Вера Малческа, Кајзерслаутерн, Германија
Самоил Малчески, Скопје

ЛАТИНСКИ КВАДРАТИ И БЛОК ДИЗАЈНИ 1

Во оваа работа ќе ги рзгледаме таканаречените латински квадрати, кои имаат огромна примена како во информатиката, така и во други научни дисциплини. За таа цел прво накратко ќе се осврнеме на поимот матрица.

Дефиниција 1. Нека $\mathbf{R}$ е множеството реални броеви. Таблицата

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix} \qquad (1)$$

каде $a_{ij} \in \mathbf{R},\ i=1,2,...,n;\ j=1,2,...,m$ ја нарекуваме *матрица од ред* $n \times m$ над полето $\mathbf{R}$. Броевите $a_{ij},\ i=1,2,...,n;\ j=1,2,...,m$ ги нарекуваме *елементи на матрицата* (1). Редот

$$a_{i1}\ \ a_{i2}\ \ \dots\ \ a_{im}$$

го нарекуваме $i-$*ти ред на матрицата* (1), а колоната

$$\begin{matrix} a_{1j} \\ a_{2j} \\ \dots \\ a_{nj} \end{matrix}$$

ја нарекуваме $j-$*та колона на матрицата* (1).

За означување на матрицата (1) ќе ја користиме и ознаката $[a_{ij}]_{n\times m}$. Ако $n=m$, тогаш ќе велиме дека матрицата (1) е *квадратна* и притоа ќе ја користиме ознаката $[a_{ij}]_{n\times n}$.

Пример 1. Матрицата $\begin{bmatrix} 1 & 2 & 3 & 2 \\ 1 & 1 & 3 & -3 \end{bmatrix}$ е од ред 2×4. Притоа $\begin{matrix} 2 \\ 1 \end{matrix}$ е нејзина втора колона, а $1\ \ 1\ \ 3\ \ -3$ е нејзина втора редица. ♦

Дефиниција 2. За матриците $[a_{ij}]_{n\times m}$ и $[b_{ij}]_{k\times l}$ ќе велиме дека се *еднакви* ако се од ист ред, т.е. $n=k,\ m=l$ и $a_{ij}=b_{ij}$, за $i=1,2,...,n,\ j=1,2,...,m$.

Пример 2. Матриците

$$A=\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix} \text{ и } B=\begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}$$

не се еднакви, бидејќи $a_{22}=2\neq 1=b_{22}$.

1. ПОИМ ЗА ЛАТИНСКИ КВАДРАТ

Дефиниција 3. Нека Q е множество од n елементи. Матрицата елементи од Q ја нарекуваме *латински* $r\times n-$ *правоаголник* ако во секој нејзин ред и во секоја нејзина колона сите елементи се различни меѓу себе.

Латинскиот $n\times n$ правоаголник го нарекуваме *латински квадрат* од $n-$ти ред.

Од дефиницијата 3 непосредно следува $r<n$. Јасно, елементите на секоја редица на латинскиот правоаголник формираат една пермутација на елементите од Q, а елементите на секоја колона формираат варијација без повторување од $r-$ти ред.

Во натамошните разгледувања за елементите на множеството Q ќе ги земеме првите n природни броеви.

Теорема 1. За секој природен број постои латински квадрат од $n-$ти ред.

Доказ. Да ја разгледаме матрицата $M=[a_{ij}]$ за која $a_{ij}\equiv i+j(\mathrm{mod} n)$, $0\leq a_{ij}\leq n-1$. Ако $a_{ij}=a_{ik}$, тогаш $i+j\equiv i+k(\mathrm{mod}\, n)$, од каде после скратувањето добиваме дека $j\equiv k(\mathrm{mod}\, n)$, што значи $j=k$, бидејќи j и k се ненегативни броеви помали од n. Слично, од $a_{ij}=a_{kj}$ следува $i=k$. Според тоа, елементите на секој ред (колона) се различни, па M е латински квадрат. ♦

Последица 1. За произволни природни броеви n и r, $r<n$ постои латински $r\times n-$ правоаголник.

Доказ. Непосредно следува од фактот дека со отстранувањето на произволен број редици од латинскиот квадрат се добива латински правоаголник. ♦

Пример 3. Ако ја искористиме теорема 1, за $n=4$ имаме

$a_{11}\equiv 1+1(\mathrm{mod}\,4)$, т.е. $a_{11}=2$, $a_{21}\equiv 2+1(\mathrm{mod}\,4)$, т.е. $a_{21}=3$,

$$a_{44}\equiv 4+4(\mathrm{mod}\,4), \text{ т.е. } a_{44}=0 \text{ итн.}$$

Според тоа го добиваме латинскиот квадрат од ред 4

$$M=\begin{bmatrix}2&3&0&1\\3&0&1&2\\0&1&2&3\\1&2&3&0\end{bmatrix}. \ \blacklozenge$$

Да зебележиме дека со пермутирање на редовите (колоните) на произволен латински правоаголник (квадрат) се добива латински правоаголник (квадрат). Исто така, со пермутирање на елементите на множеството Q, т.е. со нивно преименување, од латински квадрат се добива латински квадрат. Притоа се подразбира дека еднаквите елементи во целиот латински квадрат ги заменуваме со еднакви елементи, согласно извршената пермутација на елементите од Q.

За латинските квадрати кои еден од друг можат да се добијат со пермутирање на редиците, колоните или преименување на елементите ќе велиме дека се *изотопни*.

Во натамошните разгледувања ќе сметаме дека множеството Q е подредено. Ако елементите на Q се природни или цели броеви, тогаш го земаме основното подредување <. Ако елементите на Q ги земеме во растечки редослед, тогаш добиената пермутација ја нарекуваме *основна*. За буквите под *основната* пермутација ќе ја подразбираме пермутацијата која е согласна со нивните лексикографски поредок во соодветната азбука.

За латинскиот квадрат ќе велиме дека е *стандарден* ако елементите на првиот ред се во основен поредок (основна пермутација).

Јасно, секој латински квадрат може, со пермутирање на колоните да се доведе до стандарден.

За латинскиот квадрат ќе велиме дека е *двојностандарден* ако и елементите на првиот ред и елементите на првата колона се во основен поредок.

Јасно, со пермутирање на редиците и пермутирање на колоните секој латински квадрат може да се сведе на двојно стандарден. Меѓутоа, ова не може да се постигне со пермутирање на елементите.

За два латински квадрати $A=[a_{ij}]$ и $B=[b_{ij}]$ ќе велиме дека се *еднакви* ако

$$a_{ij}=b_{ij}, \text{ за } i,j\in\{1,2,3,...,n\}.$$

Со $l_{ss}(n)$ да го означиме бројот на неизотопните латински квадрати од ред n, т.е. бројот на различните двојностандардни латински квадрати од ред n

. Овој број со зголемувањето на n расте многу брзо и за првите 9 природни броеви вредностите на $l_{ss}(n)$ се дадени во следнава табела.

n	$l_{ss}(n)$
1	1
2	1
3	1
4	4
5	56
6	9408
7	169 942 080
8	535 281 401 856
9	377 597 570 964 258 816

2. ПРОШИРУВАЊЕ НА ЛАТИНСКИ КВАДРАТИ

Со остранување на произволен ред од латинскиот $r\times n-$правоаголник, $1<r\leq n$, се добива ларински $(r-1)\times n-$правоаголник. Се поставува обратното прашање, дали може секој латински $r\times n-$правоаголник, $r<n$со додавање на еден ред да се прошири до латински $(r+1)\times n-$правоаголник. Одговорот на ова прашање е потврден, т.е. важи следнава теорема која ќе ја прифатиме без доказ.

Теорема 2. Ако $r<n$, тогаш секој латински $r\times n-$правоаголник може да се прошири до латински $(r+1)\times n-$правоаголник. ♦

Пример 4. Даден е латински $3\times 6-$ правоаголник

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 3 & 5 & 1 & 0 & 4 \\ 5 & 4 & 0 & 2 & 3 & 1 \end{bmatrix}$$

Со $S_j, j=1,2,3,4,5,6$ да го означиме подмножеството елементи $Q=\{0,1,2,3,4,5\}$ кои не се појавуваат во $j-$та колона. Имаме

$S_1=\{0,3,4\}$, $S_2=\{0,1,5\}$, $S_3=\{1,2,4\}$, $S_4=\{0,3,5\}$, $S_5=\{1,2,4\}$, $S_6=\{2,3,5\}$

Од овие множества избираме по еден преставник, но така да сите се различни меѓу себе, т.е

$$0\in S_1,\ 1\in S_2,\ 2\in S_3,\ 3\in S_4,\ 4\in S_5 \text{ и } 5\in S_6.$$

На дадениот латински $3\times 6-$правоаголник му допишуваме редица, така што последователно ги запишуваме најдените преставници и го добиваме латинскиот $4\times 6-$правоаголник:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 3 & 5 & 1 & 0 & 4 \\ 5 & 4 & 0 & 2 & 3 & 1 \\ 0 & 1 & 2 & 3 & 4 & 6 \end{bmatrix}. \ \blacklozenge$$

Последица 2. Секој латински правоаголник може да се прошири до латински квадрат.

Доказ. Непосредно следува од теорема 2. ♦

3. ОРТОГОНАЛНОСТ НА ЛАТИНСКИ КВАДРАТИ

Дефиниција 4. За два латински квадрати $A=[a_{ij}]$ и $B=[b_{ij}]$ од $n-$ти ред ќе велиме дека се *заемно ортогонални*, ако сите n^2 подредени парови (a_{ij},b_{ij}) се различни меѓу себе.

Во случајот велиме дека со преклопување на два заемно ортогонални латински квадрати од $n-$ти ред се добиваат n^2 различни подредени парови.

Пример 5. Со преклопување на латинските квадрати

$$\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix} \text{ и } \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

се добива шема која содржи 16 различни подредени парови

$$\begin{bmatrix} a1 & b2 & c3 & d4 \\ b3 & a4 & d1 & c2 \\ c4 & d3 & a2 & b1 \\ d2 & c1 & b4 & a2 \end{bmatrix}. \ \blacklozenge$$

Разгледувајќи ги ортогоналните латински квадрати од $n-$ред, најчесто ќе земеме дека елементите на секој квадрат се од множеството $Q=\{0,1,2,...,n-1\}$. Јасно, секој подреден пар $(x,y)\in Q^2$ се појавува точно еднаш како пар на соодветните елементи (a_{ij},b_{ij}) на заемно ортогоналните квадрати. Понатаму, лесно се гледа дека два двоструко стандардни латински квадрати од ред n не можат да бидат ортогонални.

Нека се A и B заемно ортогонални латински квадрати. Лесно се гледа дека со истовремено пермутирање на соодветните редици (колони) во двата квадрати се добиваат латински квадрати кои исто така се ортогонални. Исто така, со преименување на елементите на множеството Q во еден од квадратите на ортогоналниот пар (но така да сите елементи се различно означени, нивно пермутирање) ортогоналноста се запазува. Последното е точно и кога имаме повеќе латински квадрати кои по парови се заемно ортогонални.

Теорема 3. Нека $L_1, L_2, ..., L_k$ се по парови заемно ортогонални латински квадрати. Тогаш постојат латински квадрати $L_1^{'}, L_2^{'}, ..., L_k^{'}$ кои се изотопни на дадените, стандардни и по парови заемно ортогонални.

Доказ. Без ограничување на општоста, можеме да претпоставиме дека елементите на сите квадрати се од множеството $Q = \{0,1,2,...,n-1\}$. За секој квадрат $L_i, i \in \{1,2,...,k\}$ треба елементите на Q да ги преименуваме така да од L_i се добие стандарден квадрат $L_i^{'}$. Од претходните разгледувања следува дека добиените квадрати се по парови ортогонални. ♦

Теорема 4. За секој природен број $n > 1$ постојат најмногу $n-1$ заемно ортогонални латински квадрати.

Доказ. Согласно претходната теорема, можеме да се ограничиме на разгледување само на стандардните латински квадрати со елементи од $Q = \{0,1,2,...,n-1\}$. Да го разгледаме полето во пресекот на втората редица и првата колона на секој квадрат. Во ова поле не може да се наоѓа елементот 0. Од друга страна, секои два стандардни заемно ортогонални квадрати мораат во тоа поле да имаат два различни елементи. Значи, во множеството по парови ортогонални латински квадрати од ред n не може да има повеќе од $n-1$ квадрат. ♦

За множеството од $n-1$ по парови ортогонални латински квадрати од ред n велиме дека е потполн систем ортогонални латински квадрати од ред n (скратено ПСОЛК(n)).

Може да се докаже дека ПСОЛК(n) постои за $n = p^k$ каде p е прост број. За сега се познати само такви системи. Во следната теорема ќе го презентираме доказот во случај кога $k = 1$, т.е. кога n е прост број. Во доказот ќе го користиме фактот дека зе секој прост број p множеството остатоци по модул p е поле во однос на операциите собирање и множење по модул p.

Теорема 5. За секој прост број p постои ПСОЛК(p).

Доказ. Да ги разгледаме $p-1$ матриците од ред $p\times p$ со елементите од множеството $Q=\{0,1,2,...,p-1\}: L_k=[a_{ij}^k], k=1,2,...,p-1$ каде $a_{ij}^k \equiv i+kj(\mathrm{mod}\, p)$.

Прво ќе докажеме дека за $k=1,2,...p-1$ матрицата L_k е латински квадрат. Навистина, ако за L_k важи $a_{ij_1}^k=a_{ij_2}^k$, тогаш во полето на остатоци по модул p важи $i+kj_1=i+kj_2$. Бидејќи во полето важи законот за кратење на двете операции добиваме: $kj_1=kj_2$ т.е. $j_1=j_2$. Значи, на две различни места во иста редица не може да има исти броеви. Слично се докажува дека на две различни места во една колона не може да има исти броеви, па значи L_k е латински квадрат. Нека сега L_t и L_s, $t\neq s$ се два латински квадрати добиени на опишаниот начин и нека $x=a_{ij}^t, y=a_{ij}^s$ т.е. во полето остатоци по модул p важи $x=i+tj, y=i+sj$. Тогаш $(t-s)j=x-y$, па затоа $j=(t-s)^{-1}(x-y)$ Според тоа, i и j се еднозначно определени за дадени x,y,t и s. Затоа секој пар (x,y) само еднаш се појавува како пар на соодветните елементи (a_{ij}^t,a_{ij}^s) во латинските квадрати L_t и L_s, $t\neq s$. ♦

Пример 6. Со примена на постапката од доказот на теорема 3.7 се добива ПСОЛК(5), кој се состои од следните четири квадрати:

$$\begin{bmatrix}2&3&4&0&1\\3&4&0&1&2\\4&0&1&2&3\\0&1&2&3&4\\1&2&3&4&0\end{bmatrix}, \quad \begin{bmatrix}3&0&2&4&1\\4&1&3&0&2\\0&2&4&1&3\\1&3&0&2&4\\2&4&1&3&0\end{bmatrix},$$

$$\begin{bmatrix}4&2&0&3&1\\0&3&1&4&2\\1&4&2&0&3\\2&0&3&1&4\\3&1&4&2&0\end{bmatrix} \text{ и } \begin{bmatrix}0&4&3&2&1\\1&0&4&3&2\\2&1&0&4&3\\3&2&1&0&4\\4&3&2&1&0\end{bmatrix}. \ ♦$$

Статијата прв пат е објавена во списанието СИГМА на СММ