

ЛАТИНСКИ КВАДРАТИ И БЛОК ДИЗАЈНИ

4. БЛОК ДИЗАЈНИ

Дефиниција 5. Блок-дизајн е фамилија од b подмножества на множеството $S = \{x_1, x_2, \dots, x_n\}$ таква што да за секои k и λ важи:

а) секое подмножество има k елементи,

б) секој пар елементи од S се појавува во точно λ подмножества.

Подмножествата од множеството S ги нарекуваме *блокови*. Блоковите ќе ги означуваме со $B_1, B_2, \dots, B_b$. Матрицата на инциденција на блок-дизајнот $b \times v$ -матрицата $A = [a_{ij}]$ со елементи од множеството $\{0, 1\}$, чии редици соодветствуваат на блоковите, а колоните на елементите на множеството S , при што $a_{ij} = 1$ ако и само ако елементот x_j припаѓа на блокот B_i . Притоа, најчесто матрицата ќе ја запишуваме испишувајќи ги нејзините елементи во облик на таблица, без вообичаените загради.

Од условите а) и б) следува точноста на следнава теорема.

Теорема 6. Во блок-дизајнот секој елемент се појавува во точно r блокови, каде

$$r(k-1) = \lambda(v-1) \text{ и } bk = vr. \quad (1)$$

Доказ. Нека a е произволен елемент од S и да претпоставиме дека тој се појавува во r блокови. Секој од овие r блокови содржи $k-1$ елементи различни од a , па затоа бројот на парови елементи на блок-дизајнот кој го содржат a е еднаков на $r(k-1)$. Меѓутоа, постојат $v-1$ елементи со кои a може да биде во пар и секој пар се појавува λ пати. Според тоа,

$$r(k-1) = \lambda(v-1).$$

Но, k, v и λ се дадени броеви, па од последното равенство следува дека за секој елемент од S бројот r мора да е ист.

За најдената вредност r , секој елемент се појавува r -пати во блоковите, па затоа вкупниот број на појавувања на сите елементи е еднаков на vr . Но, секој од блоковите содржи k елементи и како имаме b блокови, добиваме дека бројот на појавувања на сите елементи е еднаков на bk . Значи, $bk = vr$. ♦

Забелешка 1. Имајќи ги предвид петте параметри кои ги карактеризираат блок-дизајните, често пати за блок-дизајн го користиме терминот (b, v, r, k, λ) -конфигурација.

Пример 7. Нека

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Следниве 12 множества формираат $(12, 9, 4, 3, 1)$ -конфигурација на S :

$$\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}, \{1, 5, 9\}, \{2, 6, 7\}, \\ \{3, 4, 8\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}. \quad \blacklozenge$$

Пример 8. Нека $S = \{1, 2, 3, 4, 5, 6, 7\}$. Да ги разгледаме следниве блокови на множеството S :

$$\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \\ \{5, 6, 1\}, \{6, 7, 2\}, \{7, 1, 3\}.$$

Овде важи $b = v = 7, k = 3$. Со испитување на сите парови лементи лесно се добива дека $\lambda = 1$ и дека овие блокови формираат $(7, 7, 3, 3, 1)$ – конфигурација со матрицата на инциденција

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} . \blacklozenge$$

Блок-дизајнот од претходниот пример има едно својство кое го немаат сите блок-дизајни. Имено, во случајот бројот на елементите е еднаков на бројот на блоковите, па затоа матрицата на инциденција е квадратна матрица. Ваквите дизајни ги нарекуваат *квадратни* или *симетрични дизајни* (што не значи дека матрицата на инциденција е симетрична). Притоа, за симетричната (b, v, r, k, λ) – конфигурација едноставно ќе велиме дека е (v, k, λ) – конфигурација.

Како што видовме, петте параметри на (b, v, r, k, λ) – конфигурацијата ги задоволуваат ограничувањата (1), т.е. тие не се независни. Меѓутоа, ако параметрите ги задоволуваат условите (1), тоа не значи дека постои соодветна конфигурација. Имено, не постои $(44, 43, 7, 7, 1)$ – конфигурација иако параметрите ги задоволуваат условите (1).

Теорема 7. Нека A е матрицата на инциденција на конфигурацијата (b, v, r, k, λ) , а A^T е нејзината транспонирана матрица. Тогаш

$$C = AA^T = (r - \lambda)E + \lambda I \quad (2)$$

каде E е единствената матрица од ред v , а I е $v \times v$ матрица чии елементи се еднакви на 1.

Доказ. Елементите во пресекот на i – та редица и j – та колона на матрицата A^T е $a'_{ij} = a_{ji}$. Елементот во пресекот на i – та редица и j – та колона на матрицата C е

$$c_{ij} = \sum_{h=1}^v a'_{ih} a_{hj} = \sum_{h=1}^v a_{hi} a_{hj}$$

за $i = j$ добиваме

$$c_{ii} = \sum_{h=1}^v a_{hi}^2 = \sum_{h=1}^v a_{hi}$$

бидејќи $a_{ij} = 0$ или 1, па $a_{ij}^2 = a_{ij}$. Меѓутоа, $a_{hi} = 1$ ако и само ако i – от елемент на множеството $S(x_i)$ е во h – от блок, а во спротивно $a_{hi} = 0$. Според тоа,

$$c_{ii} = \sum_{h=1}^v a_{hi}$$

е еднаков на бројот на блоковите кои содржат x_i , т.е.

$$\sum_{h=1}^v a_{hi} = r.$$

Ако $i \neq j$, тогаш

$$c_{ij} = \sum_{h=1}^v a_{hi} a_{hj}.$$

Меѓутоа, $a_{hi} a_{hj} = 1$ ако и само ако $a_{hi} = a_{hj} = 1$, т.е. ако и само ако h -от блок ги содржи и x_i и x_j . Ако искористиме дека постојат λ такви вредности h добиваме дека $c_{ij} = \lambda$, т.е.

$$C = A^T A = \begin{bmatrix} r & \lambda & \lambda & . & . & . & \lambda \\ \lambda & r & \lambda & . & . & . & \lambda \\ . & . & . & . & . & . & . \\ \lambda & \lambda & \lambda & . & . & . & r \end{bmatrix} \\ = (r - \lambda)E + \lambda I. \blacklozenge$$

Теорема 8. За секоја (b, v, r, k, λ) – конфигурација важи $b \geq v$.

Доказ. Нека претпоставиме дека за некоја конфигурација (b, v, r, k, λ) важи $b < v$. Матрицата на инциденција A тогаш има помалку редици од колони, па со додавање на $v - b$ редици на матрицата A добиваме квадратна матрица A_1 од ред v . Според претходната теорема, и за матрицата A_1 важи

$$A_1^T A_1 = (r - \lambda)E + \lambda I.$$

Бидејќи матрицата A_1 има барем една нулта редица, нејзината детерминанта е еднаква на нула, па затоа

$$\det(A_1^T A_1) = \det A_1^T \cdot \det A_1 = 0. \quad (3)$$

Меѓутоа, ако ја одземеме првата редица на матрицата $C = A_1^T A_1$ од сите редици, а потоа додавајќи го на првата колона збирот на останатите колони добиваме

$$A_1^T A_1 = \begin{bmatrix} r + \lambda(v - 1) & \lambda & \lambda & . & . & . & \lambda \\ 0 & r - \lambda & 0 & . & . & . & 0 \\ 0 & 0 & r - \lambda & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & r - \lambda \end{bmatrix}$$

од каде добиваме

$$\det(A_1^T A_1) = [r + \lambda(v - 1)](r - \lambda)^{v-1} = rk(r - \lambda)^{v-1}.$$

Понатаму, од (1) следува $r > \lambda$ па затоа

$$\det(A_1^T A_1) \neq 0$$

што противречи на (3). Од добиената противречност следува $b \geq v$. $\blacklozenge$

5. МАТРИЦИ НА АДАМАР

Дефиниција 6. Матрицата на Адамар од ред $n \times n$ ја нарекуваме матрица H со елементи од множеството $\{-1, 1\}$, за која важи

$$HH^T = nE$$

каде E е единечната матрица од ред n .

Коментар 1. Од претходната дефиниција следува дека скаларниот производ на две различни редици на матрицата H е еднаков на O , т.е. секои две различни редици се заемно ортогонални. Понатаму, производот на секој редица со самата себе е n . Бидејќи

$$H^{-1} = \frac{1}{n} H^T,$$

добиваме дека

$$H^T H = nE \text{ ,}$$

т.е. и колоните на N го имаат наведеното својство.

Лесно се покажува дека со множење на произволна редица или колона на H со -1 се добива нова матрица на Адамар. На овој начин може да се постигне сите елементи во првата редица и првата колона да бидат еднакви на 1. За ваквата матрица на Адамар ќе велиме дека е *нормализирана*. Подолу се дадени нормализирани матрици на Адамар од ред 1, 2, 4 и 8.

$$\begin{array}{cccccccc}
& & & & 1 & 1 & 1 & 1 \\
1 & & 1 & 1 & 1 & -1 & 1 & -1 \\
& & 1 & -1 & 1 & 1 & -1 & -1 \\
& & & & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1
\end{array}$$

Шема 1

Теорема 9. Ако постои матрица на Адамар од ред n , тогаш $n = 1$, $n = 2$ или $n = 4m$ за некој природен број m . Притоа, за $n > 2$ во секоја редица, освен во првата, на нормализираната матрица на Адамар има ист број елементи 1 и -1 .

Доказ. Матриците на Адамар од ред 1 и 2 се дадени во шема 1. Нека претпоставиме дека за $n > 2$ постои нормализирана матрица на Адамар од n -ти ред. Во првата редица сите елементи се еднакви на 1, па затоа во втората редица мора да има $\frac{n}{2}$ елементи 1 и исто толку елементи -1. Понатаму колоните може да ги пермутираме така да на првите $\frac{n}{2}$ места на втората редица имаме 1. Сега да ја разгледаме третата редица. Нека меѓу првите $\frac{n}{2}$ елементи на оваа редица има a

единици, а меѓу останатите $\frac{n}{2}$ елементи има b единици. Бидејќи првата и третата редица се ортогонални добиваме

$$a + b = \frac{n}{2} \quad (1)$$

Понатаму, бидејќи втората и третата редица се ортогонални добиваме

$$a - (\frac{n}{2} - a) - b + (\frac{n}{2} - b) = 0,$$

т.е.

$$a - b = 0 \quad (2)$$

Од (1) и (2) следува $a = b = \frac{n}{2}$, т.е.

$$n = 2(a + b) = 4a. \quad \blacklozenge$$

Забелешка 2. Постои хипотеза дека за секој број n делив со 4 постои матрица на Адамар од ред n , која не е докажана. Меѓутоа, од секоја матрица на Адамар, може да се добие нова матрица на Адамар со двапати поголем ред.

Теорема 10. Ако постои матрица на Адамар од ред n , тогаш постои и матрица на Адамар од ред $2n$.

Доказ. За матрицата на Адамар H од ред n ја дефинираме матрицата

$$K = \begin{bmatrix} H & H \\ H & -H \end{bmatrix}.$$

Ќе покажеме дека K е матрица на Адамар.

Бидејќи сите елементи на матрицата K се еднакви на 1 или -1, останува да докажеме дека

$$KK^T = 2nE.$$

Навистина, секоја редица на матрицата K (освен првата) содржи по n елементи 1 и -1. Значи, со множење добиваме дека сите дијагонални елементи на матрицата KK^T се еднакви на $2n$. Конечно, од ортогоналноста на редовите на матрицата H следува ортогоналноста на матрицата K . $\blacklozenge$

Забелешка 3. Матриците на шемата 1 се добиени последователно една од друга со конструкција од претходната теорема. Да забележиме дека матрицата од ред 2^n која поаѓајќи од тривијалната матрица од ред 1, се добива со конструкцијата од теоремата 10 ја нарекуваме матрица на Силвестер.

Понатаму, секоја матрица на Адамер ни дава еден симетричен блок-дизајн, што е последица од следново тврдење.

Теорема 11. Ако постои матрица на Адамар од ред $n = 4m \geq 8$, тогаш постои и $(4m-1, 2m-1, m-1)$ – конфигурација.

Доказ. Нека A е нормализирана матрица на Адамар од $n = 4m \geq 8$. Да ја отстраниме првата редица и првата колона на матрицата A , а во преостанатиот дел секаде да го замениме -1 со 0. Добиената матрица B од ред $4m-1$ во секоја редица има $2m-1$ единици и $2m$ нули, а за секои две различни редици постојат точно $m-1$ колони во кои двете редици имаат единици. Според тоа,

$$BB^T = mE + (m-1)I,$$

од каде следува теоремата. $\blacklozenge$

Пример 9. На опишаниот начин во доказот на претходната теорема од матрицата на Адамар од ред 8 (шема 1), ја добиваме $(7, 3, 1)$ – конфигурацијата со следнава матрица на инцидентција

0	1	0	1	0	1	0
1	0	0	1	1	0	0
0	0	1	1	0	0	1
1	1	1	0	0	0	0
0	1	0	0	1	0	1
1	0	0	0	0	1	1
0	0	1	0	1	1	0

Задачи за самостојна работа

1. Докажи дека не постои латински квадрат ортогонален на латинскиот квадрат

1	2	3	0
2	3	0	1
3	0	1	2
0	1	2	3

2. Пробните пилоти Александар, Бошко, Владо, Гане и Данило (накратко А,Б,В,Г и Д) во текот во текот на пет денови испитувале пет типови авиони: A, B, C, D и E . Секој пилот летал секој ден на авион од друг тип, така што во текот на петте денови ги испробал сите пет типови авиони. Првиот ден Гане летал на авионот A , вториот ден Владо летал на авионот B , третиот ден Владо летал на авионот C , а Данило на авионот B и четвртиот ден Александар летал на авионот A , а Гане на авионот D .

а) На кој авион летал Александар првиот ден?

б) Кој пилот управувал со авионот D вториот ден?

3. На колку начини латинскиот 2×5 правоаголник

1	2	3	4	5
2	3	4	5	1

може да се прошири за еден ред?

4. На колку начини латинскиот $(n-1) \times n$ – правоаголник може да се прошири до латински квадрат?

5. Докажи дека се изотопни латинските квадрати

0	1	2	0	2	1	
1	2	0	и	2	1	0
2	0	1	1	0	2	

6. а) Докажи дека се изотопни латинските квадрати

1	2	3	4	5	3	1	4	5	2	
2	3	4	5	1	1	2	3	4	5	
3	4	5	1	2	и	4	3	5	2	1
4	5	1	2	3	5	4	2	1	3	
5	1	2	3	4	2	5	1	3	4	

- б) Докажи дека се изотопни латинските квадрати

1	2	3	4	5		5	3	4	1	2
2	3	4	5	1		3	1	2	4	5
3	4	5	1	2	и	4	2	3	5	1.
4	5	1	2	3		1	4	5	2	3
5	1	2	3	4		2	5	1	3	4

7. Нека со цртеж 2 е дадена таблица 5×5 при што во некои полиња се изпишани броеви од множеството $\{1, 2, 3, 4, 5\}$, така да во секоја редица и секоја колона запишаните броеви се различни

2	1			
			3	4
				3
1				

цртеж 2

На колку начини оваа таблица може да се дополни до латински квадрат.

8. Докажи дека таблицата од цртеж 3 не може да се пополни до латински квадрат со елементите $\{1, 2, 3, 4, 5\}$. Но, ако во долниот десен агол се избрише елементот 3 се добива таблица која еднозначно може да се дополни до латински квадрат

	4			1
2		3		
		2		
	1			3

цртеж 3

9. На колку различни начини латинскиот 2×4 правоаголници

а) $\begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{matrix}$

б) $\begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{matrix}$

може да се прошират до латински квадрати?

10. Докажете дека не постои $(18, 8, 3, 2, 1)$ – конфигурација.
11. Најди го збирот на сите елементи во нормализираната матрица на Адамар од ред n .
12. Нека A е матрица на Адамар од ред n . Докажи дека $|\det A| = n^{\frac{n}{2}}$.
13. Докажи дека ако постојат матриците на Адамар од ред 16 и 20, тогаш постои бинарен $(35, 32, 17)$ – код.