\binom{m}{2} \geq \sum_{i=1}^k \binom{r_i}{2},$$

поскольку в противном случае найдутся строки, в которых стоят 2 звезды в пересечении с одинаковыми столбцами. Значит

$$2n \cdot \binom{m}{2} \geq 2n \cdot \left(\sum_{i=1}^k \binom{r_i}{2} + \frac{n-k}{2} - \frac{n-k}{2} \right) \geq I^2 - nI \geq (I - n)^2.$$

□

1.9. Докажите, что

$$I(\mathcal{L}, P) \leq \sqrt{mr(n^2 - n)} + m.$$

Доказательство. Для вывода формулы используйте ту же аргументацию, что и в решении **1.8(b)**, при этом добавиться множитель r в левой части первого неравенства. \square

1.10. Пусть $r = 1$.

(a) Найдите $\max I(\mathcal{L}, P)$ при $n \leq 3$.

(b) Найдите $\max I(\mathcal{L}, P)$ при $m \geq C_n^2$. При каких условиях достигается этот максимум?

Решение. (b) $\max I(\mathcal{L}, P) = m + C_n^2$. Достигается при n прямых в общем положении. Возьмем точку, через которую проходит i прямых и пошевелим ее. Тогда число инцидентий изменится на $-i + 2C_i^2 - (C_i^2 - 1) > 0$ при $i \geq 3$. Таким образом, максимальное число инцидентий будет при расположении прямых в общем положении, при этом все точки пересечения прямых — отмеченные точки.

1.11. Квадрат 13×13 разбит на единичные квадратики. Центры некоторых из них отмечены так, что нет прямоугольника с вершинами в отмеченных точках и сторонами, параллельными сторонам квадрата. Найдите наибольшее возможное число отмеченных точек.

Ответ: 52. Пример строится, если каждой строке отметить по 4 точки. Верхняя оценка выводится из следующей задачи.

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}
l_1	*	*		*						*			
l_2		*	*		*						*		
l_3			*	*		*						*	
l_4				*	*		*						*
l_5	*				*	*		*					
l_6		*				*	*		*				
l_7			*				*	*		*			
l_8				*				*	*		*		
l_9					*				*	*		*	
l_{10}						*				*	*		*
l_{11}	*						*				*	*	
l_{12}		*						*				*	*
l_{13}	*		*						*				*

1.12. 100 (a) мышей вместе грызут 1000 (b) кусков сыра. Каждая мышь может попробовать несколько кусков сыра, сделав в каждом из них по одной дырке. Любые две мыши имеют дырки не более чем в 10 (c) общих кусках сыра. Докажите, что число дырок не больше $11000(b + a\sqrt{bc})$. Докажите, что число дырок не больше $10500 \left(\frac{b + \sqrt{b^2 + 4bca(a-1)}}{2} \right)$.

Доказательство. Можно считать, что каждый кусок сыра ела хотя бы одна мышь. Пусть d_i — число кусков сыра, поеденных i мышами. Обозначим число дырок через I . Тогда

$$\sum_i d_i = b, \quad \sum i d_i = I, \quad \sum \frac{i(i-1)}{2} d_i \leq c \frac{a(a-1)}{2}.$$

Тогда по неравенству о среднем арифметическом и квадратическом, примененному к числам $(i-1)$, взятым в количестве d_i , получаем:

$$I - b = \sum (i-1) d_i = b \frac{\sum (i-1) d_i}{\sum d_i} \leq b \sqrt{\frac{\sum (i-1)^2 d_i}{\sum d_i}} \leq \sqrt{b(ca(a-1) - (I-b))}.$$

Откуда (пренебрегая $I-b$ под корнем) получаем $I \leq b + a\sqrt{bc}$. Для более точной оценки сводим к квадратному неравенству $(I-b)^2 + b(I-b) - bca(a-1) \leq 0$ и решаем его. \square

1.3 Теорема о сэндвиче.

1.13. Докажите, что если на плоскости даны красные и синие точки в общем положении, то найдётся прямая, которая будет делить плоскость на две такие полуплоскости, что в каждой из них будет находиться не более половины красных и не более половины синих точек.

Доказательство. Обозначим через $R(\phi)$ множество прямых с углом наклона ϕ (отсчитанного против хода часовой стрелки от горизонтального направления), по обе стороны от каждой из которых лежит одинаковое число красных точек. Аналогично, для синих точек введём множество $B(\phi)$. Каждое из множеств $R(\phi)$ и $B(\phi)$ представляет собой полосу (возможно, из одной прямой), обозначим через $r(\phi)$ и $b(\phi)$ направленные прямые, проходящие посередине этих полос. Докажем, что для некоторого ϕ_0 имеет место равенство $r(\phi_0) = b(\phi_0)$. Если $r(0) = b(0)$, то $\phi_0 = 0$. Если же $r(0) \neq b(0)$, можно считать, что $r(0)$ проходит левее $b(0)$, если смотреть вдоль направления $r(0)$. Будем изменять ϕ от 0 до π . Поскольку прямые $r(\pi)$ и $b(\pi)$ отличаются от прямых $r(0)$ и $b(0)$ соответственно только направлением, то $r(\pi)$ проходит правее $b(\pi)$. Но $r(\phi)$ и $b(\phi)$ непрерывно зависят от ϕ , и по теореме о промежуточном значении $r(\phi) = b(\phi)$ для некоторого $\phi = \phi_0$. \square

1.14. Докажите, что если в пространстве \mathbb{R}^3 даны красные, синие и зелёные точки в общем положении, то найдётся плоскость, которая будет делить \mathbb{R}^3 на два такие полупространства, что в каждом из них будет находиться не более половины точек каждого цвета.

Доказательство. Очевидно, что эта задача является обобщением предыдущей. Зафиксируем некоторую сферическую систему координат, т.е. систему координат для отображения геометрических свойств фигуры в трёх измерениях посредством задания трёх координат (r, θ, φ) , где r — расстояние до начала координат, а θ и φ — зенитный и азимутальный углы соответственно. (Смотрите рисунок 6.)

С помощью $R(\phi, \psi)$ обозначим множество плоскостей, имеющих одинаковый нормальный вектор, который равен $\vec{n} = (1, \phi, \psi)$, и делящий пополам множество красных точек. Таким же образом, через $G(\phi, \psi)$ и $F(\phi, \psi)$ множество плоскостей, делящих пополам множество синих и красных точек соответственно. Выберем средние плоскости в множествах $R(\phi, \psi)$, $G(\phi, \psi)$ и $F(\phi, \psi)$ и обозначим их через $r(\phi, \psi)$, $g(\phi, \psi)$ и $f(\phi, \psi)$. Можно считать, что если смотреть по направлению вектора \vec{n} ,

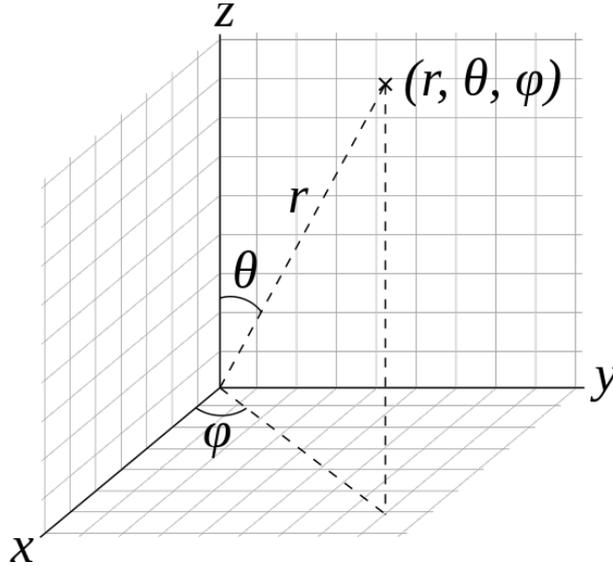


Рис. 6: Сферическая система координат

то $r(0,0)$ лежит выше $g(0,0)$ и $f(0,0)$, а $g(0,0)$ – между $r(0,0)$ и $f(0,0)$. Введем отображение A . Определим

$$A(0,0) = (\text{dist}(r(0,0); g(0,0)), -\text{dist}(g(0,0); f(0,0))),$$

где dist означает расстояние между плоскостями. Таким же образом определим $A(\phi, \psi)$ для всех значений (ϕ, ψ) , причем знак перед расстоянием зависит от взаимного расположения плоскостей (по отношению к направлению нормального вектора). Заметим, что это отображение непрерывно при $\{0 \leq \phi \leq 2\pi\} \times \{-\pi/2 \leq \psi \leq \pi/2\}$, и удовлетворяет следующему свойству $A(\phi, \psi) = -A(\phi + \pi, -\psi)$ для любого $\phi, 0 \leq \phi \leq \pi$. Тогда остается доказать, что найдется такая пара (ϕ, ψ) , при подстановки которой это отображение обнуляется.

Предположим $A(0, \pi/2) \neq (0,0)$. Зафиксируем произвольное ψ . Образ $A(\phi, \psi), \phi \in [0, 2\pi]$ является замкнутой кривой (возможно точкой). Если $\psi = 0$, то из симметрии A следует, что такой образ является симметричным относительно $(0,0)$, и точка $(0,0)$ принадлежит внутренности, ограниченной этой замкнутой кривой. Если мы меняем параметр ψ , то тем самым мы непрерывно меняем внутренность замкнутой кривой. В частности, отсюда следует, что существует такое ψ_0 , при котором $A(\phi, \psi_0) = (0,0)$ для некоторого ϕ . \square

1.15. Пусть на плоскости дано $2m$ точек общего положения, из них m красных и m синих. Докажите, что их можно разделить на пары так, что точки в каждой паре разного цвета и отрезки, соответствующие парам, не будут пересекаться.

Доказательство. Будем нумеровать красные и синие точки от 1 до n , и соединим те пары (красная-синяя) из них, которые имеют одинаковый номер. Предположим, что не существует удовлетворяющей условию нумерации. Тогда рассмотрим такую нумерацию, при которой общая длина отрезков наименьшая, и пусть AB и CD - это два пересекающихся отрезка. Несложно проверить, что $AC + AD \leq AB + CD$ и $AD + BC \leq AB + CD$. Но это противоречит тому, что данная нумерация имеет минимальную общую длину отрезков. \square

Будем обозначать прямую через $\mathbb{R} = \mathbb{R}^1$, плоскость — через \mathbb{R}^2 , а трёхмерное пространство — через \mathbb{R}^3 . Проще всего воспринимать эти объекты следующим образом: \mathbb{R} — это множество всевозможных вещественных (действительных) чисел, \mathbb{R}^2 — это множество всех пар $\mathbf{x} = (x_1, x_2)$ чисел $x_1, x_2 \in \mathbb{R}$, а \mathbb{R}^3 — множество всех троек $\mathbf{x} = (x_1, x_2, x_3)$, где $x_1, x_2, x_3 \in \mathbb{R}$. Аналогично определяется и \mathbb{R}^n . Элементами \mathbb{R}^n являются векторы (точки) $\mathbf{x} = (x_1, \dots, x_n)$, где $x_i \in \mathbb{R}$, $i = 1, \dots, n$ (x_i — координаты).

Пусть a_1, a_2, \dots, a_d — некоторые действительные числа, не равные одновременно нулю, а a_0 — произвольное действительное число. Назовём *гиперплоскостью* в пространстве \mathbb{R}^d множество таких точек \mathbf{x} , что $\sum_{i=1}^d a_i x_i = a_0$, где (x_1, x_2, \dots, x_n) — координаты \mathbf{x} .

Контрольный вопрос. Что такое гиперплоскость в \mathbb{R}^2 и \mathbb{R}^3 ?

Теорема о сэндвиче. Множества $A_1, \dots, A_d \in \mathbb{R}^d$ — конечные. Тогда существует такая гиперплоскость l , что в каждом из полупространств, образованных данной гиперплоскостью, будет не более $\lfloor A_i/2 \rfloor$ точек из A_i (некоторые точки могли лежать в гиперплоскости).

Если в случае $d = 3$ заменить множества A_1, A_2, A_3 на хлеб, сыр и ветчину, то будет существовать такой разрез ножом (плоскость), что в каждом из полученных полупространств будет одинаковое количество каждого из ингредиентов.

1.16. Пусть в пространстве дано $3n$ точек общего положения, из них n красных, n синих и n зелёных. Докажите, что их можно разделить на тройки так, что точки в каждой тройке разного цвета и треугольники, соответствующие тройкам, не будут пересекаться.

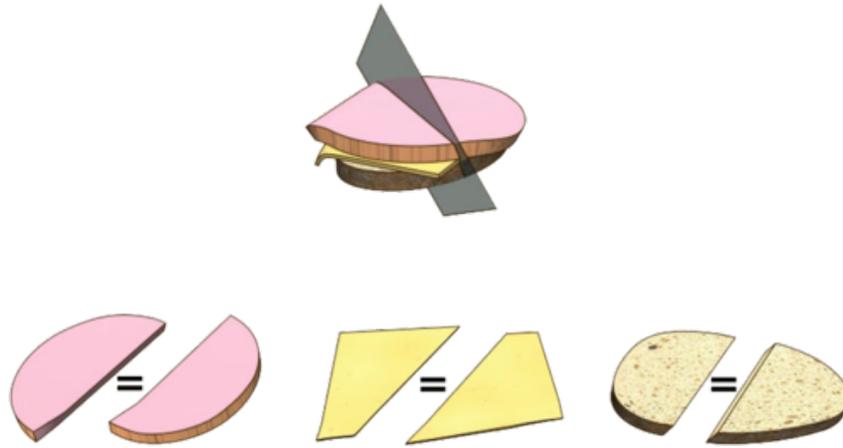


Рис. 7: Разрез сэндвича

Доказательство. Пусть A_i , $i = 1, 2, 3$ – это множество точек i -го цвета. Докажем индукцией по n . Если $n > 1$ нечетно, то существует плоскость h , делящая пополам каждое A_i и содержащая ровно по одной точке каждого цвета. Тогда пусть точки в h образуют треугольник. Далее рассматриваем каждое из открытых полупространств и пользуемся индукцией. Если n четно, опять воспользуемся теоремой о сэндвиче, которая говорит, что существует плоскость делящая пополам каждое из A_i . Опять рассматриваем каждое из полупространств и пользуемся индукцией. В конечном счете, придем к ситуации, когда все точки будут поделены на разноцветные тройки, образующие непересекающиеся треугольники. \square

1.17.* Два вора украли ожерелье с двумя концами, состоящее из платиновой цепочки, на которую нанизаны драгоценные камни d видов. Они не знают ценности каждого камня, поэтому хотят поделить камни каждого вида поровну (известно, что камней каждого вида четное количество). Чтобы потерять как можно меньше платины, воры хотят сделать наименьшее число разрезов. Могут ли они поделить ожерелье с помощью

- а) $(d - 1)$ разрезов?
- б) d разрезов?

Комментарий. Эту задачу проще воспринимать, если решить задачи на отображение Веронеза.

Доказательство. а) Заметим, что нам может не хватить $d - 1$ разрезов. Для доказательства этого достаточно рассмотреть ожерелье, в котором сначала идут все драгоценные камни первого вида, после них - второго вида и т.д.

- б) Расположим рассматриваемое ожерелье в пространстве \mathbb{R}^d вдоль

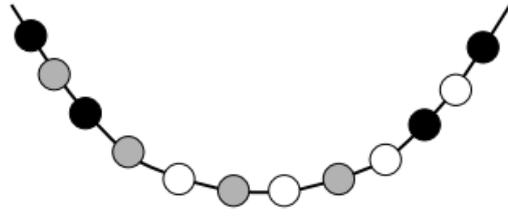


Рис. 8: Для данного ожерелья достаточно 3 разрезов

так называемой кривой моментов γ . Пусть $\gamma(t) = (t, t^2, \dots, t^d)$ параметрическая запись этой кривой γ . Будем считать, что у ожерелья n камней. Тогда определим

$$A_i = \{\gamma(k) : k\text{-й камень является представителем } i\text{-го вида, } k = 1, 2, \dots, n\}.$$

Тогда множество A_i представляет собой все камни i -го вида. По теореме о сэндвиче существует гиперплоскость h , которая одновременно делит множества A_i пополам. Заметим, что h пересекает кривую γ в не более чем d точках. Тогда очевидно, что соответствующие этой гиперплоскости d разрез являются требуемыми. \square

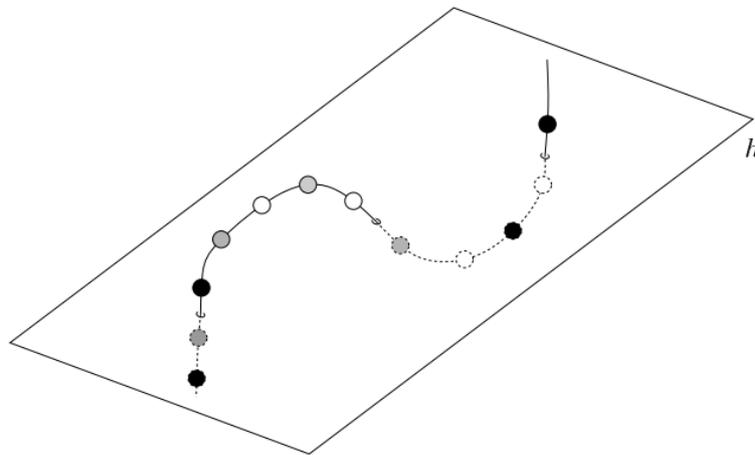


Рис. 9:

2 Конструктивная геометрия

Мы будем говорить, что n точек и n прямых на плоскости образуют *конфигурацию* n_d из точек и прямых, если на любой данной прямой лежит ровно d данных точек и через любую данную точку проходит ровно d данных прямых. Т.е. число инциденций будет равно nd .

2.1. Постройте пример конфигурации 9_3 .

(Подсказка: используйте известную геометрическую теорему)

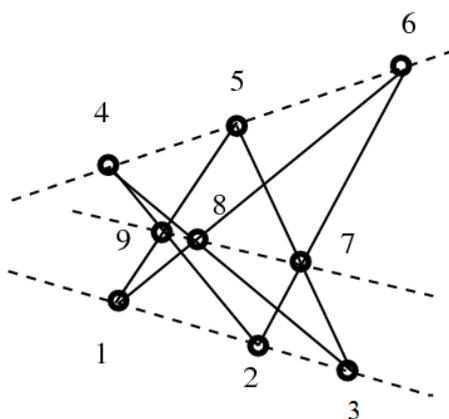


Рис. 10: Конфигурация Паша 9_3

2.2. Постройте пример конфигурации 9_3 , отличной от той, что возникла в 2.1.

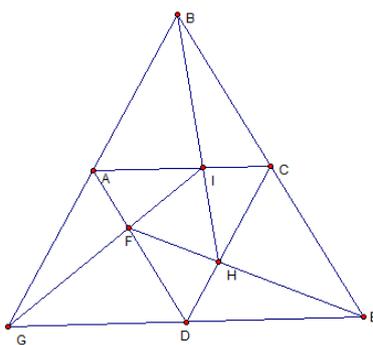


Рис. 11:

2.3. Постройте пример конфигурации 10_3 .

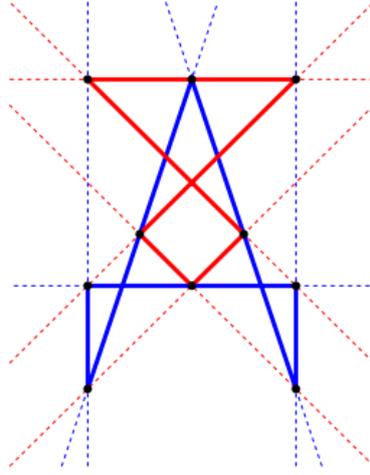


Рис. 12: Конфигурация Дезарга 10_3

2.4. Постройте пример конфигурации 10_3 , отличной от той, что возникла в 2.3.

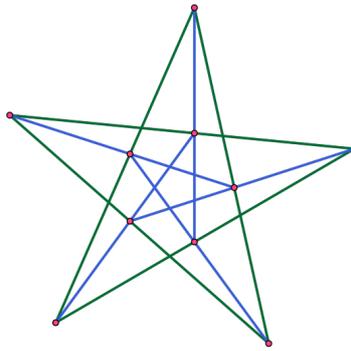


Рис. 13:

2.5.* Докажите, что найдется такая константа C , что для любого N найдутся такие $n > N$ прямых и $n > N$ точек, что число инцидентий задаваемое этими наборами прямых и точек на плоскости больше, чем $Cn^{4/3}$.

Подсказка (после промежуточного финиша). Обратите внимание на картинку на первой странице.

Доказательство. Для простоты будем считать, что $n = 4k^3$ при некотором k . Докажем, что $I(n, n) \gtrsim n^{4/3}$ для некоторой пары (L, P) . Для выбора P рассмотрим точки целочисленной решетки $\{0, 1, \dots, k\} \times \{0, 1, \dots, 4k^2 - 1\}$. Для выбора L возьмем все прямые в мдв $y = ax + b$, где $(a, b) \in \{0, 1, \dots, 2k - 1\} \times \{0, 1, \dots, 2k^2 - 1\}$. Тогда для $x \in [0; k)$ имеем $ax + b < ak + b < 2k^2 + 2k^2 = 4k^2$, таким образом, для каждого $i = 0; \dots, k_i - 1$ каждая линия содержит точку P , у которой $x = i \in \{0, 1, \dots, k\}$. Следовательно, $I(L, P) \approx k^4 \approx n^{4/3}$ \square

3 Алгебраические мотивы в геометрии

Под записью $g(x) = O(f(x))$ будем подразумевать, что существует такая постоянная $C > 0$, что $|g(x)| \leq C f(x)$ выполняется при любом x .

Дан многочлен $f(x, y)$. Множеством нулей Z_f многочлена $f(x, y)$ называется множество всех точек (x, y) , для которых $f(x, y) = 0$. Назовем степенью многочлена число равное наибольшему значению $i + j$ среди всех мономов вида $x^i y^j$ с ненулевым коэффициентом. Степень многочлена $f(x, y)$ будем обозначать через $\deg f$.

3.1. Дан многочлен $f(x, y)$ степени d и произвольная прямая l . Докажите, что либо прямая l пересекает множество Z_f не более, чем по d точкам, либо прямая l целиком содержится в множестве Z_f .

Доказательство. Запишем l в параметрической форме $\{(u_1 t + v_1, u_2 t + v_2) \mid t \in \mathbb{R}\}$. Тогда получаем, что то точки $l \cap Z(f)$ есть корни полинома $g(t) := f(u_1 t + v_1, u_2 t + v_2)$, чья степень не превосходит D . Значит, либо g есть тождественный 0, либо имеет не более D корней. \square

3.2. Дан многочлен $f(x, y)$ степени d . Докажите, что число прямых которые содержатся в множестве Z_f не превосходит d .

Доказательство. Зафиксируем точку $P \in \mathbb{R}^2$, не принадлежащую множеству $Z(f)$. Будем считать, что это множество $Z(f)$ содержит прямые l_1, \dots, l_k . Выберем прямую l , проходящую через P , и которая не параллельна ни одной из прямых l_i и не проходит через ни через одну из точек пересечения $l_i \cap l_j$. (Очевидно, что такая прямая l существует в силу того, что имеется лишь конечное число направлений прямых l_i и конечное число точек их пересечений.) Тогда l не содержится в $Z(f)$ и имеет k пересечений с $\cup_{i=1}^k l_i$. Воспользуемся результатом предыдущей задачи, тогда $k \leq D$. \square

3.3. Покажите, что количество мономов степени не выше d от двух переменных равно $\binom{d+2}{2} = \frac{(d+1)(d+2)}{2}$.

Многочлен $f(x; y)$ будем называть r -**делящим** (где $r > 1$) для данного конечного множества точек $A \subset \mathbb{R}^2$ (где $|A| = n$), если в каждой компоненте связности множества $\mathbb{R}^2 \setminus Z_f$ будет содержаться не более n/r точек из A .

3.4. Докажите, что для данного множества $A \subset \mathbb{R}^2$ (где $|A| = n$) существует многочлен степени r , который будет r -делящим.

Определение. Пусть d — произвольное натуральное число, а $D = \binom{d+2}{2} - 1$. *Отображением Веронезе степени d* назовем отображение $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^D$, заданное следующей формулой:

$$\varphi(x, y) := (x^i y^j)_{(i,j)|1 \leq i+j \leq d} \in \mathbb{R}^D.$$

(Каждой координате в \mathbb{R}^D соответствует пара (i, j) , для которой выполняется неравенство $1 \leq i + j \leq d$.)

Заметим, что с помощью применения отображения Веронезе степени 2 можно показать, что для любых пяти точек, среди которых нет четырех, лежащих на одной прямой, существует единственная коника, проходящая через эти точки (коникой называется множество нулей многочлена от двух переменных степени 2). Для этого необходимо провести гиперплоскость через образы данных пяти точек (в нашем случае $D=5$ и можно показать, что через пять образов точек можно провести единственную гиперплоскость) при отображении Веронезе и рассмотреть конику, уравнение которой имеет те же коэффициенты, что и данная гиперплоскость.

3.5. Даны конечные множества A_1, \dots, A_k . Пусть l — произвольное натуральное число, причем $\binom{l+2}{2} - 1 \geq k$. Докажите, что существует многочлен степени не выше l , который будет 2-делящим многочленом для каждого из данных множеств.

Доказательство. Воспользуемся задачей 3.3, утверждающей, что числу мономов от двух переменных степени не выше l равно $\binom{l+2}{2}$. Пусть $D := \binom{l+2}{2} - 1$, и определим $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^D$ *отображение Веронезе*, заданное следующим образом

$$\phi(x, y) := (x^i y^j)_{(i,j)|1 \leq i+j \leq l} \in \mathbb{R}^D.$$

(Координатам в \mathbb{R}^D соответствует пара (i, j) , для которой $1 \leq i + j \leq l$.)

Определим образы $A'_i := \phi(A_i)$, $i = 1, 2, \dots, k$, тогда по теореме о сэндивиче существует гиперплоскость h , делящая пополам множества A'_1, \dots, A'_k . Очевидно, что h можно записать в форме уравнения $a_{00} + \sum_{i,j} a_{i,j} z_{i,j} = 0$,

где $(z_{i,j})_{(i,j)|1 \leq i+j \leq l}$ являются координатами в \mathbb{R}^D . Легко проверить, что многочлен $f(x, y) := \sum_{i,j} a_{i,j} x^i y^j$ является требуемым. \square

3.6. Докажите, что для данного множества $P \subset \mathbb{R}^2$ (где $|P| = n$) существует многочлен степени не выше $c\sqrt{r}$, который будет r -делящим (например, можно показать, что $c < 7$)

Доказательство. Будем строить по индукции набор $\mathcal{P}_0, \mathcal{P}_1, \dots$, каждый элемент которого состоит из непересекаемых подмножеств множества P ,

причем число подмножеств в каждом элементе $|\mathcal{P}_j| \leq 2^j$ для любого j . Начнем с $\mathcal{P}_0 := \{P\}$. Тогда, построив \mathcal{P}_j , воспользуемся предыдущей задачей, чтобы построить многочлен f_j степени $\deg(f_j) \leq \sqrt{2} \cdot 2^j$, который делит пополам каждое из подмножеств, входящих в \mathcal{P}_j . Для любого $Q \in \mathcal{P}_j$ определим Q^+ как множество, состоящее из точек Q , для которых выполнено $f_j > 0$, а Q^- состоит из таких точек Q , что $f_j < 0$. Положим $\mathcal{P}_{j+1} := \cup_{Q \in \mathcal{P}_j} \{Q^+, Q^-\}$.

Каждое из множеств, входящее в \mathcal{P}_j имеет размер не более $|P|/2^j$. Пусть $t = \lceil \log 2r \rceil$; тогда каждое из \mathcal{P}_t имеет размер не более $|P|/r$. Определим $f := f_1 f_2 \dots f_t$. Как видно из построения конструкции, ни одна из связанных компонент $\mathbb{R}^2 \setminus Z(f)$ не может содержать точки двух различных множеств, входящих в \mathcal{P}_t , поскольку для любой кривой, соединяющей две точки из разных множеств, найдется точка на ней, в которой один из многочленов f_j обнуляется, а потому эта кривая пересекает $Z(f)$. Таким образом, f является r -делящим многочленом для P . Осталось оценить степень

$$\deg(f) = \deg(f_1) + \deg(f_2) + \dots + \deg(f_t) \leq \sqrt{2} \sum_{j=1}^t 2^{j/2} \leq \frac{2}{\sqrt{2}-1} 2^{t/2} \leq c\sqrt{r},$$

где $c = 2\sqrt{2}/(\sqrt{2}-1) < 7$. □

4 Первое доказательство теоремы Семереди-Троттера

4.1. Докажите, что $I(m, n) = I(n, m)$.

Доказательство. Если совершить полярное преобразование, то прямые перейдут в точки, а точки в прямые. При этом инцидентные пары прямая-точка перейдут в инцидентную пару прямая-точка (а неинцидентные соответственно в неинцидентные). Таким образом, конфигурацию на которой число инцидентных пар равно $I(n, m)$ можно перевести с помощью полярного преобразования в конфигурацию с таким же числом инцидентных пар. Но прямые и точки поменялись местами. Поэтому $I(m, n) \geq I(n, m)$. Аналогично можно получить обратное неравенство. Тем самым удается решить задачу. \square

Если применить оценку из задачи 1.8 сразу, то мы не получим доказательство теоремы Семереди-Троттера.

Далее будем считать, что $|L| = |P| = n$. Построим r -делящий многочлен $f(x, y)$ для данного множества точек P .

Обозначим через $L_0 \subset L$ множество таких прямых, что $l \in L$ и $l \subset Z_f$, а через $P_0 \subset P$ множество точек $p \in P \cap Z_f$. Пусть многочлен f поделит плоскость на s частей: точки в i -ой части будем обозначать через P_i , а прямые которые пересекают i -ую часть через L_i .

4.2. Докажите, что существуют такие константы C_1, C_2, C_3 , что

- а) $I(L_0, P_0) \leq C_1 n \sqrt{r}$;
- б) $I(L \setminus L_0, P_0) \leq C_2 n \sqrt{r}$;
- в) $\sum_{i=1}^s I(L_i, P_i) \leq C_3 (n \sqrt{r} + n^2/r)$.

Доказательство. а) Так как число прямых, содержащихся в Z_f не превосходит $\deg f$ (не превосходящей $C_1 \sqrt{r}$ для некоторой константы C_1), см. задачи **3.2** и **3.6**, а число точек в множестве P_0 не превосходит n , то из тривиальной оценки получаем $I(L_0, P_0) \leq C_1 n \sqrt{r}$.

б) Так как любая прямая из $L \setminus L_0$ пересекает Z_f не более, чем в $\deg f$ точках, так как $\deg f \geq \sqrt{r}$, то $I(L \setminus L_0, P_0) \leq C_1 n \sqrt{r}$.

в) Из задачи **1.8** следует, что

$$\sum_{i=1}^s I(L_i, P_i) \leq \sum_{i=1}^s (|L_i| + |P_i|^2)$$

Обозначим $D = \deg(f) = O(\sqrt{r})$. Тогда $\sum_{i=1}^s |L_i| = O((D + 1)n) = O(\sqrt{rn})$, поскольку нет прямой которая пересекает больше, чем $D + 1$ множество из P_i . В итоге мы получаем

$$\sum_{i=1}^s |P_i|^2 \leq (\max_i |P_i|) \cdot \sum_{i=1}^s |P_i| = O(n^2/r).$$

Значит,

$$\sum_{i=1}^s I(L_i, P_i) \leq \sum_{i=1}^s (|L_i| + |P_i|^2) = O(\sqrt{rn} + n^2/r).$$

□

4.3. Выбрав нужное r , докажите теорему Семереди-Троттера.

Доказательство. Выбирая $r = n^{2/3}$, мы получаем доказательство в случае $n = m$. □

4.4. Докажите теорему Семереди-Троттера в общем случае:

Теорема Семереди-Троттера. $I(n, m) = O((nm)^{2/3} + n + m)$.

Для этого нужно получить оценки, аналогичные тем, что были получены в задаче 4.2.

Доказательство. Мы обобщим доказательство для произвольного m следующим образом. Без ограничения общности мы можем считать, что $m \leq n$. Предположим, что $\sqrt{n} \leq m$, так как иначе теорема следует из задачи **1.8**. Тогда мы положим $r := \frac{m^{4/3}}{n^{2/3}}$. Заметим, что $1 \leq r \leq m$ для указанных m . Тогда мы продолжим доказательство, как и в случае $m = n$. Мы получаем, что $D = \deg(f) = O(m^{2/3}n^{1/3})$ и далее проверяем, что все остальные оценки равны $O(m^{2/3}n^{2/3})$. □

5 Применение теоремы Семереди-Троттера

5.1. а) Докажите, что число прямых, каждая из которых содержит по крайней мере k различных точек m -элементного множества P , равно $O(m^2/k^3 + m/k)$.

б) Докажите, что такие прямые задают $O(m^2/k^2 + m)$ инциденций с данным множеством точек P .

5.2. (*Теорема Бека*) Пусть P — множество точек на плоскости, а L — множество прямых, образованных по крайней мере двумя точками из P . Тогда найдутся такие константы $c_1, c_2 > 0$, что выполняется одно из двух условий:

1. Найдется прямая из L , которая содержит по крайней мере $c_1|P|$ точек.
2. $|L| \geq c_2|P|^2$.

5.3. Пусть $A \subset \mathbb{R}$ — конечное множество. Тогда

$$\max\{|A + A|; |A \cdot A|\} \geq |A|^{5/4}.$$

Здесь

$$A + A = \{a_1 + a_2 : a_1 \in A, a_2 \in A\}, \quad A \cdot A = \{a_1 a_2 : a_1 \in A, a_2 \in A\}.$$

Решение смотрите в [2], стр.15–17, [7].

Список литературы

- [1] *P. Brass, W. Moser, J. Pach* Research Problems in Discrete Geometry Springer, New York, 2005.
- [2] *Zeev Dvir* Incidence Theorems and Their Applications, <http://www.cs.princeton.edu/~zdvir/papers/Dvir-survey.pdf>
- [3] *Jiri Matousek* Lectures on Discrete Geometry // Springer, 2002.
- [4] *Jiri Matousek* Using the Borsuk-Ulam theorem // Springer, 2003.
- [5] *Haim Kaplan, Jiri Matousek, Micha Sharir* Simple Proofs of Classical Theorems in Discrete Geometry via the Guth–Katz Polynomial Partitioning Technique, <http://arxiv.org/abs/1102.5391v1>
- [6] *Endre Szemerédi, William T. Trotter* (1983). Extremal problems in discrete geometry, *Combinatorica* **3** (3–4): 381–392
- [7] http://en.wikipedia.org/wiki/Szemerédi-Trotter_theorem

Point-Line Incidences.

F. Nilov, A. Polyanskii, N. Polyanskii



Figure 1: Paul Erdos

Once upon a time there was a mathematician named Erdos, who invented a lot of striking problems. One day he gave us the following riddle.

Given a finite set \mathcal{L} of lines and a finite set P of points, let $I(\mathcal{L}, P)$ denote the number of incidences between \mathcal{L} and P , i.e., the number of pairs (l, p) , $l \in \mathcal{L}$, $p \in P$, such that $p \in l$.

By $I(n, m)$ denote the largest $I(\mathcal{L}, P)$ among all pairs (\mathcal{L}, P) provided that $|\mathcal{L}| = n$, $|P| = m$. (Here and below the symbol $|A|$ denotes the cardinality of the set A .)

Main question: How to estimate $I(n, m)$?

P. Erdos conjectured: there exists a constant C such that

$$I(n, n) \leq C \left(n^{4/3} \right).$$

Notice that this bound is evidently better than the trivial one $I(n, n) \leq n^2$.

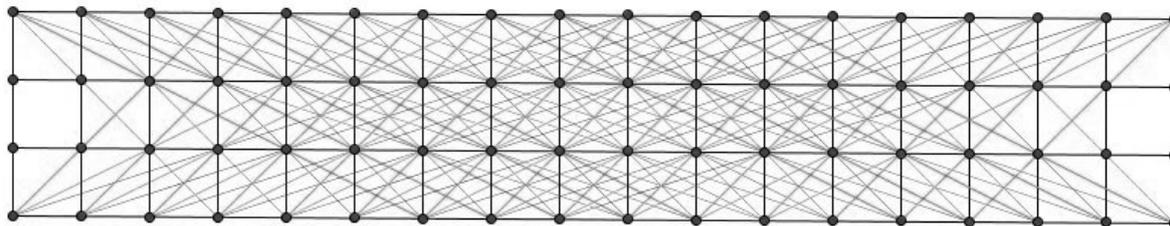


Figure 2: Many point-line incidences

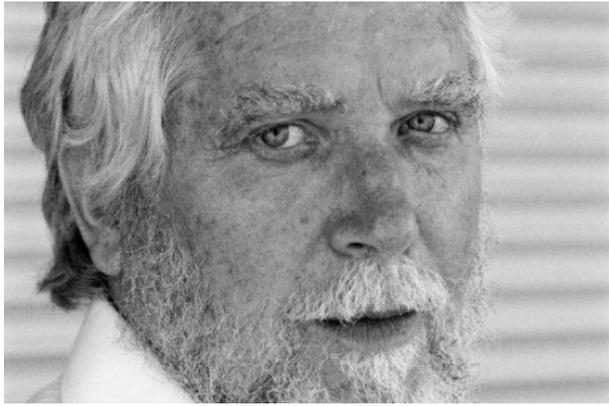


Figure 3: Endre Szemerédi



Figure 4: William Trotter

In 1983, Szemerédi and Trotter managed to prove the Erdős conjecture. This result is called the **Szemerédi–Trotter theorem**.

Our main aim is to prove it using two different approaches. Along the way, we will discover some useful tricks and handle a lot of geometric and combinatorial problems.

1 Combinatorics

1.1 Introduction. Some Combinatorial Problems in Geometry.

1.1. Consider a finite set A of points in the plane. Prove that there exists a line, which divides the plane into two half-planes such that each open half-plane contains at most $\lfloor |A|/2 \rfloor$ points of A .

1.2. Consider $2n$ points in the plane. Prove that the points can be divided into n pairs in such a way that there is no intersection between line segments joining points in pairs.

1.3. Consider n points in the plane so that no three points lie on a line. Construct a non self-intersecting polygonal line joining the given points.

1.4. Consider n points and n pairwise non-parallel straight lines in the plane. Prove that points and lines can be enumerated from 1 to n in such a way that any two segments of perpendiculars from the corresponding points onto the lines don't intersect each other.

1.5. Consider a non-convex polygon $A_1A_2 \dots A_n$. Suppose two non-adjacent vertices A_i and A_j satisfy the following property: the polygon lies completely on one closed half-plane bounded by the line A_iA_j ; then we reflect either the polyline $(A_i \dots A_j)$ or $(A_j \dots A_i)$ through the center of the segment A_iA_j . Prove that applying a finite number of reflections we must come to a convex polygon.

1.2 Incidence Problems

1.6. Let $\mathcal{M} = \{M_1, \dots, M_s\}$, $M_i \subset \{1, 2, \dots, n\}$, $|M_i| = 3$, be an arbitrary collection of subsets of n -set. Suppose $|M_i \cap M_j| \neq 1$; then find the largest possible s .

1.7. Let $\mathcal{M} = \{M_1, \dots, M_s\}$, $M_i \subset \{1, 2, \dots, n\}$, $|M_i| = 4$, be an arbitrary collection of subsets of n -set such that $|M_i \cap M_j| \neq 2$. Denote by $S(n)$ the largest possible s . Prove that $\lfloor n/4 \rfloor^2 \leq S(n) \leq n(n-1)/4$.

Definition. Let $\mathcal{L} = \{l_1, \dots, l_n\}$, $l_i \in P$, be an arbitrary collection of subsets of m -set $P = \{p_1, \dots, p_m\}$. A pair (l_i, p_k) is said to be an *incidence* if $p_k \in l_i$. Denote by $I(\mathcal{L}, P)$ the number of incidences formed by the elements of \mathcal{L} and P . Define $I(n, m) = \max_{|\mathcal{L}|=n, |P|=m} I(\mathcal{L}, P)$.

Our goal is “how to estimate $I(n, m)$ when P and \mathcal{L} satisfy certain properties”. Otherwise, we have only a trivial bound $I(\mathcal{L}, P) \leq mn$.

A typical interpretation of incidences is as follows:

Consider a blank matrix X with n rows and m columns. Rows correspond to elements of the set $\{l_1, \dots, l_n\}$, and columns correspond to elements of the set $\{p_1, \dots, p_m\}$. We will put a star in the entry $x_{i,j}$ iff $p_j \in l_i$. Now we can reformulate the problem: “how many stars are there in the matrix?”

Use this interpretation if it is convenient. (see problem **1.11.**)

Further, it is supposed that $n, m, r \in \mathbb{N}$, and $\mathcal{L} = \{l_1, \dots, l_n\}$ is an arbitrary collection of subsets of m -set $P = \{p_1, \dots, p_m\}$ such that $|l_i \cap l_j| \leq r$ for any $i \neq j$.

1.8. Let $r = 1$. Prove that

(a) $I(\mathcal{L}, P) \leq n^2 + m$, $I(\mathcal{L}, P) \leq m^2 + n$.

(b) $I(\mathcal{L}, P) \leq \sqrt{m(n^2 - n)} + m$, $I(n, m) \leq \sqrt{n(m^2 - m)} + n$.

1.9. Prove that

$$I(\mathcal{L}, P) \leq \sqrt{mr(n^2 - n)} + m, \quad I(\mathcal{L}, P) \leq \sqrt{nr(m^2 - m)} + n.$$

1.10. Let $r = 1$.

(a) Find $\max I(\mathcal{L}, P)$ if $n \leq 3$.

(b) Find $\max I(\mathcal{L}, P)$ if $m \geq C_n^2$. Find a configuration such for which the maximal bound is obtained.

1.11. Let 13×13 square be divided into the unit squares. Some centers of unit squares are marked in such a way that there is no rectangle with vertices being in marked points, sides of which are parallel to the sides of the square. Find the largest possible number of marked points.

1.12. 100 (a) little mice are nibbling 1000 (b) pieces of cheese. Each mouse eat some pieces making holes. But any two mice leave holes in at most 10 (c) common pieces of cheese.

(a) Prove that the number of holes is at most $11000(b + a\sqrt{bc})$.

(b) Prove that the number of holes is at most $10500\left(\frac{b + \sqrt{b^2 + 4bca(a-1)}}{2}\right)$.

1.3 Ham Sandwich Theorem.

1.13. Prove that for a finite set of points in general position in the plane each colored “red” or “blue”, there is a line that simultaneously bisects the red points and bisects the blue points. (“Bisecting” means that each side contains less than half of the total number of points.)

1.14. Prove that for a finite set of points in general position in space each colored “red”, “blue” or “green”, there is a plane that simultaneously bisects each coloured group, that is, the number of points of any color on either side of the plane is less than half of the total number of points.

1.15. Consider $2m$ points, in general position in the plane, such that m points are “red” and the others are “blue”. Prove that the points can be divided into n pairs in such a way that each pair consists of a red point and a blue point, and no two segments joining points in pairs intersect each other.

By $\mathbb{R} = \mathbb{R}^1$, \mathbb{R}^2 and \mathbb{R}^3 denote, respectively, a line, a plane and an 3-dimensional space. A point of $\mathbb{R} = \mathbb{R}^1$ is a real number, a point of \mathbb{R}^2 is a pair $\mathbf{x} = (x_1, x_2)$, where $x_1, x_2 \in \mathbb{R}$, and a point of \mathbb{R}^3 is a vector $\mathbf{x} = (x_1, x_2, x_3)$, where $x_1, x_2, x_3 \in \mathbb{R}$. An element of \mathbb{R}^n is a point (a vector) $\mathbf{x} = (x_1, \dots, x_n)$, where $x_i \in \mathbb{R}$, $i = 1, \dots, n$ (x_i is a coordinate).

A hyperplane h of \mathbb{R}^d is a set of points $\mathbf{x} = (x_1, \dots, x_d)$ that can be described with a single linear equation of the following form (where at least one of the a_i 's is non-zero):

$$\sum_{i=1}^d a_i x_i = a_0.$$

Checking understanding. What does mean a hyperplane in \mathbb{R}^2 and \mathbb{R}^3 ?

We will say that a hyperplane h *bisects* a finite set A if neither of the two open half-spaces bounded by h contains more than $\lfloor |A|/2 \rfloor$ points of A .

Ham Sandwich Theorem. Every d finite sets $A_1, \dots, A_d \subset \mathbb{R}^d$ can be simultaneously bisected by a hyperplane.

The ham sandwich theorem takes its name from the case when $d = 3$ and the three objects of any shape are a chunk of ham, a piece of cheese and a chunk of bread — notionally, a sandwich — which can then all be simultaneously bisected with a single cut (i.e., a plane).

1.16. Consider $3n$ points in general position in the space such that n points are “red”, other n points are “blue” and the others are “green”. Prove that

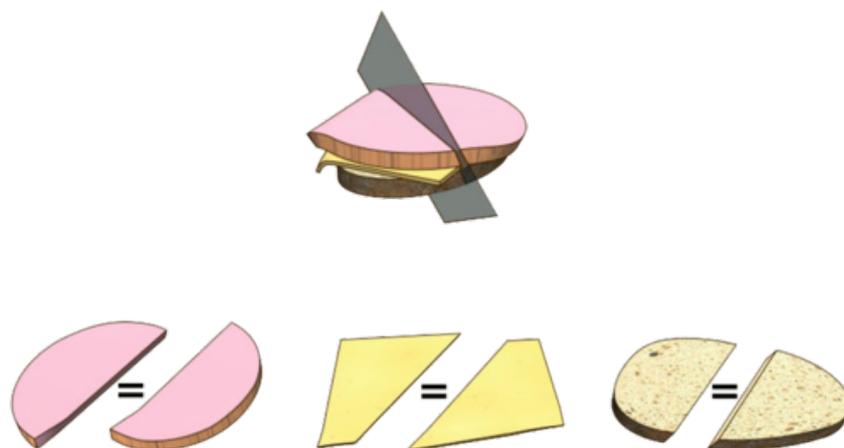


Figure 5: Sandwich cutting

the points can be partitioned into “rainbow” 3-tuples in such a way that no two triangles with vertices on points of triples intersect each other.

1.17.* Two thieves have stolen a precious necklace of nearly immeasurable value, not only because of the precious stones (diamonds, sapphires, rubies, etc.), but also because these are set in pure platinum. The thieves do not know the values of the stones of various kinds, and so they want to divide the stones of each kind evenly. In order to waste as little platinum as possible, they want to achieve this by as few cuts as possible. We assume that the necklace is open (with two ends) and that there are d different kinds of stones, an even number of each kind. How many cuts are necessary to do so?

(a) $(d - 1)$ cuts?

(b) d cuts?

Comment. Solve exercises on the Veronese map for better understanding of this problem.

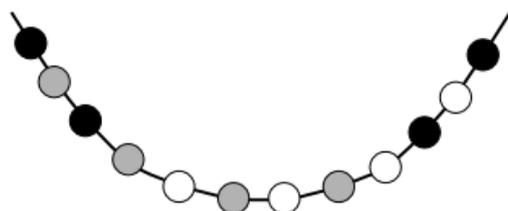


Figure 6: For the necklace here, 3 cuts should suffice

2 Geometric Constructions

We will say that a set P of n points and a set \mathcal{L} of n lines in the plane form a *configuration* n_d if, for any line of \mathcal{L} , there exist exactly d points of P lying on this line, and, for any point of P , there exist exactly d lines of \mathcal{L} passing through this point. This implies that $I(\mathcal{L}, P) = nd$

2.1. Construct an example of configuration 9_3 .

Hint: This is a well-known geometric theorem.

2.2. Construct an example of configuration 9_3 that is different from the previous one.

2.3. Construct an example of configuration 10_3 .

Hint: This is a well-known geometric theorem.

2.4. Construct an example of configuration 10_3 that is different from the previous one.

2.5.* Prove that there exist a constant factor C such that for any N we can find a set \mathcal{L} of $n, n > N$, lines and a set P of $n, n > N$, points with $I(\mathcal{L}, P) > Cn^{4/3}$.

Hint: Look at the figure 2 on the page 1.

3 Algebraic Geometry & the polynomial method

Let f and g be two functions defined on some subset of the real numbers. One writes $g(x) = O(f(x))$ if and only if there exists a positive constant $C > 0$ such that $|g(x)| \leq C f(x)$ for all x .

Given a polynomial $f(x, y) = \sum_{i,j \leq 0} a_{i,j} x^i y^j$. The zero set Z_f of $f(x, y)$ is the subset of points (x, y) in \mathbb{R}^2 on which $f(x, y) = 0$. The polynomial $f(x, y)$ is of degree p ($\deg f = p$) if $p = \max\{i + j \mid a_{i,j} \neq 0\}$.

A polynomial $f(x, y)$ is called a *monomial* if $a_{i,j} = 1$ for exactly one pair (i, j) and $a_{i,j} = 0$ otherwise.

3.1. Consider $f(x, y)$ of degree d and an arbitrary line l . Prove that either $l \in Z_f$, or $|l \cap Z_f| \leq D$.

3.2. Consider a polynomial $f(x, y)$ of degree d . Prove that the number of distinct lines contained in the set Z_f does not exceed d .

3.3. Show that the number of bivariate monomials of degree at most d equals $\binom{d+2}{2}$.

Hint. In other words, we must find the number of pairs (i, j) of nonnegative integers with $i + j \leq D$.

Let P be a set of n points in the plane, and let r be a parameter, $1 < r \leq n$. We say that $f(x, y)$ is an *r -partitioning polynomial* for P if no connected component of $\mathbb{R}^2 \setminus Z_f$ contains more than n/r points of A .

3.4. For any $r > 1$, every finite point set admits an r -partitioning polynomial of degree at most r .

Definition. Given an arbitrary integer d , and let $D = \binom{d+2}{2} - 1$. A map $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^D$ is said to be *the Veronese map of degree d* if this map is given by the following formula:

$$\varphi(x, y) := (x^i y^j)_{(i,j) \mid 1 \leq i+j \leq d} \in \mathbb{R}^D.$$

(We think of the coordinates in \mathbb{R}^D as indexed by pairs (i, j) with $1 \leq i + j \leq D$.)

Note that we can apply the Veronese map of degree 2 to prove that any 5 points in the plane such that no 4 points are collinear uniquely determines a conic passing through the given points (A conic is a zero set of a bivariate polynomial of degree 2). In order to check it, we should consider an appropriate hyperplane containing the images of the given points under the Veronese map (we have $D=5$ in the considered case, and one can show that there exists a unique

hyperplane on which all five images of the points lie). It is easy to check that the conic in the plane which corresponds to the hyperplane is required.

3.5. Given finite sets A_1, \dots, A_l . Let k be an integer such that $\binom{k+2}{2} - 1 \geq l$. Prove that there exists a polynomial of degree at most k that is an 2-partitioning polynomial for every one of these sets.

3.6. For every $r > 1$, every finite point set $P \subset \mathbb{R}^2$ admits an r -partitioning polynomial f of degree at most $O(\sqrt{r})$.

4 The First Proof of the Szemerédi-Trotter Theorem

4.1. Prove that $I(m, n) = I(n, m)$.

In what follows, we assume $|L| = |P| = n$. First of all, we construct an r -partitioning polynomial $f(x, y)$ for the given set P .

By $L_0 \subset L$ denote a subset of lines $l \in L$, $Z_l \subset Z_f$, by $P_0 \subset P$ denote a set of points $p \in P \cap Z_f$. Suppose Z_f bisects the plane into s parts. By P_i denote points of P lying in the i -th part of the plane, and by L_i denote lines of \mathcal{L} passing through the i -th part of the plane.

4.2. Prove that there exist constants C_1, C_2, C_3 such that

a) $I(L_0, P_0) \leq C_1 n \sqrt{r}$;

b) $I(L \setminus L_0, P_0) \leq C_2 n \sqrt{r}$;

c) $\sum_{i=1}^s I(L_i, P_i) \leq C_3 n^2 / r$.

4.3. Having chosen a certain r , prove the Szemerédi-Trotter theorem.

4.4. Prove the the Szemerédi-Trotter theorem in the general case:

Szemerédi-Trotter theorem. $I(n, m) = O((nm)^{2/3} + n + m)$.

In order to check this, you have to obtain bounds, similar to those in **4.2**.

5 Applications of the Szemerédi-Trotter Theorem

5.1. (a) Given a finite set P , $|P| = m$, in the plane. Prove that the number of lines passing through k distinct points of P is at most $C(m^2/k^3 + m/k)$, where C is some constant, which does not depend on m, k .

(b) Prove that such lines define at most $D(m^2/k^2 + m)$ incidences with P , where D is some constant, which does not depend on m, k .

5.2. Let P be a set of points in the plane and let L be the set of lines containing at least 2 points in P . Then there exist such $c_1, c_2 > 0$ that one of these two cases must hold:

1. There exists a line in L that contains at least $c_1|P|$ points.

2. $|L| \geq c_2|P|^2$.

5.3. Let $A \subset \mathbb{R}$ be a finite set. Then there exists $c > 0$ such that

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{5/4}.$$

Here

$$A + A = \{a_1 + a_2 : a_1 \in A, a_2 \in A\}, A \cdot A = \{a_1 a_2 : a_1 \in A, a_2 \in A\}.$$

Point-Line Incidences.

Fedor Nilov, Alexandr Polyanskii, Nikita Polyanskii
with the help of Michael Kharitonov and Igor Shmurnikov



Figure 1: Paul Erdos

Once upon a time there was a mathematician named Erdos, who invented a lot of striking problems. One day he gave us the following riddle.

Given a finite set \mathcal{L} of lines and a finite set P of points, let $I(\mathcal{L}, P)$ denote the number of incidences between \mathcal{L} and P , i.e., the number of pairs (l, p) , $l \in \mathcal{L}$, $p \in P$, such that $p \in l$.

By $I(n, m)$ denote the largest $I(\mathcal{L}, P)$ among all pairs (\mathcal{L}, P) provided that $|\mathcal{L}| = n$, $|P| = m$. (Here and below the symbol $|A|$ denotes the cardinality of the set A .)

Main question: How to estimate $I(n, m)$?

P. Erdos conjectured: there exists a constant C such that

$$I(n, n) \leq C \left(n^{4/3} \right).$$

Notice that this bound is evidently better than the trivial one $I(n, n) \leq n^2$.

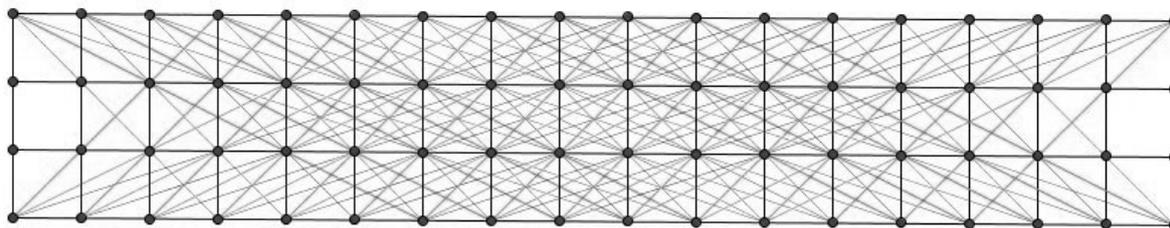


Figure 2: Many point-line incidences

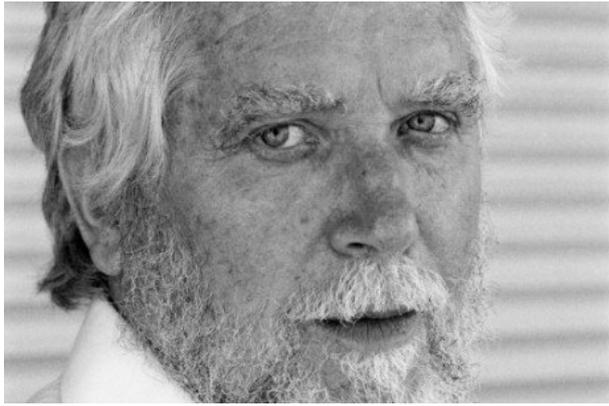


Figure 3: Endre Szemerédi



Figure 4: William Trotter

In 1983, Szemerédi and Trotter managed to prove the Erdős conjecture. This result is called the **Szemerédi–Trotter theorem**.

Our main aim is to prove it using two different approaches. Along the way, we will discover some useful tricks and handle a lot of geometric and combinatorial problems.

1 Combinatorics

1.1 Introduction. Some Combinatorial Problems in Geometry.

1.1. Consider a finite set A of points in the plane. Prove that there exists a line, which divides the plane into two half-planes such that each open half-plane contains at most $\lfloor |A|/2 \rfloor$ points of A .

Proof. Let $\{a_1, a_2, \dots, a_n\}$ be the given set and let L be an arbitrary half-plane, bound of which is parallel to no segment joining any two points of the set. We define L_i as a half-plane obtained by parallel shift of L , and bound of which passes through a_i . We note that for any j , $0 \leq j \leq n$, there exists a half-plane L_{i_j} containing exactly j points of the given set $\{a_1, a_2, \dots, a_n\}$. This implies that the bound of $L_{i_{\lfloor n/2 \rfloor}}$ is a required line. \square

1.2. Consider $2n$ points in the plane. Prove that the points can be divided into n pairs in such a way that there is no intersection between line segments joining points in pairs.

Proof. We will prove it by contradiction. Assume that points could not be divided in the required way. We note that $2n$ points can be paired in only finitely many ways. This implies that there exists a partition with the minimal sum \sum' of all segment lengths. By assumption, there exist two intersecting segments AB and CD . Then the sum of AC and BD is less than the sum of AB and CD . This contradicts the minimality of the sum \sum' . \square

1.3. Consider n points in the plane so that no three points lie on a line. Construct a non self-intersecting polygonal line joining the given points.

Proof. Consider a polygonal line Γ joining the given points, which has the minimal length. Let us prove by contradiction that the given polygonal line is required. Let two segments AC and BD intersect each other. From the triangle inequality it follows that the sum of AB and CD , also as well as the sum of AD и BC , is less than the sum of AC and BD . Let Ω be a union of segments of Γ , except AC and BD . Consider $\Gamma_1 = \Omega \cup \{AB, CD\}$. If Γ_1 is not connected, then there is no path in Ω joining A and B , also as well as no path joining C and D . Consider another union $\Gamma_2 = \Omega \cup \{AD, BC\}$. If Γ_2 is not connected, then there is no path in Ω joining A and D , also as well as no path joining C and B . This implies that if both collections Γ_1 and Γ_2 are not connected, then there is no path in Γ joining A and B . This contradicts the connectivity of Γ . Without loss of generality, let Γ_1 be connected. But

the sum of lengths of segments in Γ_1 is less than in Γ . Here we come to a contradiction. \square

1.4. Consider n points and n pairwise non-parallel straight lines in the plane. Prove that points and lines can be enumerated from 1 to n in such a way that any two segments of perpendiculars from the corresponding points onto the lines don't intersect each other.

Proof. Consider an enumeration, at which the sum of length of altitudes is minimal. By F_i denote i -th point, and by l_i denote i -th line. Assume that, for some i and j , segments of perpendicular dropped from F_i and F_j are intersected in E by each other. Let A and B be the feet of perpendiculars dropped from F_i and F_j onto l_i and l_j correspondently. Draw altitudes dropped from F_i and F_j onto l_j and l_i with foot C and D correspondently.

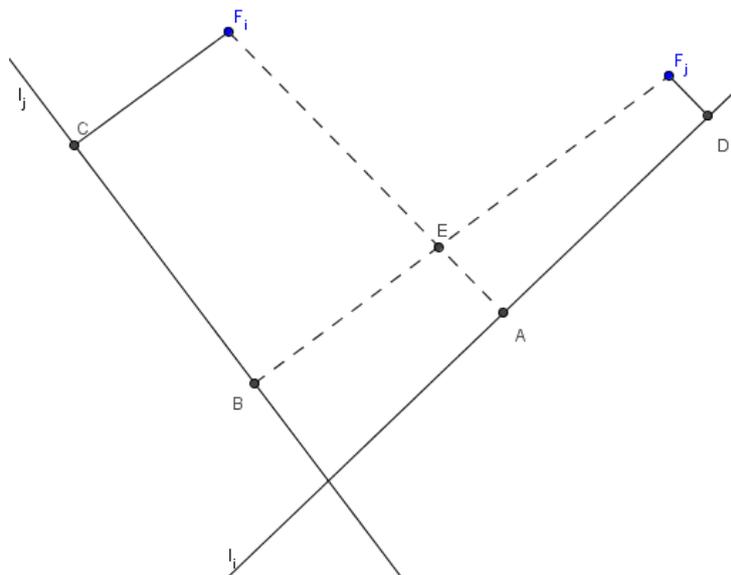


Figure 5:

Thus, we have

$$\begin{aligned} F_iA + F_jB &= F_iE + EA + F_jE + BE = (EA + F_jE) + (F_iE + BE) \geq \\ &\geq F_jA + F_iB \geq F_jD + F_iC. \end{aligned}$$

This means that we come to a contradiction. \square

1.5. Consider a non-convex polygon $A_1A_2 \dots A_n$. Suppose two non-adjacent vertices A_i and A_j satisfy the following property: the polygon lies completely on one closed half-plane bounded by the line A_iA_j ; then we reflect either the

polyline $(A_i \dots A_j)$ or $(A_j \dots A_i)$ through the center of the segment $A_i A_j$. Prove that applying a finite number of reflections we must come to a convex polygon.

Proof. Let $\gamma_i, i \in [n - 1]$, be the smaller angle between $A_i A_{i+1}$ and X -axis. By γ_n denote the smaller angle between $A_n A_1$ and OX -axis. Consider a collection of pairs ("segment length", "angle") $\Omega = \{(|A_1 A_2|, \gamma_1), (|A_2 A_3|, \gamma_2), \dots, (|A_n A_1|, \gamma_n)\}$. After each reflection, Ω will be recalculated for a new polygon. Note that the difference between any two collections is in the order of pairs. This implies that we can get a finitely many polygons. We also note that the area of the next polygon is more than the area of the current polygon. It follows that we will come to a point when the current polygon is convex. \square

1.2 Incidence Problems

1.6. Let $\mathcal{M} = \{M_1, \dots, M_s\}$, $M_i \subset \{1, 2, \dots, n\}$, $|M_i| = 3$, be an arbitrary collection of subsets of n -set. Suppose $|M_i \cap M_j| \neq 1$; then find the largest possible s .

Proof. Consider two intersecting sets $A \in \mathcal{M}$ and $B \in \mathcal{M}$. Let $F = A \cap B$, $G = A \cup B$ and $A = \{a, b, c\}$. Without loss of generality, $B = \{b, c, d\}$, $F = \{b, c\}$. Now let us see which sets can intersect G . We distinguish two cases.

Case 1: No other set of \mathcal{M} contains F , i.e., $\nexists C \in \mathcal{M} : C \supset F, C \notin \{A, B\}$.

Let $C \cap (A \cup B) \neq \emptyset$. We have $\{a, d\} \subset C$, since $C \not\supset F$. Thus, either $C = \{a, b, d\}$, or $C = \{a, c, d\}$.

Notice that four sets $A, B, \{a, b, d\}$ and $\{a, c, d\}$ could be elements of \mathcal{M} at one time. Moreover, no other set is intersected by $A \cup B$. Such union of four sets is said to be a *cookie*.

Case 2: There exist exactly $k + 2 \geq 3$ sets of \mathcal{M} containing F :

$$\{A, B, A_1, A_2, \dots, A_k\}.$$

Assume that $A_i = \{a_i, b, c\}$, and there exists $D \in \mathcal{M}$, $D \not\supset F$ such that

$$D \cap (A \cup B \cup A_1 \cup A_2 \cup \dots \cup A_k) \neq \emptyset.$$

Without loss of generality, $D \cap A \neq \emptyset$, $D \cap A = \{a, b\}$ and $D = \{a, b, x\}$. But since $D \cap B \neq \emptyset$, $D \cap A_1 \neq \emptyset$ and $x \neq c$, then we have that $x = d$ and $x = a_1$ at one time. It means we come to a contradiction, and there is no such set D .

Note that this collection $A, B, A_1, A_2, \dots, A_k$ can be a subset of \mathcal{M} . Such collection of $k + 2$ sets will be called a *flower with $k + 2$ petals*.

Thus, n -set is divided into disjoint cookies and flowers.

We note that a cookie has exactly 4 elements, while a flower with k petals has $k + 2$ elements. It follows that we get $s \leq n - 2t$, where t is the number of flowers.

This implies that we have the maximal $s = 4 \cdot \lfloor \frac{n}{4} \rfloor$ for $n \equiv 0, 1, 2 \pmod{4}$, which is attained when n -set is divided into $\lfloor \frac{n}{4} \rfloor$ cookies (there may remain 1 or 2 elements not included in any set of \mathcal{M}). For $n \equiv 3 \pmod{4}$, we have $s = n - 2$ if all elements are included in one flower. \square

1.7. Let $\mathcal{M} = \{M_1, \dots, M_s\}$, $M_i \subset \{1, 2, \dots, n\}$, $|M_i| = 4$, be an arbitrary collection of subsets of n -set such that $|M_i \cap M_j| \neq 2$. Denote by $S(n)$

the largest possible s . Prove that $\lfloor n/4 \rfloor^2 \leq S(n) \leq n(n-1)/4$.

Proof. 1) An upper bound. Consider an arbitrary element A of n -set. Let \mathcal{F}_A be a collection of elements of \mathcal{M} containing A . Consider a collection \mathcal{F}'_A obtained from \mathcal{F}_A by removing A from each set of \mathcal{F}_A . Any two sets of \mathcal{F}'_A are either disjoint, or intersected in two elements. Thus, we can apply the result of problem 1.6. We get that \mathcal{F}'_A has at most $(n-1)$ sets. The number of sets in \mathcal{F}_A is equal to the number of sets in \mathcal{F}'_A . Hence, for any $A \in [n]$, the collection \mathcal{F}_A has at most $(n-1)$ four-element sets. This implies $s \leq \frac{n(n-1)}{4}$.

2) A lower bound. Here we give an example. Enumerate elements from 1 to n . Consider the following sets $\{4k+1, 4k+2, 4k+3, 4t\}$, where $k = 0, 1, \dots, \lfloor \frac{n}{4} \rfloor - 1$ and $t = 1, 2, \dots, \lfloor \frac{n}{4} \rfloor$. We have exactly $\lfloor \frac{n}{4} \rfloor^2$ such sets. It is easy to check that the considered collection is desired. \square

Definition. Let $\mathcal{L} = \{l_1, \dots, l_n\}$, $l_i \in P$, be an arbitrary collection of subsets of m -set $P = \{p_1, \dots, p_m\}$. A pair (l_i, p_k) is said to be an *incidence* if $p_k \in l_i$. Denote by $I(\mathcal{L}, P)$ the number of incidences formed by the elements of \mathcal{L} and P . Define $I(n, m) = \max_{|\mathcal{L}|=n, |P|=m} I(\mathcal{L}, P)$.

Our goal is “how to estimate $I(n, m)$ when P and \mathcal{L} satisfy certain properties”. Otherwise, we have only a trivial bound $I(\mathcal{L}, P) \leq mn$.

A typical interpretation of incidences is as follows:

Consider a blank matrix X with n rows and m columns. Rows correspond to elements of the set $\{l_1, \dots, l_n\}$, and columns correspond to elements of the set $\{p_1, \dots, p_m\}$. We will put a star in the entry $x_{i,j}$ iff $p_j \in l_i$. Now we can reformulate the problem: “how many stars are there in the matrix?”

Use this interpretation if it is convenient. (see problem **1.11**.)

Further, it is supposed that $n, m, r \in \mathbb{N}$, and $\mathcal{L} = \{l_1, \dots, l_n\}$ is an arbitrary collection of subsets of m -set $P = \{p_1, \dots, p_m\}$ such that $|l_i \cap l_j| \leq r$ for any $i \neq j$.

1.8. Let $r = 1$. Prove that

(a) $I(\mathcal{L}, P) \leq n^2 + m$, $I(\mathcal{L}, P) \leq m^2 + n$.

(b) $I(\mathcal{L}, P) \leq \sqrt{m(n^2 - n)} + m$, $I(n, m) \leq \sqrt{n(m^2 - m)} + n$.

Proof. (a) Let us prove $I(\mathcal{L}, P) \leq m^2 + n$. Divide subsets in \mathcal{L} into two groups: subsets in \mathcal{L}_1 are incidence to at most one element of P , and let $\mathcal{L}_2 = \mathcal{L} \setminus \mathcal{L}_1$. Then $I(\mathcal{L}_1, P) \leq |\mathcal{L}_1| \leq n$. It remains to bound $I(\mathcal{L}_2, P)$.

Notice that any element p of P may have at most $m - 1$ incidences with the elements of \mathcal{L}_2 , since otherwise there exist two elements in \mathcal{L}_2 that have at least two common elements of P (p and another one). Thus, $I(\mathcal{L}_2, P) \leq m(m - 1) \leq m^2$.

The other inequality follows using the geometric duality leading, in particular, to $I(n, m) = I(m, n)$.

(b) Use the above-mentioned analogue with a matrix. By r_i , $1 \leq i \leq n$, denote the number of stars in the corresponding row. Let $r_i \geq r_j$ for $i \leq j$ and let k be a such number that $r_k \geq 2$ and $r_i = 1$ for $i > k$. Then notice

$$\binom{m}{2} \geq \sum_{i=1}^k \binom{r_i}{2},$$

since otherwise there exist two rows which have 2 stars in the intersection of the same columns. Then we have

$$2n \cdot \binom{m}{2} \geq 2n \cdot \left(\sum_{i=1}^k \binom{r_i}{2} + \frac{n-k}{2} - \frac{n-k}{2} \right) \geq I^2 - nI \geq (I - n)^2.$$

□

1.9. Prove that

$$I(\mathcal{L}, P) \leq \sqrt{mr(n^2 - n)} + m$$

Proof. Use the same arguments as in the proof of problem **1.8(b)** (the factor r appears on the left-hand side of the considered chains of inequalities). □

1.10. Let $r = 1$.

(a) Find $\max I(\mathcal{L}, P)$ if $n \leq 3$.

(b) Find $\max I(\mathcal{L}, P)$ if $m \geq C_n^2$. Find a configuration such for which the maximal bound is obtained.

Добавить решения.

Proof. (a) Assume $|\mathcal{L}| = n = 1$, then $\max I(\mathcal{L}, P) = m$. For $|\mathcal{L}| = n = 2$, we get $\max I(\mathcal{L}, P) = m + 1$, since otherwise (if $I(\mathcal{L}, P) \geq m + 2$) there exist at least two common elements of P contained in l_1 and l_2 . If $|\mathcal{L}| = n = 3$, then we have $\max I(\mathcal{L}, P) = m + 3$,

(b) $\max I(\mathcal{L}, P) = m + \binom{n}{2}$. The maximum is attained when all n lines are in general position. □

1.11. Let an 13×13 square be divided into the unit squares. Some centers of unit squares are marked in such a way that there is no rectangle with vertices being in marked points, sides of which are parallel to the sides of the square. Find the largest possible number of marked points.

Answer: 52 points could be (see Figure 6). An upper bound on the number of stars follows from the problem **1.12** (b).

	A ₁	A ₂	A ₃	A ₄	A ₅	A ₆	A ₇	A ₈	A ₉	A ₁₀	A ₁₁	A ₁₂	A ₁₃
l ₁	*	*		*						*			
l ₂		*	*		*						*		
l ₃			*	*		*						*	
l ₄				*	*		*						*
l ₅	*				*	*		*					
l ₆		*				*	*		*				
l ₇			*				*	*		*			
l ₈				*				*	*		*		
l ₉					*				*	*		*	
l ₁₀						*				*	*		*
l ₁₁	*						*				*	*	*
l ₁₂		*						*				*	*
l ₁₃	*		*						*				*

Figure 6:

1.12. 100 (a) little mice are nibbling 1000 (b) pieces of cheese. Each mouse eats some pieces making holes. But any two mice leave holes in at most 10 (c) common pieces of cheese.

(a) Prove that the number of holes is at most 11000 $(b + a\sqrt{bc})$.

(b) Prove that the number of holes is at most $10500 \left(\frac{b + \sqrt{b^2 + 4bca(a-1)}}{2} \right)$.

Proof. Suppose that each piece of cheese is eaten. Let d_i be the number of pieces bitten by i mice. By I denote the number of holes. Then we have

$$\sum_i d_i = b, \quad \sum_i id_i = I, \quad \sum_i \frac{i(i-1)}{2} d_i \leq c \frac{a(a-1)}{2}.$$

Applying the inequality of arithmetic and quadratic means, we obtain

$$I - b = \sum (i-1)d_i = b \frac{\sum (i-1)d_i}{\sum d_i} \leq b \sqrt{\frac{\sum (i-1)^2 d_i}{\sum d_i}} \leq \sqrt{b(ca(a-1) - (I-b))}.$$

Thus, $I \leq b + a\sqrt{bc}$. In order to get a more precise bound, we should reduce the above-mentioned inequality to

$$(I - b)^2 + b(I - b) - bca(a - 1) \leq 0$$

and solve it. □

1.3 Ham Sandwich Theorem.

1.13. Prove that for a finite set of points in general position in the plane each colored “red” or “blue”, there is a line that simultaneously bisects the red points and bisects the blue points. (“Bisecting” means that each side contains less than half of the total number of points.)

Proof. By $R(\phi)$ denote the set of directed lines which make an angle ϕ with OX -axis clockwise and bisect red points. In the same way, by $B(\phi)$ denote the set of directing lines bisecting blue points having the slope ϕ . For any fixed ϕ , $R(\phi)$ is either a strip or a line. We let $r(\phi)$ be the “middle” directed line of $R(\phi)$, and $b(\phi)$ is denoted similarly. Let us prove that $r(\phi_0) = b(\phi_0)$ for a certain ϕ_0 . If $r(0) = b(0)$, then $\phi_0 = 0$. Otherwise without loss of generality, we may assume that $R(0)$ is on the left of $b(0)$ if we are looking across the direction of $r(0)$. One will change ϕ from 0 to π . Notice that $r(\pi)$ is on the right of $b(\pi)$, since $r(\pi)$ and $b(\pi)$ look like $r(0)$ and $b(0)$, except the reverse directions. For $r(\phi)$ and $b(\phi)$ are continuous on $\phi \in [0, \pi]$, we finally obtain that there exist a required ϕ_0 . \square

1.14. Prove that for a finite set of points in general position in space each colored “red”, “blue” or “green”, there is a plane that simultaneously bisects the red points, the blue points and the green points.

Proof. We generalize the previous proof. Fix a spherical coordinate system in the space. This means the position of a point is specified by three numbers: the radial distance of that point from a fixed origin, its polar angle measured from a fixed zenith direction, and the azimuth angle of its orthogonal projection on a reference plane that passes through the origin and is orthogonal to the zenith, measured from a fixed reference direction on that plane (See Figure 7.)

By $R(\varphi, \psi)$ denote the set of planes, normal vectors of which are equal to $\vec{n} = (1, \varphi, \psi)$, and that also bisect red points. In the same way, by $G(\varphi, \psi)$ and by $F(\varphi, \psi)$ denote the sets of planes bisecting blue and green points correspondently. We choose the middle planes of $R(\varphi, \psi)$, $G(\varphi, \psi)$ and $F(\varphi, \psi)$ and designates them by $r(\varphi, \psi)$, $g(\varphi, \psi)$ and $f(\varphi, \psi)$. Without loss of generality, assume that if we are looking along the direction of \vec{n} , then $r(0, 0)$ is above $g(0, 0)$ and $f(0, 0)$, and $g(0, 0)$ is lying between $r(0, 0)$ and $f(0, 0)$. Introduce

$$A(0, 0) = (\text{dist}(r(0, 0); g(0, 0)), -\text{dist}(g(0, 0); f(0, 0))),$$

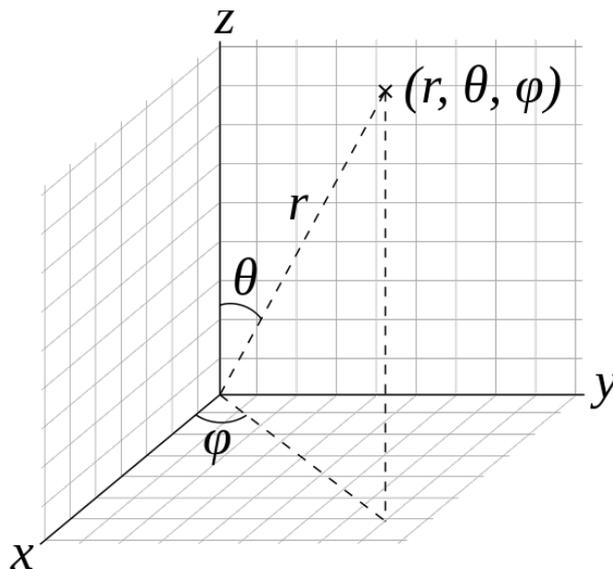


Figure 7: A spherical coordinate system

where $dist$ is a distance between planes. In the same way, define $A(\varphi, \psi)$ for all (φ, ψ) (a sign before distance depends on the positional relationship of the planes). Notice that the considered map is continuous on $\{0 \leq \varphi \leq 2\pi\} \times \{-\pi/2 \leq \psi \leq \pi/2\}$, and satisfy the following property $A(\varphi, \psi) = -A(\varphi + \pi, -\psi)$ for any $\varphi, 0 \leq \varphi \leq \pi$. There remains to prove that there is a pair (φ, ψ) , at which the function A vanishes.

Suppose that $A(0, \pi/2) \neq (0, 0)$. Fix an arbitrary ψ . We have that the image $A(\varphi, \psi), \varphi \in [0, 2\pi]$ is a closed curve (it may be a point). If $\psi = 0$, then from symmetry of A , it follows that such image is symmetrical with respect to $(0, 0)$, and the point $(0, 0)$ belongs to the interior bounded by this loop. Shifting a parameter ψ continually changes the interior of the loop. In particular, this means that there is a ψ_0 such that $A(\varphi, \psi_0) = (0, 0)$ for some φ .

□

1.15. Consider $2m$ points in general position in the plane such that m points are “red” and the others are “blue”. Prove that the points can be divided into n pairs in such a way that each pair consists of a red point and a blue point, and no two segments joining points in pairs intersect each other.

Proof. One can enumerate blue points and red points from 1 to n , and join blue and red points having the same numbers. Assume from the contrary that each enumeration does not satisfy the condition of the problem. Consider such enumeration that the total length of the segments is minimal, and let AB and CD be intersecting segments of this numbering. It is easy to check

that $AC + AD \leq AB + CD$, also as well as $AD + BC \leq AB + CD$. Here we come to a contradiction with the minimality of the sum of the segments. \square

By $\mathbb{R} = \mathbb{R}^1$, \mathbb{R}^2 and \mathbb{R}^3 denote, respectively, a line, a plane and an 3-dimensional space. A point of $\mathbb{R} = \mathbb{R}^1$ is a real number, a point of \mathbb{R}^2 is a pair $\mathbf{x} = (x_1, x_2)$, where $x_1, x_2 \in \mathbb{R}$, and a point of \mathbb{R}^3 is a vector $\mathbf{x} = (x_1, x_2, x_3)$, where $x_1, x_2, x_3 \in \mathbb{R}$. An element of \mathbb{R}^n is a point (a vector) $\mathbf{x} = (x_1, \dots, x_n)$, where $x_i \in \mathbb{R}$, $i = 1, \dots, n$ (x_i is a coordinate).

A hyperplane h of \mathbb{R}^d is a set of points $\mathbf{x} = (x_1, \dots, x_d)$ that can be described with a single linear equation of the following form (where at least one of the a_i 's is non-zero):

$$\sum_{i=1}^d a_i x_i = a_0.$$

Checking understanding. What does mean a hyperplane in \mathbb{R}^2 and \mathbb{R}^3 ?

We will say that a hyperplane h *bisects* a finite set A if neither of the two open half-spaces bounded by h contains more than $\lfloor |A|/2 \rfloor$ points of A .

Ham Sandwich Theorem. Every d finite sets $A_1, \dots, A_d \subset \mathbb{R}^d$ can be simultaneously bisected by a hyperplane.

The ham sandwich theorem takes its name from the case when $d = 3$ and the three objects of any shape are a chunk of ham, a piece of cheese and a chunk of bread — notionally, a sandwich — which can then all be simultaneously bisected with a single cut (i.e., a plane).

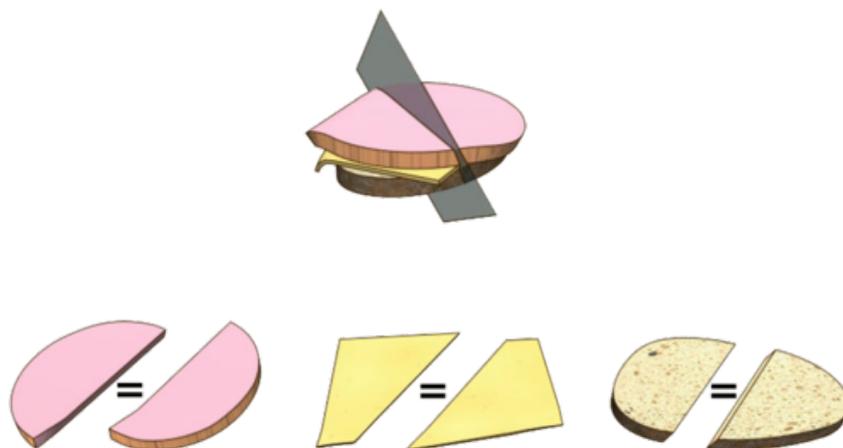


Figure 8: Sandwich cutting

1.16. Consider $3n$ points in general position in the space such that n points are “red”, other n points are “blue” and the others are “green”. Prove that

the points can be portioned into “rainbow” 3-tuples in such a way that no two triangles with vertices on points of triples intersect each other.

Proof. Let A_i , $i = 1, 2, 3$, be a set of points of i -th colour. We proceed by induction on n . If $n > 1$ is odd, there is a plane h bisecting each A_i and containing exactly one point of each color. We let the points in h form one 3-tuple and use induction for the subsets in the open half-spaces. For n even, we invoke the ham-sandwich theorem, which provides a plane bisecting all the A_i . Then we should consider each open half-space, and this completes proving of the inductive step. \square

1.17.* Two thieves have stolen a precious necklace of nearly immeasurable value, not only because of the precious stones (diamonds, sapphires, rubies, etc.), but also because these are set in pure platinum. The thieves do not know the values of the stones of various kinds, and so they want to divide the stones of each kind evenly. In order to waste as little platinum as possible, they want to achieve this by as few cuts as possible. We assume that the necklace is open (with two ends) and that there are d different kinds of stones, an even number of each kind. How many cuts are necessary to do so?

- (a) $(d - 1)$ cuts?
- (b) d cuts?

Comment. Solve exercises on the Veronese map for better understanding of this problem.

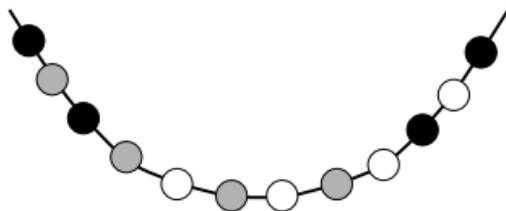


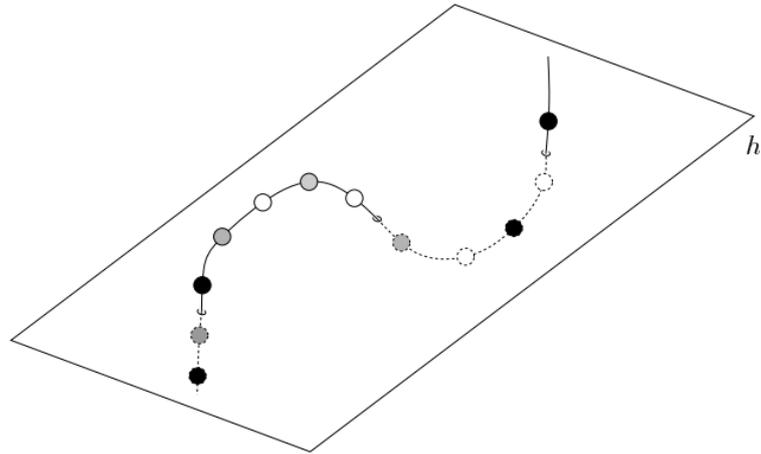
Figure 9: For the necklace here, 3 cuts should suffice

Proof. (a) It is easy to see that at least d cuts may be necessary: place the stones of the first kind first, then the stones of the second kind, and so on.

(b) We place the considered necklace into \mathbb{R}^d along the moment curve. Let $\gamma(t) = (t, t^2, \dots, t^d)$ be the parametric expression of the moment curve γ . If the necklace has n stones, we define

$$A_i = \{\gamma(k) : \text{the } k\text{-th stone is of the } i\text{-th kind, } k = 1, 2, \dots, n\}.$$

Let us also call the points of A_i the stones of the i -th kind. By the ham sandwich theorem, there exists a hyperplane h simultaneously bisecting each A_i . This h cuts the moment curve, and the necklace lying along it, in at most d places. All the sets A_i were assumed to be of even size, so h contains no stones, and these cuts are as required in the necklace problem.



□

2 Geometric Constructions

We will say that a set P of n points and a set \mathcal{L} of n lines in the plane form a *configuration* n_d if, for any line of \mathcal{L} , there exist exactly d points of P lying on this line, and, for any point of P , there exist exactly d lines of \mathcal{L} passing through this point. This implies that $I(\mathcal{L}, P) = nd$

2.1. Construct an example of configuration 9_3 .

Hint: This is a well-known geometric theorem.

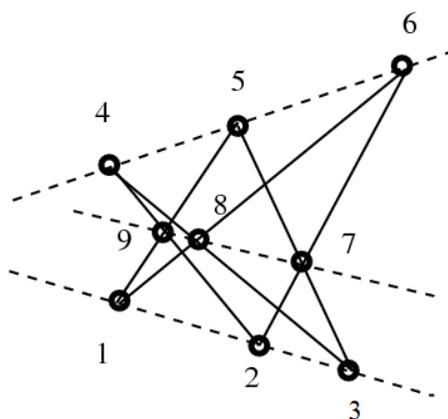
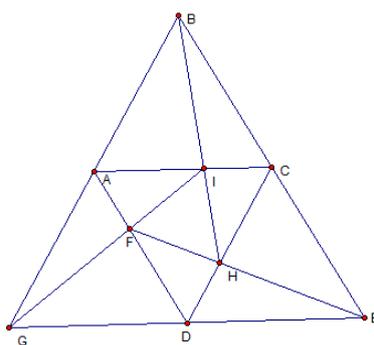


Figure 10: Pappus's 9_3

2.2. Construct an example of configuration 9_3 that is different from the previous one.



2.3. Construct an example of configuration 10_3 .

Hint: This is a well-known geometric theorem.

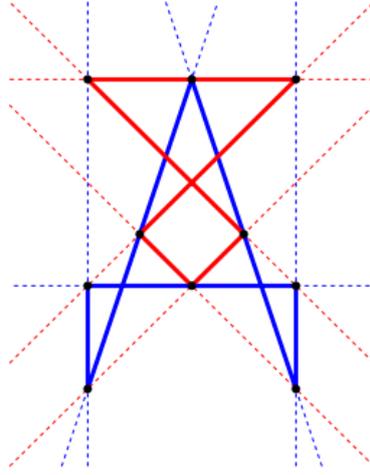
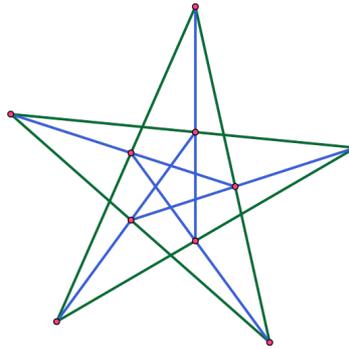


Figure 11: Desargue's 10_3

2.4. Construct an example of configuration 10_3 that is different from the previous one.



2.5.* Prove that there exist a constant factor C such that for any N we can find a set \mathcal{L} of $n, n > N$, lines and a set P of $n, n > N$, points with $I(\mathcal{L}, P) > Cn^{4/3}$.

Hint: Look at the figure 2 on the page 1.

Proof. For simplicity, we suppose that $n = 4k^3$ for a natural k . Let us prove that $I(n, n) \gtrsim n^{4/3}$ for some arrangement (L, P) of points and straight lines to be constructed. For P take the grid $\{0, 1, \dots, k\} \times \{0, 1, \dots, 4k^2 - 1\}$. For L take all lines $y = ax + b$, with $(a, b) \in \{0, 1, \dots, 2k - 1\} \times \{0, 1, \dots, 2k^2 - 1\}$. Then for $x \in [0; k)$ one has $ax + b < ak + b < 2k^2 + 2k^2 = 4k^2$, so for each $i = 0; \dots, k_i - 1$ each line contains a point of P with $x = i \in \{0, 1, \dots, k\}$. Thus $I(L, P) \approx k^4 \approx n^{4/3}$ \square

3 Algebraic Geometry

Let f and g be two functions defined on some subset of the real numbers. One writes $g(x) = O(f(x))$ if and only if there exists a positive constant $C > 0$ such that $|g(x)| \leq C f(x)$ for all x .

Given a polynomial $f(x, y) = \sum_{i,j \leq 0} a_{i,j} x^i y^j$. The zero set Z_f of $f(x, y)$ is the subset of points (x, y) in \mathbb{R}^2 on which $f(x, y) = 0$. The polynomial $f(x, y)$ is of degree p ($\deg f = p$) if $p = \max\{i + j \mid a_{i,j} \neq 0\}$.

A polynomial $f(x, y)$ is called a *monomial* if $a_{i,j} = 1$ for exactly one pair (i, j) and $a_{i,j} = 0$ otherwise (roughly speaking, a polynomial which has only one term).

3.1. Consider $f(x, y)$ of degree d and an arbitrary line l . Prove that either $l \in Z_f$, or $|l \cap Z_f| \leq D$.

Proof. Writing l in parametric form $\{(u_1 t + v_1, u_2 t + v_2) \mid t \in \mathbb{R}\}$, we get that the points of $l \cap Z(f)$ are roots of the univariate polynomial $g(t) := f(u_1 t + v_1, u_2 t + v_2)$, which is of degree at most D . Thus, either g is identically 0, or it has at most D roots. \square

3.2. Consider a polynomial $f(x, y)$ of degree d . Prove that the number of distinct lines contained in the set Z_f does not exceed d .

Proof. We need to know that a nonzero bivariate polynomial (i.e., with at least one nonzero coefficient) does not vanish on all of \mathbb{R}^2 . Now we fix a point $P \in \mathbb{R}^2$ not belonging to $Z(f)$. Let us suppose that $Z(f)$ contains lines l_1, \dots, l_k . We choose another line l passing through P that is not parallel to any l_i and not passing through any of the intersections $l_i \cap l_j$. (Such an l exists since only finitely many directions need to be avoided.) Then l is not contained in $Z(f)$ and it has k intersections with $\cup_{i=1}^k l_i$. A result of the previous problem yields $k \leq D$. \square

3.3. Show that the number of bivariate monomials of degree at most d equals $\binom{d+2}{2}$.

Hint. In other words, we must find the number of pairs (i, j) of nonnegative integers with $i + j \leq D$.

Let P be a set of n points in the plane, and let r be a parameter, $1 < r \leq n$. We say that $f(x, y)$ is an *r-partitioning polynomial* for P if no connected component of $\mathbb{R}^2 \setminus Z_f$ contains more than n/r points of A .

In the sequel, we will sometimes call the connected components of $\mathbb{R}^2 \setminus Z(f)$ cells. Let us also stress that the cells are open sets. The points lying on $Z(f)$ do not belong to any cell.

3.4. For any $r > 1$, every finite point set admits an r -partitioning polynomial of degree at most r .

Hint. Construct r parallel lines dividing the given set into equal parts.

Definition. Given an arbitrary integer d , and let $D = \binom{d+2}{2} - 1$. A map $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^D$ is said to be the *Veronese map of degree d* if this map is given by the following formula:

$$\varphi(x,y) := (x^i y^j)_{(i,j) | 1 \leq i+j \leq d} \in \mathbb{R}^D.$$

(We think of the coordinates in \mathbb{R}^l as indexed by pairs (i,j) with $1 \leq i+j \leq D$.)

Note that we can apply the Veronese map of degree 2 to prove that any 5 points in the plane such that no 4 points are collinear uniquely determine a conic passing through the given points (A conic is a zero set of a bivariate polynomial of degree 2). In order to check it, we should consider an appropriate hyperplane containing the images of the given points under the Veronese map (We have $D=5$ in the considered case, and one can show that there exists a unique hyperplane on which all five images of the points lie). It is easy to check that the conic in the plane which corresponds the hyperplane is required.

3.5. Given finite sets A_1, \dots, A_k . Let k be an integer such that $\binom{k+2}{2} - 1 \geq l$. Prove that there exists a polynomial of degree at most k that is an l -partitioning polynomial for every one of these sets.

Proof. Problem 3.3 yields that $\binom{D+2}{2}$ is the number of monomials in a bivariate polynomial of degree at most D . We set $l := \binom{D+2}{2} - 1$, and we let $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^l$ denote the *Veronese map*, given by

$$\phi(x,y) := (x^i y^j)_{(i,j) | 1 \leq i+j \leq D} \in \mathbb{R}^l.$$

(We think of the coordinates in \mathbb{R}^l as indexed by pairs (i,j) with $1 \leq i+j \leq D$.)

We set $A'_i := \phi(A_i)$, $i = 1, 2, \dots, k$, and by ham sandwich theorem, we let h be a hyperplane simultaneously bisecting A'_1, \dots, A'_k . Then h has an equation of the form $a_{00} + \sum_{i,j} a_{i,j} z + i j = 0$, where $(z_{i,j})_{(i,j) | 1 \leq i+j \leq d}$ are the coordinates in \mathbb{R}^k . It is easy to check that $f(x,y) := \sum_{i,j} a_{i,j} x^i y^j$ is the desired polynomial (where here the sum includes a_{00} too). \square

3.6. For every $r > 1$, every finite point set $P \subset \mathbb{R}^2$ admits an r -partitioning polynomial f of degree at most $O(\sqrt{r})$.

Proof. We inductively construct collections $\mathcal{P}_0, \mathcal{P}_1, \dots$, each consisting of disjoint subsets of P , such that $|\mathcal{P}_j| \leq 2^j$ for each j . We start with $\mathcal{P}_0 := \{P\}$. Having constructed \mathcal{P}_j , we use the previous problem to construct a polynomial f_j , of degree $\deg(f_j) \leq \sqrt{2 \cdot 2^j}$, that bisects each of the sets of \mathcal{P}_j . Then for every subset $Q \in \mathcal{P}_j$, we let Q^+ consist of the points of Q at which $f_j > 0$, and let Q^- consist of the points of Q with $f_j < 0$, and we put $\mathcal{P}_{j+1} := \cup_{Q \in \mathcal{P}_j} \{Q^+, Q^-\}$.

Each of the sets in \mathcal{P}_j has a size at most $|P|/2^j$. We let $t = \lceil \log 2r \rceil$; then each of the sets in \mathcal{P}_t has a size at most $|P|/r$. We set $f := f_1 f_2 \dots f_t$. By the construction, no component of $\mathbb{R}^2 \setminus Z(f)$ can contain points of two different sets in \mathcal{P}_t , because any arc connecting a point in one subset to a point in another subset must contain a point at which one of the polynomials f_j vanishes, so the arc must cross $Z(f)$. Thus, f is an r -partitioning polynomial for P . It remains to bound the degree:

$$\deg(f) = \deg(f_1) + \deg(f_2) + \dots + \deg(f_t) \leq \sqrt{2} \sum_{j=1}^t 2^{j/2} \leq \frac{2}{\sqrt{2} - 1} 2^{t/2} \leq c\sqrt{r},$$

where $c = 2\sqrt{2}/(\sqrt{2} - 1) < 7$. □

4 The First Proof of the Szemerédi-Trotter Theorem

4.1. Prove that $I(m, n) = I(n, m)$.

Proof. Applying the polar transformation, lines are replaced by points and points are replaced by lines. Notice that a 'line-point' incidence enters to a 'point-line' incidence (as well as a line which has no incidence with a point goes to the point not incidence to the corresponding line). Thus, if we have a set of points and lines having $I(n, m)$ incidences, then we can transformate it to the set of points and lines, which has the same number of incidences. This yields $I(m, n) \geq I(n, m)$. Similarly, we can get the converse inequality. \square

If we apply a bound in the problem 1.8, then we will not get a proof of the Szemerédi-Trotter theorem immediately.

In what follows, we assume $|L| = |P| = n$. First of all, we construct an r -partitioning polynomial $f(x, y)$ of minimal degree for the given set P .

By $L_0 \subset L$ denote a subset of lines such that $l \in L$ and $l \subset Z_f$, by $P_0 \subset P$ denote a set of points $p \in P \cap Z_f$. Suppose Z_f divides the plane into s parts. By P_i denote points of P lying in the i -th part of the plane, and by L_i denote lines of \mathcal{L} passing through the i -th part of the plane.

4.2. Prove that there exist constants C_1, C_2, C_3 such that

- a) $I(L_0, P_0) \leq C_1 n \sqrt{r}$;
- b) $I(L \setminus L_0, P_0) \leq C_2 n \sqrt{r}$;
- c) $\sum_{i=1}^s I(L_i, P_i) \leq C_3 (n \sqrt{r} + n^2/r)$.

Proof. a) Since the number of distinct lines contained in Z_f is at most $\deg f \leq C_1 \sqrt{r}$, where C_1 is a certain constant (see problems **3.2** and **3.6**), and since the number of points in P_0 does not exceed n , then by trivial bound, we obtain $I(L_0, P_0) \leq C_1 n \sqrt{r}$.

b) Since each line of $L \setminus L_0$ intersects Z_f in at most $\deg f$ points, and since $\deg f \leq C_2 \sqrt{r}$, then $I(L \setminus L_0, P_0) \leq C_2 n \sqrt{r}$.

c) By the Problem **1.8 (a)** we get

$$\sum_{i=1}^s I(L_i, P_i) \leq \sum_{i=1}^s (|L_i| + |P_i|^2)$$

Let $D = \deg(f) = O(\sqrt{r})$. We have

$$\sum_{i=1}^s |L_i| = O((D + 1)n) = O(\sqrt{r}n),$$

since no line intersects more than $D + 1$ of the sets P_i . Finally,

$$\sum_{i=1}^s |P_i|^2 \leq (\max_i |P_i|) \cdot \sum_{i=1}^s |P_i| = O(n^2/r).$$

□

4.3. Having chosen a certain r , prove the Szemerédi-Trotter theorem.

Proof. Setting $r = n^{2/3}$, we obtain the proof of the Szemerédi-Trotter theorem for the case $n = m$. □

4.4. Prove the Szemerédi-Trotter theorem in the general case:

The Szemerédi-Trotter theorem. $I(n, m) = O((nm)^{2/3} + n + m)$.

Proof. We generalize the proof for an arbitrary m as follows. We may assume, without loss of generality, that $m \leq n$; the complementary case is handled by interchanging the roles of P and L , via a standard planar duality. We may also assume that $\sqrt{n} \leq m$, since otherwise, the theorem follows from Problem 1.8. Then we set $r := \frac{m^{4/3}}{n^{2/3}}$. Noting that $1 \leq r \leq m$ for the assumed range of m , we then proceed as in the case $m = n$ above. We get $D = \deg(f) = O(m^{2/3}n^{1/3})$, and we check that all the partial bounds in the proof are at most $O(m^{2/3}n^{2/3})$. □

5 Applications of the Szemerédi-Trotter Theorem

5.1. (a) Given a finite set P , $|P| = m$, in the plane. Prove that the number of lines passing through k distinct points of P is at most $C(m^2/k^3 + m/k)$, where C is some constant, which does not depend on m, k .

(b) Prove that such lines define at most $D(m^2/k^2 + m)$ incidences with P , where D is some constant, which does not depend on m, k .

5.2. Let P be a set of points in the plane and let L be the set of lines containing at least 2 points in P . Then there exist such $c_1, c_2 > 0$ that one of these two cases must hold:

1. There exists a line in L that contains at least $c_1|P|$ points.
2. $|L| > c_2|P|^2$.

5.3. Let $A \subset \mathbb{R}$ be a finite set. Then

$$\max\{|A + A|; |A \cdot A|\} \geq |A|^{5/4}.$$

Here

$$A + A = \{a_1 + a_2 : a_1 \in A, a_2 \in A\}, A \cdot A = \{a_1 \cdot a_2 : a_1 \in A, a_2 \in A\}.$$

Solutions. See [2], pp.15–17, [7].

References

- [1] *P. Brass, W. Moser, J. Pach* Research Problems in Discrete Geometry Springer, New York, 2005, Chapter 7.
- [2] *Zeev Dvir* Incidence Theorems and Their Applications, <http://www.cs.princeton.edu/~zdvir/papers/Dvir-survey.pdf>
- [3] *Jiri Matousek* Lectures on Discrete Geometry // Springer, 2002, Chapter 5.
- [4] *Jiri Matousek* Using the Borsuk-Ulam theorem // Springer, 2003.
- [5] *Haim Kaplan, Jiri Matousek, Micha Sharir* Simple Proofs of Classical Theorems in Discrete Geometry via the Guth–Katz Polynomial Partitioning Technique, <http://arxiv.org/abs/1102.5391v1>
- [6] *Endre Szemerédi, William T. Trotter* Extremal problems in discrete geometry, *Combinatorica* **3** (1983), 381–392
- [7] http://en.wikipedia.org/wiki/Szemerédi-Trotter_theorem