Математичка гимназија

Матурски рад
из математике

Ортогоналност латинских квадрата

Ученик
Ђорђе Томић, IVд

Ментор
др Соња Чукић

Београд, 27. мај 2024. године

Садржај

Увод **1**

1 Уводни појмови **3**

2 Ортогоналност латинских квадрата **5**

2.1 Парови ортогоналних латинских квадрата 6

2.2 Комплетан скуп МОЛК-а 13

2.2.1 Афине и пројективне равни 13

2.2.2 Афина раван и комплетан скуп МОЛК 16

2.3 Ограничење максималног броја МОЛК-а 22

2.4 Примена 23

Закључак **25**

Литература **27**

Увод

Приликом играња карата, нама непозната особа се досетила да оне „најјаче” у игри распореди на следећи начин:

A♣	Q♠	J♦	K♥
K♦	J♥	Q♣	A♠
Q♥	A♦	K♠	J♣
J♠	K♣	A♥	Q♦

На први поглед ништа необично, али ако се боље загледамо примећујемо да се у свакој врсти и свакој колони појављује свака од четири вредности и сваки од четири знака наших карата.
У математици се оваква конфигурација назива *Ојлеров квадрат* (у овом случају реда четири), добивши име по чувеном швајцарском математичару Леонарду Ојлеру (1707–1783).

Можда Ојлер није играо карте, али је увелико изучавао овакве типове уређености квадрата $n \times n$, и поставио претпоставку чију ће тачност желети да испитају многи велики математичари после њега.

1

Уводни појмови

Латински квадрат реда n представља квадрат димензија $n \times n$ попуњен са n различитих објеката, при чему не постоји врста или колона у којој се налазе два иста објекта.

Објекти у овом случају могу бити било које ствари из реалног живота, попут боја, титула, занимања, међутим у овом раду ћемо се фокустирати на скуп ненегативних целих бројева којим попуњавамо дати латински квадрат.

Дефиниција 1.1. Латински квадрат реда n представља квадрат димензија $n \times n$ попуњен бројевима из скупа $N = \{a_1, a_2, \ldots, a_n\}$, тако да не постоји врста или колона у којој се налазе два иста броја.

Навешћемо једно од основних својстава латинских квадрата, које ће нам бити потребно за касније:

Лема 1.1. Нека је дат латински квадрат L реда n попуњен бројевима из скупа $N = \{a_1, a_2, \ldots, a_n\}$. Било којом пермутацијом σ бројева скупа N, $\sigma : N \to N$, добија се нов квадрат $\sigma(L)$ који је такође латински.

Доказ. Претпоставимо супротно, да у квадрату $\sigma(L)$ постоје два иста броја a_j у некој врсти или колони, при чему је $\sigma(a_i) = a_j$. Пошто је пермутација σ бијекција, то би значило да се и у квадрату L два броја a_i налазе у истој врсти или колони. Контрадикција. $\square$

2

Ортогоналност латинских квадрата

Дефиниција 2.1. Нека су $A = (a_{ij})$ и $B = (b_{ij})$ два латинска квадрата реда n ($i, j \in \{1, 2, \ldots, n\}$). Тада се квадрат димензија $n \times n$, у чијем се пољу (i, j) налази уређени пар (a_{ij}, b_{ij}), означен са (A, B), назива *Ојлеров квадрат* уколико се сваки уређени пар бројева, којих има n^2, јавља тачно једном.

Латински квадрати A и B који заједно граде Ојлеров квадрат називају се *пар ортогоналних латинских квадрата.*

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

(1,1)	(2,2)	(3,3)
(2,3)	(3,1)	(1,2)
(3,2)	(1,3)	(2,1)

Пример Ојлеровог квадрата из два латинска квадрата реда 3

Навешћемо једно својство пара ортогоналних латинских квадрата које ће нам бити потребно касније у једном доказу:

Лема 2.1. Нека је дат пар ортогоналних латинских квадрата A и B. Применом било које пермутације σ на скупу којим попуњавамо дате латинске квадрате, над само једним од датих латинских квадрата, очувава се међусобна ортогоналност постојећег и новонасталог латинског квадрата. (Уколико пермутацију примењујемо на оба квадрата, тврђење је јасно.)

Доказ. Да је новонастали квадрат добијен пермутацијом σ остао латински показује нам лема 1.1. Нека је, без умањења општости, пермутација извршена над квадратом B. Претпоставимо да квадрат $(A, \sigma(B))$ није Ојлеров, то јест да се неки уређени пар (a, b_2) јавља два пута, при чему је $\sigma(b_1) = b2$. Међутим, тада би се и у квадрату (A, B) на тим местима уређени пар (a, b_1) јављао два пута, те то не би био Ојлеров квадрат, односно A и B не би били пар ортогоналних латинских квадрата. Контрадикција. □

2.1 Парови ортогоналних латинских квадрата

Године 1779. Леонард Ојлер је истраживао ортогоналне латинске квадрате и покушавао да нађе пар ортогоналних латинских квадрата сваког реда. У његовом раду из 1779. године, који је објављен 1782, Ојлер је знао да конструише Ојлеров квадрат сваког реда n, где је n или непаран број или дељив са 4. Дакле, успео је да докаже постојање Ојлеровог квадрата за свако $n \equiv 0, 1, 3 \pmod 4$. Једини случај који је остао неразрешен јесте $n \equiv 2 \pmod 4$. Ово нас доводи до случаја који је посебно разматрао, а који је поставио као математичку загонетку под називом *Проблем 36 официра*:

„Постоји 36 војних официра, из сваког од 6 различитих пукова и са сваким од 6 различитих чинова, при чему не постоје два официра из истог пука и са истим чином. Да ли је могуће распоредити ових 36 официра у квадратни распоред 6×6 тако да се сваки пук и сваки чин појављују у сваком реду и свакој колони?"

Уколико би одговор на постављено питање био потврдан, јасно је да би он заправо представљао Ојлеров квадрат реда 6. Сам Ојлер је тражио одговор на ово питање, те како није успео, нити да изведе конструкцију, нити да докаже супротно, генерализовао је проблем и поставио следећу претпоставку:

Ојлерова претпоставка: Не постоји пар ортогоналних латинских квадрата реда n, где је $n \equiv 2 \pmod 4$.

После много времена, први који је направио успешан помак у решавању проблема 36 официра је француски математичар Гатсон Тари, који је 1900. године доказао непостојање пара ортогоналних латинских квадрата реда 6, исцрпном ручном претрагом делећи латинске квадрате реда 6 на одређене подгрупе ([8]). Касније су други математичари дали краће доказе примењујући знања из компликованијих области математике ([9]).
Примећујемо међутим да овиме Ојлерова претпоставка још увек није оповргнута, напротив, остала је још безмало шест деценија као проблем међу математичарима

Први резултат који изазива озбиљну сумњу у истинитост Ојлерове претпоставке су извели индијски математичари Рај Чандра Бозе и Шараџандра Шанкар Шриканде, који су 1959. године конструисали Ојлеров квадрат реда 22. Исте године, амерички математичар Ернест Тилден Паркер је, доказујући другу теорему, добио пар ортогоналних латинских квадрата реда 10. Приликом налажења Ојлеровог квадрата реда 10, Паркер је користио UNIVAC компјутер и то се сматра једним од првих покушаја коришћења компјутера у сврху решавања комбинаторног проблема.
Како су пронађени Ојлерови квадрати реда 10 и 22, а и 10 и 22 су конгруентни са 2 по модулу 4, више није било икакве сумње да Ојлерова претпоставка није тачна.

Штавише ова три математичара су извели доказ којим су у потпуности оповргли Ојлерову претпоставку и доказали да постоји барем један пар међусобно ортогоналних латинских квадрата реда n, где је $n \equiv 2 \pmod 4$ и $n \neq 6$. Метод који су они између осталог користили у доказу је познат као балансирани непотпуни блок дизајни, чије су варијације биле познате и раније математичарима, међутим они су први који су успели да их добро изуче и повежу са темом ортогоналности латинских квадрата.

Коначни резултат Бозеа, Шрикандеа и Паркера о нетачности Ојлерове претпоставке био је објављен на годишњем састанку Америчког друштва математичара, одржаном у Њујорку током последње недеље априла 1959. године. Ово велико математичко постигнуће објављено је и на насловној страни недељног издања Њујорк тајмса од 26. априла 1959. године са насловом:

„Велика математичка претпоставка објављена пре 177 година је одбачена.”

Њујорк тајмс је такође навео да су тројица математичара који су коначно оповргли претпоствку међу својим колегама познати као „Euler's spoilers”.

Систематизујући доказе које су извели Ојлер и велика тројица имамо важну теорему:

Теорема 2.1. За сваки природан број $n > 2$, $n \neq 6$, постоји пар ортогоналних латинских квадрата реда n.

Кренимо сада путевима Леонарда Ојлера и потоњих математичара и уверимо се у постојање одређених парова ортогоналних латинских квадрата.

Теорема 2.2. Постоји пар ортогоналних латинских квадрата реда n где је n непаран број.

Доказ. Као доказ наводимо конструкцију при којој је у сваком пољу (i, j) $(0 \leqslant i, j \leqslant n-1)$ првог латинског квадрата L_1 уписан број $i + j$, а у сваком пољу (i, j) другог латинског квадрата L_2 уписан број $2i + j$, при чему добијене вредности посматрамо по модулу n.

0	$\cdots$	j	$\cdots$	$n-1$
$\vdots$		$\vdots$		$\vdots$
i	$\cdots$	$i+j$	$\cdots$	$n+i-1$
$\vdots$		$\vdots$		$\vdots$
$n-1$	$\cdots$	$n+j-1$	$\cdots$	$2n-1$

0	$\cdots$	j	$\cdots$	$n-1$
$\vdots$		$\vdots$		$\vdots$
$2i$	$\cdots$	$2i+j$	$\cdots$	$n+2i-1$
$\vdots$		$\vdots$		$\vdots$
$n-1$	$\cdots$	$2n+j-2$	$\cdots$	$3n-3$

Латински квадрати L_1 и L_2

За почетак тврдимо да су оба квадрата латинска. Наиме, уколико би вредности у пољима (i, j_1) и (i, j_2) латинског квадрата L_1 у реду i биле једнаке, тада би морало да важи $i + j_1 \equiv i + j_2 \pmod{n}$, односно $j_1 \equiv j_2$, што је по конструкцији немогуће ($j_1 \neq j_2$). Аналогно се доказује непостојање два иста броја и у колони латинског квадрата L_1, а и у реду латинског квадрата L_2. Када би се у колони j латинског квадрата L_2 налазиле две исте вредности у пољима (i_1, j) и (i_2, j) тада би важило $2i_1 + j \equiv 2i_2 + j \pmod{n}$ односно $2i_1 \equiv 2i_2$, а пошто је n непаран број, морало би да важи $i_1 \equiv i_2$, што није могуће. Дакле, оба квадрата су латинска.

Да бисмо доказали да су L_1 и L_2 међусобно ортогонални, претпоставимо супротно, то јест да исти уређени пар бројева граде поља (i_1, j_1) и (i_2, j_2). Тада би морало да важи $i_1 + j_1 \equiv i_2 + j_2 \pmod{n}$ и $2i_1 + j_1 \equiv 2i_2 + j_2 \pmod{n}$. Одузимањем прве једначине од друге добијамо да мора да важи $i_1 \equiv i_2$, тј. $i_1 = i_2$, што заједно са првом једначином даје и $j_1 \equiv j_2$ односно $j_1 = j_2$.

Дакле, дати латински квадрати су међусобно ортогонални. $\square$

Поставља се питање да ли, уколико имамо конструисане парове ортогоналних латинских квадрата за одређене природне бројеве n, можемо конструисати пар ортогоналних латинских квадрата већег реда. То би нам помогло да из конкретних примера парова ортогоналних латинских квадрата мањег реда, за које лако знамо да постоје, генерализујемо постојање на све природне бројеве n одређеног облика.

Дефиниција 2.2. Нека је $A = (a_{ij})$ латински квадрат реда n ($a_{ij} \in \{1, 2, \ldots, n\}$) и $B = (b_{st})$ латински квадрат реда m ($b_{st} \in \{1, 2, \ldots, m\}$).

Тада је *Кронекеров производ* квадрата A и B квадрат $A \otimes B$ димензија $mn \times mn$ задат са:

(a_{11}, B)	(a_{12}, B)	$\cdots$	(a_{1n}, B)
(a_{21}, B)	(a_{22}, B)	$\cdots$	(a_{2n}, B)
$\vdots$	$\vdots$	$\ddots$	$\vdots$
(a_{n1}, B)	(a_{n2}, B)	$\cdots$	(a_{nn}, B)

Табела 2.1: Редуковани производ квадрата A и B

при чему је сваки (a_{ij}, B) квадрат димензија $m \times m$:

$b_{11}+(a_{ij}-1)m$	$b_{12}+(a_{ij}-1)m$	$\cdots$	$b_{1m}+(a_{ij}-1)m$
$b_{21}+(a_{ij}-1)m$	$b_{22}+(a_{ij}-1)m$	$\cdots$	$b_{2m}+(a_{ij}-1)m$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$b_{m1}+(a_{ij}-1)m$	$b_{m2}+(a_{ij}-1)m$	$\cdots$	$b_{mm}+(a_{ij}-1)m$

Теорема 2.3. Ако су A и B латински квадрати онда је и Кронекеров производ $A \otimes B$ такође латински квадрат.

Доказ. Квадрат $mn \times mn$ је попуњен бројевима од 1 до $m + (n-1)m = mn$. Треба доказати да не постоје два иста броја у једној врсти и два иста броја у једној колони. Претпоставимо да постоје два иста броја у било којој врсти i_1 било које врсте i_2 редукованог производа квадрата (видети табелу 2.1). У тој врсти квадрата фигуришу a_{i_1k} и b_{i_2j} за неко j и k. Ако претпоставимо да су два броја из врсте иста, било би $b_{i_2j_1} + (a_{i_1k_1} - 1)m = b_{i_2j_2} + (a_{i_1k_2} - 1)m$ односно $b_{i_2j_1} - b_{i_2j_2} = m(a_{i_1k_2} - a_{i_1k_1})$. Одавде, пошто важи $|b_{i_2j_1} - b_{i_2j_2}| \leqslant m - 1$, морало би да важи $b_{i_2j_1} = b_{i_2j_2}$ што је немогуће, јер је B латински квадрат.
Слично, за два броја у истој колони би важило $b_{i_1j_2} + (a_{k_1j_1} - 1)m = b_{i_2j_2} + (a_{k_2j_1} - 1)m$, одакле би морало да важи $b_{i_1j_2} = b_{i_2j_2}$, што је контрадикција са тиме да је квадрат B латински.

Дакле, на овај начин конструисан квадрат димензија $mn \times mn$ је латински. $\square$

Теорема 2.4. Ако су A и B међусобно ортогонални латински квадрати реда n и C и D међусобно ортогонални латински квадрати реда m, онда су и квадрати $A \otimes C$ и $B \otimes D$ међусобно ортогонални.

Доказ. Знамо из претходне теореме да су ова два квадрата латински и димензије $mn \times mn$. Означимо поље квадрата са (w, t, x, y), при чему (w, t) представља поље редукованог производа квадрата (табела 2.1) односно то је квадрат $m \times m$, док (x, y) представља поље унутар тог квадрата. Дакле, број који одговара пољу (w, t, x, y) квадрата $A \otimes C$ је $c_{xy} + (a_{wt} - 1)m$.

Претпоставимо да дати квадрати нису ортогонални, то јест да се исти уређени пар налази у пољима (w, t, x, y) „упарених " латинских квадрата $A \otimes C$ и $B \otimes D$, као и у пољима (w_1, t_1, x_1, y_1).
Тада би морало да важи:
$c_{xy} + (a_{wt} - 1)m = c_{x_1y_1} + (a_{w_1t_1} - 1)m$ и $d_{xy} + (b_{wt} - 1)m = d_{x_1y_1} + (b_{w_1t_1} - 1)m$.
Из прве једнакости пошто је $|c_{xy} - c_{x_1y_1}| \leqslant m - 1$ мора да важи

$$c_{xy} = c_{x_1y_1} \text{ и } a_{wt} = a_{w_1t_1}.$$

Слично из друге једначине следи

$$d_{xy} = d_{x_1y_1} \text{ и } b_{wt} = b_{w_1t_1}.$$

Међутим, тада би уређени парови (a_{wt}, b_{wt}) и $(a_{w_1t_1}, b_{w_1t_1})$ били исти, те квадрати A и B не би били ортогонални. Такође би важило $(c_{xy}, d_{xy}) = (c_{x_1y_1}, d_{x_1y_1})$ што је у супротности са ортогоналношћу квадрата C и D. Контрадикција. □

Примећујемо да нам Кронекеров производ омогућава управо оно што смо желели - налажење парова ортогоналних латинских квадрата већег реда из знања да они постоје за специјалне случајеве.
Како се Кронекеровим производом ред новонасталог квадрата добија производом редова почетних латинских квадрата, уочавамо да бисмо могли да изведемо постојање пара ортогоналних латинских квадрата којима је ред степен природног броја. Ако је тај број непаран, доказ је свакако дат теоремом 2.2, тако да нас занима да ли постоји пар ортогоналних латинских квадрата реда n, када је n степен двојке.

Теорема 2.5. Постоји пар ортогоналних латинских квадрата реда $n = 2^m$ за свако $m \geqslant 2$.

Доказ. Доказ ћемо спровести индукцијом.
База: Постоји пар ортогоналних латинских квадрата реда $n = 2^2$:

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

Пар ортогоналних латинских квадрата реда 4

Постоји пар ортогоналних латинских квадрата реда $n = 2^3$:

1	3	4	5	6	7	8	2
5	2	7	1	8	4	6	3
6	4	3	8	1	2	5	7
7	8	5	4	2	1	3	6
8	7	2	6	5	3	1	4
2	5	8	3	7	6	4	1
3	1	6	2	4	8	7	5
4	6	1	7	3	5	2	8

1	4	5	6	7	8	2	3
8	2	6	5	3	1	4	7
2	8	3	7	6	4	1	5
3	6	2	4	8	7	5	1
4	1	7	3	5	2	8	6
5	7	1	8	4	6	3	2
6	3	8	1	2	5	7	4
7	5	4	2	1	3	6	8

Пар ортогоналних латинских квадрата реда 8

Индуктивна хипотеза: Претпоставимо да постоји пар ортогоналних латинских квадрата реда 2^k за свако $2 \leqslant k \leqslant m$, $m \geqslant 3$.
Индуктивни корак: Докажимо сада да постоји пар ортогоналних латинских квадрата реда 2^{m+1}. На основу теореме 2.4 узимањем два ортогонална латинска квадрата A и B реда 2^2 (који на основу базе постоје) и два ортогонална латинска квадрата C и D реда 2^{m-1} ($m > m-1 \geqslant 2$ одакле следи да они на основу индуктивне хипотезе такође постоје) можемо конструисати два међусобно ортогонална латинска квадрата $A \otimes C$ и $B \otimes D$ који су реда $2^2 2^{m-1} = 2^{m+1}$.

Јаком Индукцијом следи да постоји пар ортогоналних латинских квадрата реда 2^m за свако $m \geqslant 2$.
Напомена: Не постоји пар ортогоналних латинских квадрата реда 2, јер постоји само један латински квадрат реда 2. □

Уколико опет применимо особине Кронекеровог производа, сада комбинујући латинске квадрате непарног реда и реда степена двојке, лако доказујемо следећу теорему:

Теорема 2.6. Постоји пар ортогоналних латинских квадрата реда $4k$.

Доказ. Напишимо $4k = 2^m n$ где је $m \geqslant 2$, а n непаран број.

Из теореме 2.2 следи да постоји пар ортогоналних латинских квадрата реда n - A и B.

Из теореме 2.5 следи да постоји пар ортогоналних латинских квадрата реда 2^m - C и D.

Сада имамо, служећи се теоремом 2.4 конструкцију пара ортогоналних латинских квадрата $A \otimes C$ и $B \otimes D$ који су реда $2^m n = 4k$. □

У досадашњем делу смо навели доказе за постојање пара ортогоналних латинских квадрата у зависности од реда n, а сада желимо да посматрамо више латинских квадрата одједном, уз додатни услов да су по паровима међусобно ортогонални. Стога имамо следећу дефиницију.

Дефиниција 2.3. Скуп међусобно ортогоналних латинских квадрата (скраћено МОЛК) представља скуп латинских квадрата истог реда међу којима су свака два по паровима међусобно ортогонална.

Занима нас које максималне кардиналности може бити тај скуп.

Теорема 2.7. Ако је S скуп међусобно ортогоналних латинских квадрата реда n онда је $|S| \leqslant n-1$.

Доказ. Можемо претпоставити да је попуњавање вршено скупом бројева $N = \{1, 2, \ldots, n\}$. У сваком латинском квадрату у S можемо независно да пермутујемо бројеве и то урадимо тако да први ред сваког латинског квадрата буду редом бројеви од 1 до n, при чему ће (према леми 2.1) дати скуп латинских квадрата и даље остати међусобно ортогоналан.

Сада, ако изаберемо било које $i \in N$ и посматрамо било који пар латинских квадрата, уређени пар (i, i) се јавља у првом реду. Посматрајмо садржај поља (2,1) сваког латинског квадрата S. Он не може да буде број 1, јер се 1 већ налази у првој колони у првом реду. Штавише, ниједна два квадрата не могу имати исти број j на том пољу јер би се онда уређени пар (j, j) јављао два пута, како на овом пољу тако и на j-том пољу у првом реду, те та два квадрата не би били међусобно ортогонални. Дакле, не може бити више квадрата него што је могућих бројева на позицији (2,1) којих је $n-1$ (од 2 до n). Стога, скуп међусобно ортогоналних латинских квадрата може имати највише $n-1$ чланова, што је и тврђено. □

Нас ће посебно занимати за које природне бројеве n постоји скуп од тачно $n-1$ међусобно ортогоналних латинских квадрата реда n.

2.2 Комплетан скуп међусобно ортогоналних латинских квадрата

Дефиниција 2.4. Комплетан скуп међусобно ортогоналних латинских квадрата реда n представља скуп од $n-1$ латинских квадрата реда n, при чему су свака два међусобно ортогонална.

У потрази за постојањем комплетног скупа МОЛК-а налазимо интересантну повезаност између ортогоналности латинских квадрата и пројективне геометрије. Наиме, доказаћемо да је постојање комплетног скупа МОЛК-а реда n еквивалентно постојању пројективне равни реда n.

За ту сврху, навешћемо основна својства афиних и пројективних равни.

2.2.1 Афине и пројективне равни

Коначна геометрија представља било који геометријски систем који се састоји од коначно много тачака. Насупрот њој, Еуклидска геометрија не представља тип коначне геометрије зато што права у Еуклидској геометрији садржи бесконачно много тачака.

Коначне равни представљају равни које се састоје од коначно много тачака. Два главна типа коначних равни су афина и пројективна коначна раван. У коначној афиној равни, важи Плејферова аксиома, док се у коначној пројективној равни сваке две праве секу у тачно једној тачки.
Навешћемо аксиоме које дефинишу коначне афине и коначне пројективне равни:

Дефиниција 2.5. Коначна афина раван представља непразан скуп тачака и правих које задовољавају следеће аксиоме

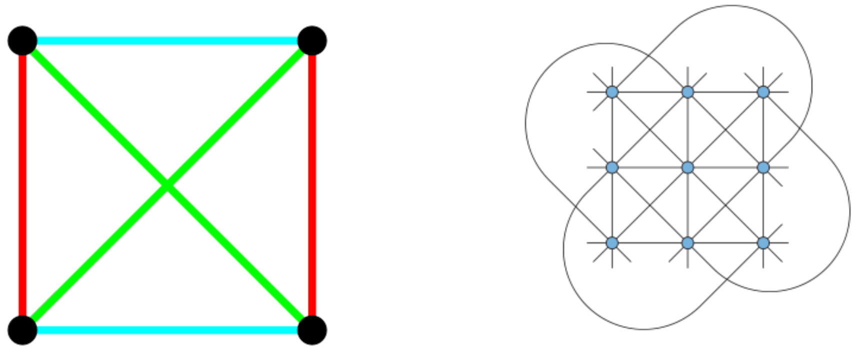
(A1) За сваке две различите тачке постоји јединствена права која их садржи.

(A2) За дату праву ℓ и тачку P која није на правој ℓ постоји јединствена права која садржи P и нема пресечних тачака са ℓ.

(A3) Постоји скуп од 4 тачке, међу којима никоје три нису колинеарне (ово је зарад искључивања тривијалних случајева где су све тачке на једној правој).

Коначна афина раван реда n има n^2 тачака и n^2+n правих. Свака права садржи n тачака и свака тачка је на $n+1$ правој.

Паралелна класа коначне афине равни је скуп правих које су међусобно паралелне. У коначној афиној равни постоји $n+1$ паралелних класа, од којих свака садржи n правих. (Ова тврђења наводимо без доказа, јер су позната у математици инцидентне геометрије и доказују се преко наведених аксиома.)



Коначне афине равни реда 2 и 3

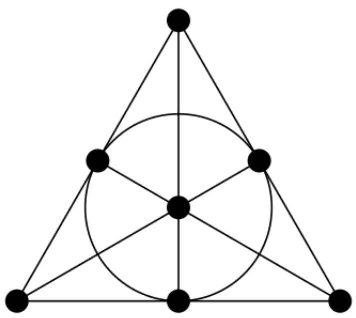
Дефиниција 2.6. Коначна пројективна раван представља непразан скуп тачака и правих које задовољавају следеће аксиоме

(P1) За сваке две различите тачке постоји јединствена права која их садржи.

(P2) Пресек било које две различите праве је тачно једна тачка.

(P3) Постоји скуп од 4 тачке, међу којима никоје три нису колинеарне.

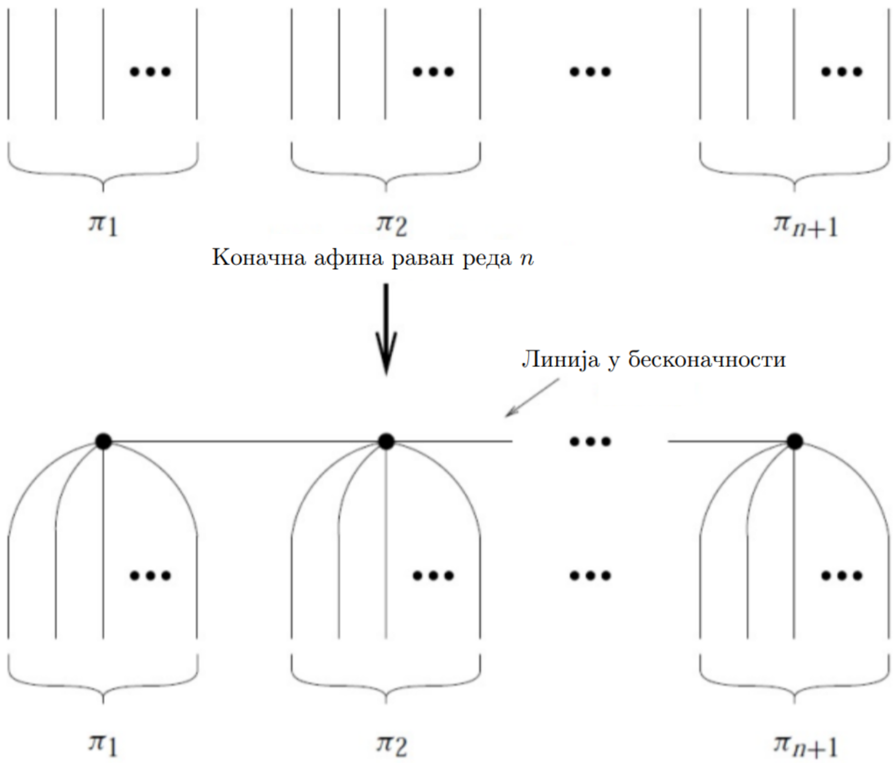
Коначна пројективна раван реда n има n^2+n+1 тачака и исто толико правих. Свака права садржи $n+1$ тачака и свака тачка је на $n+1$ правих.



Коначна пројективна раван реда 2 - *Фано раван*

Теорема 2.8. Од сваке коначне афине равни реда n може се конструисати коначна пројективна раван реда n и обратно. Ово значи да је постојање коначне афине равни реда n еквивалентно постојању коначне пројективне равни реда n

Доказ. ($\Longrightarrow$) Конструкцију започињемо од коначне афине равни реда n (P, B) (P је скуп тачака, а B скуп правих). Знамо да она садржи $n+1$ паралелних класа. Назовимо те паралелне класе, односно скупове правих π_1,π_2,...,π_{n+1}. Додајмо нове (различите) тачке ∞_1,∞_2,...,∞_{n+1} и нову праву која пролази кроз те тачке $\infty = \{\infty_1, \infty_2, \ldots, \infty_{n+1}\}$. Нека су нови скупови $P(\infty) = P \cup \{\infty_1, \infty_2, \ldots, \infty_{n+1}\}$ и $B(\infty) = \{b \cup \infty_i \mid b \in \pi_i\} \cup \{\infty\}$. Овај поступак се зове *додавање праве у бесконачност* и тиме смо добили пројективну раван $(P(\infty), B(\infty))$.



Конструисање пројективне равни реда n из афине равни

Потребно је уверити се да овако конструисан скуп тачака и правих заиста и задовољава аксиоме пројективне равни.

(P1) Ако су у питању две већ постојеће тачке из скупа P, постојање јединствене праве кроз њих следи директно из (A1). Ако је једна од тачака

∞_i, а друга из скупа P приметимо да се у паралелној класи π_i налазе све почетне тачке афина равни (паралелна класа садржи n правих са по $n+1$ различитом тачком што је n^2+n различитих тачака колико их у афина равни укупно и има), одакле следи да, пошто тачка ∞_i лежи на свакој од n почетно паралелних правих, да кроз њу и било коју другу тачку из скупа P пролази тачно једна права. Ако су у питању две тачке ∞_i и ∞_j, кроз њих пролази тачно једна права и то права ∞.

(P2) Пресек две праве из исте класе π_i је тачно једна тачка ∞_i по конструкцији. Ако су у питању две праве из различитих класа π_i и π_j, оне по дефиницији паралелних класа имају пресек (јединствен, јер би у супротном била нарушена $(A1)$) и он је остао ненарушен додавањем тачака ∞_i и ∞_j. На крају, пресек праве ∞ и било које друге праве b је јединствена тачка ∞_i ако $b \in \pi_i$, по конструкцији.

(P3) Директно следи из (A3).

Ради бољег разумевања конструкције, приложимо илустрацију конструкције пројективне равни реда 2 из афина равни реда 2. Имамо $P = \{1,2,3,4\}$ и
$B = \{\ \{1,2\},\{1,3\},\{1,4\},$
$\{3,4\},\{2,4\},\{2,3\}\ \}$, при чему су 3 паралелне класе дате у колонама. Означимо колоне са π_1,π_2,π_3. Уведимо нову праву $\infty = \{\infty_1,\infty_2,\infty_3\}$, при чему је сада $P(\infty) = \{1,2,3,4,\infty_1,\infty_2,\infty_3\}$ и
$B = \{\ \{1,2,\infty_1\},\{1,3,\infty_2\},\{1,4,\infty_3\},$
$\{3,4,\infty_1\},\{2,4,\infty_2\},\{2,3,\infty_3\},\{\infty_1,\infty_2,\infty_3\}\ \}$
Ова конструкција тачно даје пројективну раван реда 2, заменом симбола $\infty_1 \to 5, \infty_2 \to 6, \infty_3 \to 7$.

($\Longleftarrow$) Конструкција афине равни из пројективне равни представља само обрнути процес. Означимо једну праву (било коју) и обришимо њу, као и све тачке на њој. Доказивање аксиома коначне афине равни слични су као у претходном случају.

Дакле, тврђење је доказано конструкцијом. $\square$

2.2.2 Афина раван и комплетан скуп међусобно ортогоналних латинских квадрата

Анализирајући афину раван, на први поглед се могу наћи сличности са копмлетним скупом МОЛК-а у виду паралелних класа и својстава инцидентности, међутим, изненађујуће, повезаност између њих је много већа. О томе нам говори следећа теорема:

Теорема 2.9. Комплетан скуп међусобно ортогоналних латинских квадрата реда n постоји **ако и само ако** постоји коначна афина раван реда n.

Доказ. ($\Longrightarrow$) Прво ћемо описати конструкцију коначне афине равни из комплетног скупа МОЛК-а. За тачке, узмимо све уређене парове (i, j), $1 \leqslant i, j \leqslant n$ (има их дакле n^2). Што се тиче правих, груписаћемо их у скупове од по n правих, које одговарају $n+1$ паралелној класи, које афина раван садржи, као што смо објаснили раније:

- За било које i, сва поља у реду i формирају праву. Скуп ових n правих представља паралелну класу.
- За било које j, сва поља у колони j формирају праву. Скуп ових n правих представља паралелну класу.
- Узмимо било који латински квадрат L_a из нашег скупа од $n-1$ МОЛК-а. За било који број s, нека сва поља у латинском квадрату L_a која садрже s формирају праву. Скуп свих ових n правих, једна за сваки број, представља паралелну класу. Добили смо $n-1$ паралелних класа, једну за сваки латински квадрат у нашем скупу.

(A1): Не постоје две различите тачке кроз које пролазе две различите праве: За праве добијене из редова и колона, ово је јасно. Ако би кроз две различите тачке пролазиле праве добијене симболом a латинског квадарта L_a и симболом b латинског квадрата L_b следило би да се у та два различита поља (која представљају те две различите тачке) Ојлеровог квадрата, добијеног „спајањем" ортогоналних латинских квадрата L_a и L_b, налази исти уређени пар бројева (a, b) што је из њихове ортогоналности немогуће.
Кроз сваке две различите тачке постоји права: За било коју тачку (i, j) показали смо да она лежи на $n+1$ правих (једна одговара реду i, једна колони j и $n-1$ из толико латинских квадрата), од којих свака садржи других n различитих тачака. Дакле, све ове праве садрже $(n+1)(n-1)+1 = n^2$ тачака. Другим речима, тачка (i, j) је повезана са сваком другом тачком наше конструкције.
Из ова два дела следи да кроз сваке две различите тачке пролази тачно једна права.

(A2): Узмимо било коју праву m и било коју тачку (i, j) која није на m. Ако је m ред, узмимо ред i; ова права је паралелна са m и штавише је јединствена (из разлога што свака права формирана од скупа поља који одговарају неком броју a у неком L_1 мора пресећи ред m, јер се број a мора налазити у сваком реду латинског квадрата L_1). Слично, ако је m колона, узмимо колону j; ово је такође јединствена права паралелна са m кроз (i, j). Коначно, ако је m права фомрирана од скупа поља која одговарају неком симболу s у латинском квадрату L_a, узмимо праву формирану од скупа поља који одговарају симболу (било који да је) у пољу (i, j) у латинском квадрату L_a.

Ова права је паралелна са m по конструкцији, и штавише је јединствена:

За било коју другу праву n која садржи (i,j), n мора бити или ред или колона (и у том случају свакако сећи m), или мора бити формирана од неког другог симбола t из латинског квадрата L_b. Међутим, тада тачку, односно поље (k,l) Ојлеровог квадрата које саржи уређени пар (s,t) (а мора да садржи тај уређени пар, јер су L_a и L_b међусобно ортогонални) садрже обе праве m и n. Наиме, $(k,l) \in m$ јер је у пољу (k,l) латинског квадрата L_a симбол s. Такође, $(k,l) \in n$ јер је у пољу (k,l) латинског квадрата L_b симбол t.
Дакле доказана је аксиома А2 афине равни.

(А3): Како смо почели са најмање једним МОЛК, најмањег реда 2, конструисали смо барем 6 правих (најмање по 2 за редове и колоне и 2 за најмање један латински квадрат), свака са барем 2 тачке, те је аксиома А3 задовољена.

Конструкцијом смо остварили афину раван!

($\Longleftarrow$) Процес конструкције комплетног скупа МОЛК-а из афине равни је потпуно исти, само обратан. Нека је дата коначна афина раван реда n, поделимо је у $n+1$ паралелне класе C_0,C_1,$\dots C_n$, свака са по n елемената. Означимо елементе сваке класе C_i од 1 до n.

Одредимо паралелну класу C_0 да одговара редовима наших латинских квадрата и паралелну класу C_n да одговара колонама наших латинских квадрата. Нека свакој координати (i,j) одговара јединствена тачка пресека i-те праве паралелне класе C_0 и j-те праве паралелне класе C_n. Овиме се добија бијекција између тачака наше афине равни и поља (i,j).

За било који број k између 1 и $n-1$, попуњавамо латински квадрат L_k на следећи начин: ставимо симбол s у поље (i,j) ако права s класе C_k садржи тачку која је идентификована са (i,j) раније. Пошто је свака тачка на некој од правих из C_k (n дисјунктних правих са по n тачака), свако поље ће бити попуњено. Такође, ово очувава латинско својство, зато што се свака права наше класе C_k појављује у сваком реду (тј. пресеца сваку праву из C_0, јер су из различитих паралелних класа) и свакој колони (тј. пресеца сваку праву из C_n, јер су из различитих паралелних класа) тачно једном (ако би пресек био више од једне тачке, била би нарушена аксиома (А1)).

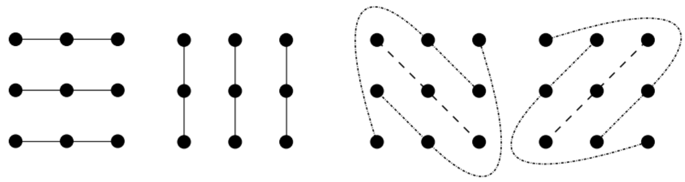
Овиме је креирано $n-1$ латинских квадрата. Штавише, за свака два таква латинска квадрата L_a и L_b, и било које две праве $s \in C_a$, $t \in C_b$, знамо да се s и t секу у тачно једној тачки, тј. постоји тачно једно поље где је s у том пољу латинског квадрата L_a и уједно t у том пољу латинског квадрата L_b. Другим речима, сваки пар симбола се појављује тачно једном одакле следи да су овако конструисани квадрати међусобно ортогонални!

Латински квадрати:

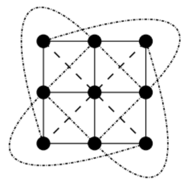
1	2	3
3	1	2
2	3	1

1	2	3
2	3	1
3	1	2

Одговарајуће паралелне класе:



Афина раван:



Конструисање афине равни реда 3 из комплетног скупа МОЛК-а реда 3

□

Сада можемо извести и коначан закључак, који смо навели још на почетку поглавља:

Теорема 2.10. Постојање комплетног скупа међусобно ортогоналних латинских квадрата реда n еквивалентно је постојању коначне пројективне равни реда n.

Доказ. Доказ следи, применом теореме 2.9 и теореме 2.8.

Постојање комплетног скупа МОЛК $\Longleftrightarrow$ постојање коначне афине равни реда n $\Longleftrightarrow$ постојање коначне пројективне равни реда n. □

Овим доказом смо питање постојања комплетног скупа међусобно ортогоналних латинских квадрата пренели на поље коначне геометрије.
Из математичких достигнућа у области пројективних равни знамо да пројективна раван реда n постоји за сваки природан број n који је степен простог броја. Доказ овог тврђења нећемо наводити, али напоменућемо да се изводи конструкцијом пројективне равни из Галоавог поља реда n, које када је n степен простог броја постоји, при чему се на тај начин конструисана пројективна раван назива Галоаова раван. Стога наводимо следећу теорему:

Теорема 2.11. Постоји комплетан скуп међусобно ортогоналних латинских квадрата реда n, где је n степен простог броја.

Постојање пројективне равни било ког другог реда је и даље отворено питање, са тим што су амерички математичари Ричард Хуберт Брук и Херберт Џон Рајзер 1949. године доказали битно својство о непостојању пројективних равни одређеног реда:

Теорема 2.12. Ако је $n \equiv 1, 2 \pmod 4$ и n се не може представити као збир квадрата два природна броја, онда пројективна раван реда n не постоји.

Како све ово важи и за комплетан скуп МОЛК-а, систематизујмо наведена тврђења у наредну теорему:

Теорема 2.13. Нека је n природан број, тада:

А) Ако је n степен простог броја, постоји комплетан скуп МОЛК-а.

Б) Ако је $n \equiv 1, 2 \pmod 4$ и n се не може представити као збир квадрата два цела броја, комплетан скуп МОЛК-а реда n не постоји.

В) У сваком другом случају, комплетан скуп МОЛК-а може и не мора постојати.

Први природан број n који припада случају под В) јесте број 10 и непостојање комплетног скупа МОЛК-а (и пројективне равни) је доказано уз помоћ компјутера 1989. године. После њега, следећи такав број је 12 и постојање комплетног скупа МОЛК-а реда 12 је и даље отворено питање!
Следећа табела нам даје добар преглед о постојању комплетног скупа МОЛК-а чији су редови мали природни бројеви, у овом случају до 25.

n	Закључак	Коментар
2	постоји	А
3	постоји	А
4	постоји	А
5	постоји	А
6	не постоји	Тари, Б
7	постоји	А
8	постоји	А
9	постоји	А
10	не постоји	компјутер
11	постоји	А
12		В
13	постоји	А
14	не постоји	Б
15		В
16	постоји	А
17	постоји	А
18		В
19	постоји	А
20		В
21	не постоји	Б
22	не постоји	Б
23	постоји	А
24		В
25	постоји	А

Постојање комплетног скупа МОЛК-а за одређене редове

Због своје једноставности, навешћемо конструкцију постојања комплетног скупа међусобно ортогоналних латинских квадрата реда простог броја p.

Теорема 2.14. За било који прост број p постоји комплетан скуп МОЛК-а реда p.

Доказ. Користићемо скуп $N = \{0, 1, \dots, p-1\}$. Означимо квадрате са S_1, S_2,..., S_{p-1} и наведимо следећу конструкцију, при чему су све вредности дате по модулу p. Нека је за $k \in \{1, 2, \dots, p-1\}$ квадрат S_k конструисан на следећи начин:

0	1	...	$p-1$
k	$k+1$	...	$k+(p-1)$
$2k$	$2k+1$	...	$2k+(p-1)$
$\vdots$	$\vdots$		$\vdots$
$(p-1)k$	$(p-1)k+1$	...	$(p-1)k+(p-1)$

Латински квадрат S_k

Уверићемо се да је он заиста латински. Јасно је да не могу постојати два иста броја у неком реду. Претпоставимо да постоје два иста броја у колони j у пољима (i_1, j) и (i_2, j). Тада би важило $i_1k + j \equiv i_2k + j \pmod p$, односно $i_1k \equiv i_2k$, а пошто је $(k, p) = 1$ $(1 \leqslant k \leqslant p-1)$ следи $i_1 \equiv i_2 \pmod p$, што није могуће. Дакле, дати квадрати су заиста латински.

Сада ћемо доказати да су свака два квадрата ортогонална. Изаберимо произвољно два квадрата S_i и S_j, $i \neq j$, и претпоставимо да се исти уређени пар бројева налази у пољима (k_1, m_1) и (k_2, m_2) који граде та два латинска квадрата. Наш циљ биће да докажемо да је заправо онда $k_1 = k_2$ и $m_1 = m_2$. Према конструкцији сваког латинског квадрата следи

$$(k_1-1)i + m_1 - 1 \equiv (k_2-1)i + m_2 - 1 \pmod p,$$
$$(k_1-1)j + m_1 - 1 \equiv (k_2-1)j + m_2 - 1 \pmod p,$$

Одатле $k_1i + m_1 \equiv k_2i + m_2 \pmod p$ и $k_1j + m_1 \equiv k_2j + m_2 \pmod p$
Следи $(k_2 - k_1)i = k_2i - k_1i \equiv m_1 - m_2 \equiv k_2j - k_1j = (k_2 - k_1)j \pmod p$
Како је $1 \leqslant i, j \leqslant p-1$, односно $-(p-2) \leqslant i - j \leqslant p-2$ и претпоставили смо $i \neq j$, имамо $(i-j, p) = 1$, одакле из добијеног $(k_2 - k_1)i \equiv (k_2 - k_1)j \pmod p$ следи $k_2 - k_1 \equiv 0 \pmod p$ што због $1 \leqslant k_1, k_2 \leqslant p$ даје $k_1 = k_2$. Даље, у том случају мора да важи и $m_2 - m_1 \equiv 0 \pmod p$, односно такође $m_1 = m_2$, што смо и желели.

Дакле, овако конструисан скуп $\{S_k \mid 1 \leqslant k \leqslant p-1\}$ представља комплетан скуп међусобно ортогоналних латинских квадрата. $\square$

2.3 Ограничење максималног броја међусобно ортогоналних латинских квадрата

У претходним поглављима је било речи о максималној кардиналности скупа међусобно ортогоналних латинских квадрата, док ћемо у овом поглављу навести додатна ограничења која зависе од реда n латинских квадрата које посматрамо.

Дефиниција 2.7. Нека је $N(n)$ највећи број међусобно ортогоналних латинских квадрата реда n.

У теореми 2.7 смо доказали да је $N(n) \leqslant n-1$ и доказали да се тај број достиже за природне бројеве n који су степени простог броја.
Међутим, математичари су се дуго трудили да нађу доње ограничење за $N(n)$ у зависности од n. Један од првих резултата у овом смеру је поставио математичар Харис Френклин Макнајш 1922. године.

Теорема 2.15. Нека је $n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ канонска факторизација природног броја n. Тада је $N(n) \geqslant \min\limits_i \{p_i^{a_i} - 1\}$.

Доказ. Из теореме 2.11 нам је познато да за свако $n_i = p_i^{a_i}$ постоји $n_i - 1$ међусобно ортогоналних латинских квадрата. Нека је најмањи од бројева n_i $(1 \leqslant i \leqslant m)$ n_{min}. Тада постоји бар $n_{min} - 1$ међусобно ортогоналних латинских квадрата за сваки ред n_i. Узимајући по $n_{min} - 1$ МОЛК-а за сваки n_i и применом Кронекеровог производа, односно теореме 2.4 $m-1$ пута, добијамо $n_{min} - 1$ међусобно ортогоналних латинских квадрата реда $n_1 n_2 \dots n_m = n$. (Наиме, прво примењујемо теорему 2.4 на по $n_{min} - 1$ МОЛК-а реда n_1 и n_2 у паровима и тиме добијамо $n_{min} - 1$ МОЛК-а реда $n_1 n_2$. Даље, процес настављамо применом теореме на новодобијених $n_{min} - 1$ МОЛК-а и оних $n_{min} - 1$ реда n_3, и тако даље све до n_m чиме задржавамо $n_{min} - 1$ МОЛК-а, сада коначног реда n).
Дакле, $N(n)$ је барем $\min\limits_i \{p_i^{a_i} - 1\}$ $\square$

Имајући у виду Ојлерову претпоставку, из разлога што је у случају $n \equiv 2 \pmod 4$ $\min\limits_i \{p_i^{a_i} - 1\} = 2^1 - 1 = 1$, Макнајш је претпоставио да, не само да је $N(n) \geqslant \min\limits_i \{p_i^{a_i} - 1\}$, већ и да је то горње ограничење, односно да је $N(n) = \min\limits_i \{p_i^{a_i} - 1\}$.

Међутим, с обзиром на то да су математичари Бозе, Шриканде и Паркер оповргли Ојлерову претпоставку, тиме су оповргнули и претпоставку Макнајша.

Макнајшијева теорема нам даје лошу оцену $N(n) \geqslant 1$ када је $n \equiv 2 \pmod 4$, мада како генерално није познато колики је број међусобно ортогоналних латинских квадрата за природан број n који није степен простог броја, ова теорема нам може (а и не мора) дати добар осећај за тај број у зависности од n.

2.4 Примена

Ојлерова заинтересованост за пар ортогоналних латинских квадрата произишла је из његове жеље да конструише магичне квадрате. Међутим, од краја осамнаестог века поље примене латинских квадрата и њихове ортогоналности се знатно проширило.

Геометрија: Скуп од k међусобно ортогоналних латинских квадрата реда n је еквивалентан $(k+2)$-мрежи реда n. Специјално, када је $k = n-1$, комплетан скуп МОЛК-а је еквивалентан $(n+1)$-мрежи, односно пројективној равни реда n.

Теорија графова: Скуп од k међусобно ортогоналних латинских квадрата реда n је еквивалентан партицији грана комплетног $(k+2)$-партитивног графа $K_{n,\dots,n}$ на комплетне подграфове реда $k+2$.

Кодирање: Ортогонални латински квадрати се користе у теорији кодирања у различите сврхе од којих је једна откривање грешака и исправљање кода, у циљу квалитетног преноса поруке у дигиталном облику, било она једнодимензионална или дводимензионална (попут слике).

У раду смо такође уочили повезаност са теоријом поља, док се практична примена ортогоналности користи и у дизајну експеримената, као и у конструисању такмичарских турнира.

Закључак

Без обзира на то да ли се играмо картама или изучавамо озбиљне математичке структуре, у оба случаја се можемо сусрести са ортогоналношћу латинских квадрата. С обзиром на корелисаност ортогоналности латинских квадрата са осталим математичким темама, достигнућа у њима ће бити међусобно повезана чиме ће се, надамо се, решити преостала отворена питања, било конструкцијом напреднијег математичког алгоритма или прављењем софтвера који ће бити у могућности да реши дате проблеме.

На крају, желео бих да упутим посебну захвалност менторки Соњи Чукић на помоћи при изради матурског рада и одабиру литературе.

Литература

[1] A. D. Keedwell, J. Dénes *Latin Squares and their Applications*, North Holland, 2015.

[2] C. C. Linder, C. A. Rodger *Discrete Mathematics and Its Applications*, Chapman and Hall_CRC, 2008.

[3] L. Lovász, J. Pelikán, K. Vesztergombi, *Discrete Mathematics Elementary and Beyond*, Undergraduate Texts in Mathematics, Springer Verlag, Berlin, 2003.

[4] C. F. Laywine, G. L. Mullen, *Discrete Mathematics Using Latin Squares*, Brock University, The Pennsylvania State University, 1998.

[5] J. Morris, *Combinatorics*, University of Lethbridge, The LibreTexts.

[6] D. Guichard, *Combinatorics and Graph Theory*, Department of Mathematics Whitman College.

[7] J. Kåhrström, *On Projective Planes*, Mid Sweden University, 2002.

[8] M. G. Tarry, *Le probleme des 36 officiers*, Springer Universitext, Comptes Rendus Ass. Franc. Sci. Nat. 1900(2), 170–203 (1901).

[9] D. R. Stinson, *A short proof of the nonexistence of a pair of orthogonal latin squares of order six*, Department of Computer Science, University of Manitoba, Journal of Combinatorial Theory Series A, 1982.