Ortogonalni latinski kvadrati i konačne projektivne ravnine

Rafael Mrđen
student na PMF–Matematičkom odjelu
e-mail: rafaelmrdjen@gmail.com

Sažetak

U ovom članku uvodi se pojam latinskog kvadrata, njegove ortogonalnosti, te konačne projektivne ravnine (s kombinatornog aspekta). Navode se i dokazuju neka njihova osnovna svojstva i veze. Dokazuje se dovoljan uvjet egzistencije konačne projektivne ravnine zadanog reda. Najjači rezultat koji se dokazuje jest Bruck-Ryserov teorem, koji daje neke nužne uvjete na red konačne projektivne ravnine. Na kraju, kratko i informativno daje se uvid u generalizaciju.

Sadržaj

1 Ortogonalni latinski kvadrati

Tijekom povijesti latinski su kvadrati bili dio zabavne matematike. Međutim, u jednom su trenu matematičari uvidjeli netrivijalnost kombinatornih problema koji proizilaze iz razmatranja o latinskim kvadratima, kao i primjenu u drugim granama matematike. Mi ćemo razviti teoriju latinskih kvadrata u mjeri koja nam je potrebna da uspostavimo vezu s konačnim projektivnim ravninama.

Definicija. Kažemo da je kvadratna matrica A reda $n \in \mathbb{N}$ *latinski kvadrat* ako vrijedi:

- Elementi matrice A su elementi nekog n-članog skupa[1] $\{a_1, a_2, \ldots, a_n\}$;
- U svakom retku matrice A, svaki a_i, $i = 1, 2, \ldots, n$ nalazi se na točno jednom mjestu;
- U svakom stupcu matrice A, svaki a_i, $i = 1, 2, \ldots, n$ nalazi se na točno jednom mjestu.

Primjer 1. Vrlo je lako provjeriti da su matrice

$$M := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{i} \quad N := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

latinski kvadrati reda 3.

Općeniti latinski kvadrati neće nam biti posebno zanimljivi, ali hoće familije latinskih kvadrata istog reda koje imaju sljedeće svojstvo:

Definicija. Za latinske kvadrate $A_1 = \left(a_{ij}^{(1)}\right)_{ij}$ i $A_2 = \left(a_{ij}^{(2)}\right)_{ij}$ reda n kažemo da su *ortogonalni* ako skup[2]

$$\left\{\left(a_{ij}^{(1)}, a_{ij}^{(2)}\right) \ : \ i, j = 1, 2, \ldots, n\right\}$$

sadržava n^2 različitih uređenih parova. Očito je ekvivalentno zahtijevati da je

$$\left(a_{i_1 j_1}^{(1)}, a_{i_1 j_1}^{(2)}\right) \neq \left(a_{i_2 j_2}^{(1)}, a_{i_2 j_2}^{(2)}\right), \text{ čim je } i_1 \neq i_2 \text{ ili } j_1 \neq j_2.$$

Kažemo da je skup $\{A_1, A_2, \ldots, A_t\}$ latinskih kvadrata istog reda *ortogonalan* ako su svaka dva različita elementa tog skupa ortogonalna.

Napomena. Uz ortogonalne latinske kvadrate veže se jedna poznata Eulerova hipoteza: Ako je $n \equiv 2 \pmod 4$, tada ne postoje ortogonalni latinski kvadrati reda n. Pokazalo se poslije da je hipoteza pogrešna, točnije, da postoje ortogonalni latinski kvadrati reda n za $n \in \mathbb{N} \setminus \{2, 6\}$. Više o tome vidi u [2], str. 151.–152.

Propozicija 1. *Neka je $S = \{A_1, A_2, \ldots, A_t\}$ ortogonalan skup latinskih kvadrata, reda $n \geq 3$. Tada je $t \leq n - 1$.*

Dokaz. Budući da nam je bitan samo raspored elemenata u latinskom kvadratu, a ne svojstva samih elemenata, možemo bez smanjenja općenitosti svakom posebno preimenovati elemente; time nećemo pokvariti ni definicijska svojstva latinskog kvadrata, niti ortogonalnost s drugim latinskim kvadratima, naravno, uz uvjet da različitim elementima pridružimo različito ime. Svakom latinskom kvadratu $A_i \in S$ preimenujmo prvi redak u $(1 \ 2 \ \ldots \ n)$. Budući da se u prvom

[1] Možemo bez smanjenja općenitosti uzimati da je riječ o skupu $\{1, 2, \ldots, n\}$.
[2] Skup dobiven *superpozicijom* matrica A_1 i A_2.

retku od A_i nalazi svaki element (točno jednom), time su jedinstveno određena imena elemenata u svim preostalim retcima od A_i. Dakle, možemo smatrati da su

$$A_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 2 & \dots & n \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}, \quad \dots$$

$$\dots, \quad A_t = \begin{pmatrix} 1 & 2 & \dots & n \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Promotrimo koji brojevi mogu biti na mjestu $(2, 1)$ u tim matricama. Tu ne može biti 1, jer su te matrice latinski kvadrati. Također, zbog međusobne ortogonalnosti, ti brojevi očito moraju biti različiti za različite matrice, kojih ima t. Brojevi su iz skupa $\{2, 3, \dots, n\}$, pa slijedi $t \leq n - 1$, tj. tvrdnja teorema. $\square$

Napomena. Gornji dokaz možemo provesti i u slučaju $n = 2$, te zaključiti da ne postoje dva različita ortogonalna latinska kvadrata reda 2.

Primjer 2. Latinski kvadrati M i N iz primjera 1 su ortogonalni, jer njihovom superpozicijom dobivamo skup

$$\left\{ \begin{matrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{matrix} \right\}$$

u kojem se nalaze svi mogući uređeni parovi elemenata iz skupa $\{1, 2, 3\}$. Možemo po propoziciji 1 zaključiti da ne postoji ni jedan latinski kvadrat koji bi istovremeno bio ortogonalan s M i N.

Sada kada znamo da postoje ortogonalni latinski kvadrati, te kada imamo gornju među za njihov broj, postavlja se pitanje koliko ih zapravo može biti za zadani red. Odgovor na to općenito nije poznat. Međutim, u nekim posebnim slučajevima ipak možemo primjetiti da se ta gornja međa postiže. To je sadržaj sljedećeg teorema.

Definicija. Ako ortogonalan skup latinskih kvadrata reda n ima $n-1$ element, kažemo da je taj skup *potpun* (ili *zasićen*).

Teorem 2. *Neka je n prim-potencija*[3]*. Tada postoji potpun skup ortogonalnih latinskih kvadrata reda n.*

Dokaz. Za brojeve oblika $n = p^m$ postoji konačno (Galoisovo) polje reda n, u oznaci $(GF(n), +, \cdot)$ – vidi [1], str. 280. Neka su svi (međusobno različiti) elementi tog polja sljedeći[4]: $a_0 = 0$, $a_1 = 1$, a_2, a_3, $\dots$, a_{n-1}. Definirajmo matrice

$$A_k = \left(a_{ij}^{(k)}\right)_{i,j=0,1,\dots,n-1} \qquad k = 1, 2, \dots, n-1 \tag{1}$$

[3] *Prim-potencija* je broj oblika p^n za neke brojeve $p, n \in \mathbb{N}$, gdje je p prost broj.

[4] Standardno, 0 je neutralni element za operaciju $+$, a 1 za operaciju $\cdot$ u danom polju.

na sljedeći način:

$$a_{ij}^{(k)} := a_k a_i + a_j \qquad i,j = 0,1,\ldots,n-1 \quad k = 1,2,\ldots,n-1. \tag{2}$$

Dokažimo da je svaka matrica iz (1) latinski kvadrat. Budući da u našem polju ima n elemenata, kao i mjesta u svakom retku (stupcu) matrice A_k, dovoljno je dokazati da se u svakom retku (stupcu) pojavljuju samo različiti elementi. Pretpostavimo da matrica A_k u istom retku ima dva ista elementa, tj. neka je $a_{ij_1}^{(k)} = a_{ij_2}^{(k)}$. Zbog (2) vrijedi:

$$a_k a_i + a_{j_1} = a_k a_i + a_{j_2} \quad \Rightarrow \quad a_{j_1} = a_{j_2} \quad \Rightarrow \quad j_1 = j_2,$$

pa vidimo da ti elementi moraju biti i u istom stupcu. Slično za stupce, pretpostavimo da matrica A_k u istom stupcu ima dva ista elementa, tj. $a_{i_1 j}^{(k)} = a_{i_2 j}^{(k)}$. Opet zbog (2) imamo:

$$a_k a_{i_1} + a_j = a_k a_{i_2} + a_j \quad \Rightarrow \quad a_k a_{i_1} = a_k a_{i_2} \quad \Rightarrow \quad a_k(a_{i_1} - a_{i_2}) = 0.$$

Sad iskoristimo činjenicu da u polju nema djelitelja nule, te $a_k \neq 0$ (jer je $k > 0$), pa imamo

$$a_{i_1} - a_{i_2} = 0 \quad \Rightarrow \quad a_{i_1} = a_{i_2} \quad \Rightarrow \quad i_1 = i_2.$$

Dakle, matrice (1) su latinski kvadrati (reda n). Dokažimo još da su svaka dva međusobno ortogonalna. Neka su $k, k' \in \{1,2,\ldots,n-1\}$ međusobno različiti. Uočimo da je tada i $a_k \neq a_{k'}$, tj. $a_k - a_{k'} \neq 0$. Pretpostavimo da za neke $i_1, i_2, j_1, j_2 \in \{0,1,\ldots,n-1\}$ vrijedi

$$\left(a_{i_1 j_1}^{(k)}, a_{i_1 j_1}^{(k')}\right) = \left(a_{i_2 j_2}^{(k)}, a_{i_2 j_2}^{(k')}\right).$$

To povlači $a_{i_1 j_1}^{(k)} = a_{i_2 j_2}^{(k)}$ i $a_{i_1 j_1}^{(k')} = a_{i_2 j_2}^{(k')}$, iz čega slijede izrazi

$$a_k a_{i_1} + a_{j_1} = a_k a_{i_2} + a_{j_2}, \tag{3}$$

$$a_{k'} a_{i_1} + a_{j_1} = a_{k'} a_{i_2} + a_{j_2}. \tag{4}$$

Nakon što od (3) oduzmemo (4) te iskoristimo komutativnost, asocijativnost i distributivnost u polju, dobijemo

$$(a_k - a_{k'}) a_{i_1} = (a_k - a_{k'}) a_{i_2} \quad \Rightarrow \quad (a_k - a_{k'})(a_{i_1} - a_{i_2}) = 0$$

$$\Rightarrow \quad a_{i_1} - a_{i_2} = 0 \quad \Rightarrow \quad a_{i_1} = a_{i_2} \quad \Rightarrow \quad i_1 = i_2.$$

Nakon što izraz $i_1 = i_2$ stavimo u (3), trivijalno slijedi i $j_1 = j_2$, pa su latinski kvadrati A_k i $A_{k'}$ ortogonalni (uočimo da to povlači i da su međusobno različiti). Stoga je skup $\{A_1, A_2, \ldots, A_{n-1}\}$ ortogonalan te sadržava $n-1$ različitih elemenata, pa je potpun. $\square$

Sljedeći teorem nama je više tehničkog karaktera, iako je značajan i sam za sebe (npr. u *teoriji kodiranja*).

Teorem 3. *Neka su $n \geq 3$, $t \geq 2$ prirodni brojevi. Postoji ortogonalan skup od t latinskih kvadrata reda n ako i samo ako postoji matrica tipa $(t+2, n^2)$ s elementima iz skupa $\{1, 2, \dots, n\}$, koja ima svojstvo da stupci svake podmatrice tipa $(2, n^2)$ tvore n^2 različitih uređenih parova iz skupa $\{1, 2, \dots, n\}$, ili ekvivalentno tomu, da se pojavljuju svi mogući uređeni parovi elemenata iz tog skupa.*[5] *Nazovimo to svojstvo $(*)$.*

Dokaz. Neka su

$$A_1 = \left(a_{ij}^{(1)}\right)_{ij}, \quad A_2 = \left(a_{ij}^{(2)}\right)_{ij}, \quad \dots, \quad A_t = \left(a_{ij}^{(t)}\right)_{ij}$$

t latinskih kvadrata reda n, takvih da su svaka dva različita međusobno ortogonalna. Neka su, bez smanjenja općenitosti, elementi svih tih latinskih kvadrata iz skupa $\{1, 2, \dots, n\}$. Posložimo elemente tih matrica u matricu tipa $(t+2, n^2)$ na sljedeći način:

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 2 & 2 & \dots & 2 & \dots & n & n & \dots & n \\ 1 & 2 & \dots & n & 1 & 2 & \dots & n & \dots & 1 & 2 & \dots & n \\ a_{11}^{(1)} & a_{12}^{(1)} & \dots & a_{1n}^{(1)} & a_{21}^{(1)} & a_{22}^{(1)} & \dots & a_{2n}^{(1)} & \dots & a_{n1}^{(1)} & a_{n2}^{(1)} & \dots & a_{nn}^{(1)} \\ a_{11}^{(2)} & a_{12}^{(2)} & \dots & a_{1n}^{(2)} & a_{21}^{(2)} & a_{22}^{(2)} & \dots & a_{2n}^{(2)} & \dots & a_{n1}^{(2)} & a_{n2}^{(2)} & \dots & a_{nn}^{(2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{11}^{(t)} & a_{12}^{(t)} & \dots & a_{1n}^{(t)} & a_{21}^{(t)} & a_{22}^{(t)} & \dots & a_{2n}^{(t)} & \dots & a_{n1}^{(t)} & a_{n2}^{(t)} & \dots & a_{nn}^{(t)} \end{pmatrix}.$$

Nazovimo tu matricu A. Ako primijetimo da je svaka podmatrica tipa $(2, n^2)$ matrice A zapravo kombinacija 2 različita retka matrice A, lako se vidi da joj stupci tvore sve različite uređene parove (njih n^2). Naime, za prva dva retka poprilično je jasno. Ako bi i-ti redak $(2 < i \leq t+2)$ s prvim ili drugim retkom tvorio dva jednaka uređena para, to bi bilo u kontradikciji s činjenicom da je A_{i-2} latinski kvadrat. Ako bi i-ti i j-ti redak $(2 < i < j \leq t+2)$ tvorili dva jednaka uređena para, to bi bilo u kontradikciji s ortogonalnošću latinskih kvadrata A_{i-2} i A_{j-2}. Dakle, matrica A ima i svojstvo $(*)$.
Obrnuto, neka je A' matrica tipa $(t+2, n^2)$, s elementima iz $\{1, 2, \dots, n\}$, koja ima svojstvo $(*)$. Primijetimo očitu činjenicu da se svaki broj u svakom retku pojavljuje točno n puta. Naime, ako bi se neki broj k pojavljivao više od n puta u i-tom retku, tada bi tvorio više od n uređenih parova oblika $(k, \text{nešto})$, u nekoj podmatrici u kojoj se nalazi i-ti redak, pa bi neka dva para morala biti jednaka. Ako bi se pak k pojavljivao manje od n puta, tada bi se neki drugi broj k' morao pojaviti više od n puta, pa provedemo analogno razmatranje za k'. Također primijetimo da se svojstvo $(*)$ neće pokvariti pri permutiranju stupaca A', pa možemo pretpostaviti da A' ima prvi redak kao matrica A. Promotrimo početni komad duljine n drugog retka matrice A'. Iznad tog komada nalaze

[5] Takvu matricu zovemo *ortogonalna shema reda n, jakosti* 2 *i indeksa* 1. Za detalje vidi [3], str. 25. ili [2] str. 140. odnosno str. 225.

se samo jedinice, pa prvih n stupaca možemo permutirati da nam taj početni komad bude $(1 \quad 2 \quad \ldots \quad n)$, a da se ne promijeni prvi redak. To ponovimo i za sljedeći blok duljine n (ispod dvojki), te analogno sve do kraja drugog retka. Dobili smo da prva dva retka matrice A' izgledaju kao prva dva retka matrice A, te je ostalo sačuvano svojstvo $(*)$. Dakle, bez smanjenja općenitosti, neka je $A' = A$. Sad očito možemo reverzibilnim postupkom (dobivanja matrice A iz skupa $\{A_1, A_2, \ldots, A_t\}$) iz matrice A dobiti skup $S := \{A_1, A_2, \ldots, A_t\}$. Lako se vidi kako svojstvo $(*)$ i prva dva retka matrice A garantiraju da su matrice $A_1, A_2, \ldots, A_t$ latinski kvadrati. Jednako je lako vidjeti da svojstvo $(*)$ povlači i međusobnu ortogonalnost od A_i i A_j, za međusobno različite $i, j = 1, 2, \ldots, t$. Stoga je S ortogonalan skup od t latinskih kvadrata reda n. $\square$

Primjer 3. Ortogonalna shema latinskih kvadrata M i N primjera 1 je

$$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 2 & 3 & 2 & 3 & 1 & 3 & 1 & 2 \\ 1 & 2 & 3 & 3 & 1 & 2 & 2 & 3 & 1 \end{pmatrix}.$$

Primjer 4. Dva ortogonalna latinska kvadrata reda 10 (prvi se dobije uzimajući u obzir samo znamenke jedinica brojeva u matrici, a drugi gledajući samo znamenke desetica):

$$\begin{pmatrix} 00 & 67 & 58 & 49 & 91 & 83 & 75 & 12 & 24 & 36 \\ 76 & 11 & 07 & 68 & 59 & 92 & 84 & 23 & 35 & 40 \\ 85 & 70 & 22 & 17 & 08 & 69 & 93 & 34 & 46 & 51 \\ 94 & 86 & 71 & 33 & 27 & 18 & 09 & 45 & 50 & 62 \\ 19 & 95 & 80 & 72 & 44 & 37 & 28 & 56 & 61 & 03 \\ 38 & 29 & 96 & 81 & 73 & 55 & 47 & 60 & 02 & 14 \\ 57 & 48 & 39 & 90 & 82 & 74 & 66 & 01 & 13 & 25 \\ 21 & 32 & 43 & 54 & 65 & 06 & 10 & 77 & 88 & 99 \\ 42 & 53 & 64 & 05 & 16 & 20 & 31 & 89 & 97 & 78 \\ 63 & 04 & 15 & 26 & 30 & 41 & 52 & 98 & 79 & 87 \end{pmatrix}.$$

Za kraj odjeljka spomenimo da ne postoji „elegantna" matematička teorija uz pomoć koje bi se tražile familije ortogonalnih latinskih kvadrata. Uglavnom se za proučavanje ortogonalnih latinskih kvadrata koriste računalne metode za nalaženje, te asimptotske formule za broj takvih.

2 Konačne projektivne ravnine

U ovom odjeljku želimo istaknuti samo kombinatorna svojstva projektivnih ravnina, dok geometrijska svojstva zanemarujemo (npr. ne zanima nas je li neka projektivna ravnina *Desarguesova*[6]).

[6]Vidi npr. [5], str. 26.

Definicija. *(Konačna) projektivna ravnina* Π (*reda* $n \in \mathbb{N} \setminus \{1\}$) je uređena trojka $(\mathcal{T}, \mathcal{P}, \mathbf{I})$ nepraznih skupova; elemente skupa $\mathcal{T}$ zovemo *točke*, skupa $\mathcal{P}$ *pravci*, a $\mathbf{I} \subseteq \mathcal{T} \times \mathcal{P}$ je binarna relacija koju zovemo *relacija incidencije* (ako je $(T, p) \in \mathbf{I}$, kažemo da točka T *leži na* pravcu p, ili pak da pravac p *prolazi* točkom T), te vrijedi[7]:

(P1) Za svake dvije različite točke postoji jedinstven pravac na kojem obje leže;

(P2) Za svaka dva različita pravca postoji jedinstvena točka kojom oba prolaze;

(P3) Svakom točkom prolazi točno $n+1$ pravac;

(P4) Na svakom pravcu leži točno $n+1$ točka.

Za dva različita pravca koja prolaze istom točkom kažemo da se *sijeku* u toj točki, te je ona *sjecište* danih pravaca. Za pravac koji prolazi kroz dvije različite točke kažemo da je *spojnica* tih dviju točaka, tj. da *spaja* te dvije točke.

Napomena. Primijetimo da je definicija projektivne ravnine simetrična s obzirom na pojmove *točka* i *pravac*. Stoga koju god tvrdnju dokažemo, vrijedit će i njoj *dualna* tvrdnja dobivena zamjenom pojmova *točka*$\leftrightarrow$*pravac* i svih izvedenih pojmova.

Primjer 5. Ako stavimo $\mathcal{T} := \{1, 2, \ldots, 7\}$ i

$$\mathcal{P} := \Big\{\{1,2,3\}, \{3,4,5\}, \{1,5,6\}, \{1,4,7\}, \{2,5,7\}, \{3,6,7\}, \{2,4,6\}\Big\},$$

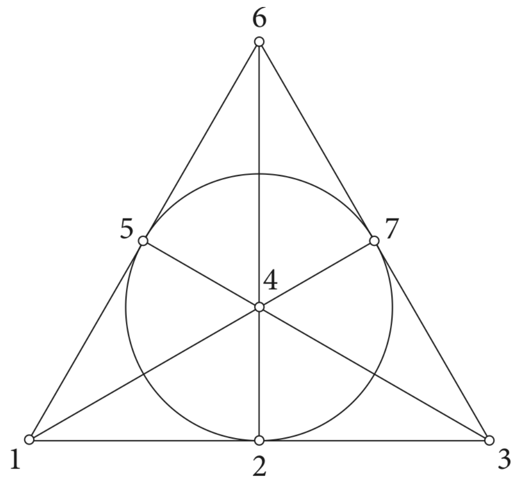
tada se lako provjeri da je $(\mathcal{T}, \mathcal{P}, \in)$ projektivna ravnina reda 2, koju zovemo *Fanova ravnina*. Možemo je predočiti slikom:

Propozicija 4. *Projektivna ravnina reda* n *sadržava* $n^2 + n + 1$ *točku i isto toliko pravaca.*

Dokaz. Neka je P bilo koja točka spomenute projektivne ravnine. Kroz nju (po (P3)) prolazi $n+1$ različitih pravaca, pri čemu na svakom leži n različitih točaka koje nisu P (po (P4)). Ti se pravci sijeku u P pa nemaju drugih zajedničih točaka (po (P2)). Dakle, imamo $1 + (n+1) \cdot n = n^2 + n + 1$ različitih točaka. Ostaje provjeriti ima li preostalih. Ako je Q neka točka različita od P, onda (po (P1)) postoji pravac koji ih spaja. Taj pravac jedan je od onih $n+1$, pa smo točku Q već uračunali. Dakle, točaka ima n^2+n+1, a po prethodnoj napomeni isto toliko ima i pravaca. $\square$

Sljedećim teoremom potpuno razotkrivamo vezu između projektivne ravnine reda n i potpunog skupa ortogonalnih latinskih kvadrata reda n. Izlazi da je ta veza 1–1 korespondencija. Štoviše, u dokazu dajemo efektivan način konstrukcije jedne strukture iz druge. To će, u kombinaciji s rezultatima iz prethodnog odjeljka osigurati neke dovoljne uvjete za egzistenciju projektivnih ravnina.

[7] *Projektivna ravnina* najčešće se definira uz pomoć tri aksioma: (P1)), (P2) i (P5): postoje 4 točke od kojih tri ne leže na istom pravcu. Ako je neki od skupova $\mathcal{T}$ ili $\mathcal{P}$ konačan, tada se pokazuje da vrijede (P3) i (P4) za neki $n \in \mathbb{N}$, koji tada zovemo *red* dane projektivne ravnine. Za datalje vidi npr. [4], str. 79. ili [5], str. 55.



Slika 1: Fanova ravnina – projektivna ravnina reda 2.

Teorem 5. *Neka je $n \geq 3$ prirodan broj. Postoji projektivna ravnina reda n ako i samo ako postoji potpun skup ortogonalnih latinskih kvadrata reda n.*

Dokaz. Neka je dana projektivna ravnina reda n, te fiksirajmo neki pravac p. Neka su sve (međusobno različite) točke koje leže na pravcu p sljedeće: $P_1, P_2, \ldots, P_{n+1}$. Preostalo je $n^2+n+1-(n+1) = n^2$ različitih točaka koje ne leže na pravcu p. Neka su sve takve $Q_1, Q_2, \ldots, Q_{n^2}$. Kroz svaku točku P_i prolazi još n različitih pravaca koji nisu p, pa tim n injektivno pridružimo oznake iz skupa $\{1, 2, \ldots, n\}$, za $i = 1 \ldots n+1$ (dakle, dva pravca s istom oznakom ne moraju biti jednaka, dok dva pravca s istom oznakom koja oba prolaze točkom P_i, za neki $i \in \{1, 2, \ldots, n+1\}$ moraju biti isti pravac). Definirajmo a_{ij} kao pravac koji je jedinstveno određen točkama P_i i Q_j, te promotrimo matricu

$$A := \big(\text{oznaka od } a_{ij}\big)_{i=1,2,\ldots,n+1, j=1,2,\ldots,n^2}$$

tipa $(n+1, n^2)$. Elementi te matrice očito su iz skupa $\{1, 2, \ldots, n\}$. Dokažimo da A ima svojstvo $(*)$. Ako pretpostavimo da nije tako, tada postoje međusobno različiti $i_1, i_2 \in \{1, 2, \ldots, n+1\}$ i međusobno različiti $j_1, j_2 \in \{1, 2, \ldots, n^2\}$ takvi da vrijedi

$$(\text{oznaka od } a_{i_1 j_1},\ \text{oznaka od } a_{i_2 j_1}) = (\text{oznaka od } a_{i_1 j_2},\ \text{oznaka od } a_{i_2 j_2}).$$

Izjednačavanjem prvih komponenti uređenih parova dobijemo da je oznaka od $a_{i_1 j_1}$ ista kao i oznaka od $a_{i_1 j_2}$, za pravce $a_{i_1 j_1}$ i $a_{i_1 j_2}$ koja oba prolaze točkom P_{i_1}. Stoga mora biti $a_{i_1 j_1} = a_{i_1 j_2}$. Potpuno analogno je i $a_{i_2 j_1} = a_{i_2 j_2}$. Neka je q pravac određen točkama Q_{j_1} i Q_{j_2}. Vrijedi:

$$Q_{j_1} \text{ leži na } a_{i_1 j_1} = a_{i_1 j_2},\ Q_{j_2} \text{ leži na } a_{i_1 j_2} \overset{(P1)}{\Rightarrow} q = a_{i_1 j_2} \Rightarrow P_{i_1} \text{ leži na } q.$$

Potpuno analogno vidi se da i P_{i_2} leži na q, pa je $p = q$ (po (P1)). To povlači da Q_{j_1} leži na p, što je očita kontradikcija. Dakle, matrica A tipa $(n+1, n^2)$, s elementima iz skupa $\{1, 2, \ldots, n\}$, ima svojstvo $(*)$. Prema teoremu 3, postoji $(n-1)$-člani ortogonalan skup latinskih kvadrata reda n, a to je upravo potpuni skup ortogonalnih latinskih kvadrata reda n.
Obrnuto, ako postoji potpuni ortogonalni skup latinskih kvadrata reda n, tada po teoremu 3 postoji matrica A tipa $(n+1, n^2)$, s elementima iz $\{1, 2, \ldots, n\}$, koja ima svojsto $(*)$. Stupce matrice A proglasimo točkama $Q_1, Q_2, \ldots, Q_{n^2}$ (zbog svojstva $(*)$ svaka dva stupca su različita), te uvedimo i dodatne točke $P_1, P_2, \ldots, P_{n+1}$. Neka pravac p sadržava točke $P_1, P_2, \ldots, P_{n+1}$ i samo te. Uzmimo da pravac p_{ij}, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n+1$ prolazi točkom P_j, te onima i samo onima Q_k $(k = 1, 2, \ldots, n^2)$ kojima se u j-tom retku nalazi broj i. Provjerimo da je konstrukcija dobra, tj. da smo zaista dobili projektivnu ravninu (potrebno je provjeriti aksiome (P1)–(P4)):

(P1): Za kombinaciju točaka P_i i P_j $(i, j = 1, 2, \ldots, n+1,\ i \neq j)$ jasno vrijedi – pravac p je jedini koji ih spaja). Također je jasno i za kombinaciju Q_i i P_j $(i = 1, 2, \ldots, n^2,\ j = 1, 2, \ldots, n+1)$ – jedino ih spaja pravac p_{kj}, gdje je k broj na mjestu (j, i) matrice A. Za kombinaciju Q_i i Q_j $(i, j = 1, 2, \ldots, n^2,$ $i \neq j)$ dovoljno je pokazati da i-ti i j-ti stupac matrice A imaju u točno jednom retku isti broj (reći ćemo da se *preklapaju* točno jednom). Budući da se svaki broj, u svakom retku matrice A javlja točno n puta, broj svih preklapanja svih stupaca je $\binom{n}{2} \cdot n \cdot (n+1)$. Očito se zbog svojstva $(*)$ dva različita stupca mogu preklapati najviše jednom. Ako se neka dva stupca ne preklapaju, tada je

$$\binom{n^2}{2} > \binom{n}{2} \cdot n \cdot (n+1) \quad \Rightarrow \quad \frac{n^2(n^2-1)}{2} > \frac{n^2(n-1)(n+1)}{2},$$

što je nemoguće. Dakle, svaka dva stupca preklapaju se točno jednom. Neka se broj k nalazi u stupcima i i j matrice A, u istom retku r. Sada je jasno da je p_{kr} jedini pravac koji spaja točke Q_i i Q_j.

(P2): Za pravce p i p_{ij} $(i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, n+1)$ očito vrijedi, sijeku se samo u točki P_j. Također je jasno da je jedina zajednička točka pravaca $p_{i_1 j}$ i $p_{i_2 j}$ $(i_1, i_2 = 1, 2, \ldots, n,\ i_1 \neq i_2,\ j = 1, 2, \ldots, n+1)$ upravo P_j. Sad promotrimo pravce $p_{i_1 j_1}$ i $p_{i_2 j_2}$ $(i_1, i_2 = 1, 2, \ldots, n,\ j_1, j_2 = 1, 2, \ldots, n+1,$ $j_1 \neq j_2)$. Redci j_1 i j_2 matrice A (svojstvo $(*)$) tvorit će sve uređene parove iz skupa $\{1, 2, \ldots, n\}$, pa među ostalim i par (i_1, i_2), i to točno jednom. Zato promatrani pravci imaju jedinstveno sjecište.

(P3): Za točke P_i $(i = 1, 2, \ldots, n+1)$ očito vrijedi. Međutim, vrijedi i za Q_j $(j = 1, 2, \ldots, n^2)$, jer se u svakom stupcu matrice A nalazi $n+1$ brojeva.

(P4): Za pravac p očito vrijedi. Pravac p_{ij} $(i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, n+1)$ osim P_j, sadržava još točno n različitih točaka, jer se u j-tom retku matrice A broj i pojavljuje točno n puta.

Dakle, konstruirali smo projektivnu ravninu, koja je očigledno reda n. Time je teorem potpuno dokazan. $\square$

Sada smo se domogli glavnog rezultata ovog odjeljka:

Korolar 6 (Veblen–Bussey)**.** *Za svaku prim-potenciju p^n postoji projektivna ravnina reda p^n.*

Dokaz. Za $p^n = 2$ imamo Fanovu ravninu. Za ostale prim-potencije egzistencija slijedi direktno iz teorema 2 i teorema 5. $\square$

Prirodno se postavlja pitanje vrijedi li obrat korolara 6 (je li red svake konačne projektivne ravnine prim-potencija?). To pitanje i dalje nije riješeno, te je preraslo u tzv. *hipotezu o prim-potencijama*[8], koja kaže da je red svake konačne projektivne ravnine prim-potencija. Rezultat koji bi bio najbliži spomenutoj hipotezi dali su još 1949. godine R. H. Bruck i H. J. Ryser, a mi ćemo ga dokazati. Međutim, bit će nam potrebni neki netrivijalni rezultati iz teorije brojeva.

3 Rezultati iz teorije brojeva

Dokazi sljedećih dvaju teorema nisu trivijalni te nemaju direktne veze s našom temom. Stoga ćemo navesti samo iskaze teorema, uz naznaku gdje se ti dokazi mogu pronaći.

Teorem 7. *Broj $n \in \mathbb{N}$ može se zapisati u obliku $n = k^2 + m^2$ za neke $k, m \in \mathbb{Z}$ ako i samo ako se u rastavu broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.*

Dokaz. Vidi [6], str. 43. $\square$

Teorem 8 (Lagrange)**.** *Za svaki $n \in \mathbb{N}$ postoje $x, y, z, w \in \mathbb{Z}$ takvi da je*

$$n = x^2 + y^2 + z^2 + w^2.$$

Dokaz. Vidi [6], str. 44.–45. $\square$

Lema 9. *Neka je $n \in \mathbb{N}$ takav da je $n = p^2 + q^2$ za neke $p, q \in \mathbb{Q}$. Tada postoje $m, k \in \mathbb{Z}$ takvi da je $n = m^2 + k^2$.*

Dokaz. Neka je $n = \left(\frac{p_1}{q_1}\right)^2 + \left(\frac{p_2}{q_2}\right)^2$, gdje su $p_1, p_2 \in \mathbb{Z}$, $q_1, q_2 \in \mathbb{N}$. Slijedi $(q_1q_2)^2 n = p_1^2 + p_2^2$. Po teoremu 7 slijedi da se u prikazu broja $(q_1q_2)^2 n$ na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom. U prikazu broja $(q_1q_2)^2$ na proste faktore očito se svaki prosti faktor javlja s parnom potencijom. Dakle, u prikazu broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja se s parnom potencijom. Po teoremu 7 slijedi da je $n = k^2 + m^2$ za neke $k, m \in \mathbb{Z}$. $\square$

[8] Eng. „*Prime power conjecture*".

Lema 10. *Za brojeve $a, b, c, d, x, y, w, z \in \mathbb{R}$ vrijedi identitet*

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = \\ = (ax-by-cz-dw)^2+(bx+ay-dz+cw)^2+ \\ +(cx+dy+az-bw)^2+(dx-cy+bz+aw)^2.\end{aligned}$$

Dokaz. Trivijalan je posao izmnožiti obje strane i provjeriti jednakost. □

Za potrebe sljedećeg dokaza bit će nam zgodna i sljedeća definicija.

Definicija. Reći ćemo da uređena četvorka $(x, y, z, w) \in \mathbb{Z}^4$ *reprezentira* broj $t \in \mathbb{Z}$ ako je $t = x^2 + y^2 + z^2 + w^2$.

4 Bruck–Ryserov teorem

Teorem 11 (Bruck–Ryser)**.** *Neka je Π projektivna ravnina reda n te neka je $n \equiv 1$ ili $2 \pmod 4$. Tada je $n = k^2 + m^2$ za neke $k, m \in \mathbb{Z}$.*

Dokaz. Neka je Π projektivna ravnina reda n te neka je $n \equiv 1$ ili $2 \pmod 4$. Po propoziciji 4, ravnina Π sadržava $n^2 + n + 1 =: v$ točku, i jednako toliko pravaca. Lako je vidjeti da je $v + 1 \equiv 0 \pmod 4$. Neka su $P_1, P_2, \ldots, P_v$ točke, a $l_1, l_2, \ldots, l_v$ pravci ravnine Π. Neka su $x_1, x_2, \ldots, x_v$ varijable s vrijednostima u $\mathbb{R}$, te označimo

$$L_i := \sum_{\{j\ :\ P_j \text{ leži na } l_i\}} x_j, \qquad i = 1, 2, \ldots, v. \tag{5}$$

Vrijede identiteti:

$$\sum_{i=1}^{v} L_i^2 = 2\sum_{i=1}^{v}\sum_{j=i+1}^{v} x_i x_j + (n+1)\sum_{i=1}^{v} x_i^2, \tag{6}$$

$$\sum_{i=1}^{v} L_i^2 = n\sum_{i=1}^{v} x_i^2 + \Big(\sum_{i=1}^{v} x_i\Big)^2. \tag{7}$$

Identitet (6) dobijemo tako da nakon kvadriranja identiteta (5) i sumiranja po $i = 1, 2, \ldots, v$ iskoristimo aksiome (P1) i (P3). Identitet (7) je malo zgodnije zapisan identitet (6). Uvedimo još jednu varijablu x_{v+1} s vrijednošću u $\mathbb{R}$ te pribrojimo nx_{v+1}^2 u (7). Dobijemo

$$\sum_{i=1}^{v} L_i^2 + nx_{v+1}^2 = n\sum_{i=1}^{v+1} x_i^2 + T^2, \tag{8}$$

gdje je $T := \sum_{i=1}^{v} x_i$. Po teoremu 8 postoje nenegativni brojevi $a, b, c, d \in \mathbb{Z}$ takvi da je $n = a^2 + b^2 + c^2 + d^2$. Neka je matrica $A_n \in M_4(\mathbb{R})$ dana s

$$A_n := \begin{pmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{pmatrix}.$$

Nije teško vidjeti da je $\det A_n = (a^2+b^2+c^2+d^2)^2 = n^2 \neq 0$, pa je A_n regularna matrica. Ako (x,y,z,w) reprezentira broj t, tada lema 10 povlači da $(x,y,z,w)A_n$ reprezentira broj tn. Zato možemo pisati

$$n(x_1^2+x_2^2+x_3^2+x_4^2) = y_1^2+y_2^2+y_3^2+y_4^2, \tag{9}$$

gdje je

$$(y_1,y_2,y_3,y_4) = (x_1,x_2,x_3,x_4)A_n. \tag{10}$$

Sustav (10) možemo napisati u obliku

$$(x_1,x_2,x_3,x_4) = (y_1,y_2,y_3,y_4)A_n^{-1}.$$

Primijetimo da su elementi matrice A_n^{-1} iz $\mathbb{Q}$. Dakle, svaki x_1,x_2,x_3,x_4 je linearna kombinacija varijabli y_1,y_2,y_3,y_4 s racionalnim koeficijentima. Te linearne kombinacije zajedno s (9) uvrstimo u (8) te dobijemo

$$\sum_{i=1}^{v} L_i^2 + nx_{v+1}^2 = y_1^2+y_2^2+y_3^2+y_4^2+n\sum_{i=5}^{v+1} x_i^2 + T^2,$$

gdje su $L_1,L_2,\ldots,L_v,T$ linearne kombinacije (s racionalnim koeficijentima) varijabli y_1,y_2,y_3,y_4,$x_5,x_6,\ldots,x_{v+1}$. Isti postupak napravimo i za sljedeću uređenu četvorku (x_5,x_6,x_7,x_8), i tako dalje, sve do $(x_{v-2},x_{v-1},x_v,x_{v+1})$ jer je $v+1\equiv 0 \pmod 4$. Dobijemo identitet

$$\sum_{i=1}^{v} L_i^2 + nx_{v+1}^2 = \sum_{i=1}^{v+1} y_i^2 + T^2, \tag{11}$$

gdje su $L_1,L_2,\ldots,L_v,x_{v+1},T$ linearne kombinacije varijabli $y_1,y_2,\ldots,y_{v+1}$. Izraz (11) je valjan za svaku valuaciju varijabli $y_1,y_2,\ldots,y_{v+1}$. Želimo uzeti takav y_1 da bude $y_1^2=L_1^2$. Kako bismo se uvjerili da je to moguće, promotrimo sljedeća dva slučaja:

- Ako u linearnoj kombinaciji L_1, y_1 dolazi s koeficijentom 1, tada jednadžbu $y_1=-L_1$ očito možemo riješiti po y_1, tj. možemo za y_1 uzeti neku linearnu kombinaciju varijabli $y_2,y_3,\ldots,y_{v+1}$ takvu da je $y_1^2=L_1^2$.
- Ako u linearnoj kombinaciji L_1, y_1 dolazi s koeficijentom različitim od 1, tada možemo analogno izvesti isti zaključak kao u prošlom slučaju, proučavajući jednadžbu $y_1=L_1$.

Nakon te supstitucije, identitet (11) sada postaje

$$\sum_{i=2}^{v} L_i^2 + nx_{v+1}^2 = \sum_{i=2}^{v+1} y_i^2 + T^2,$$

gdje su $L_2,L_3,\ldots,L_v,x_{v+1},T$ linearne kombinacije varijabli $y_2,\ldots,y_{v+1}$. Ponavljajući taj postupak (za $y_2,y_3,\ldots,y_n$ redom), dobijemo identitet

$$nx_{v+1}^2 = y_{v+1}^2 + T^2, \tag{12}$$

gdje su x_{v+1}, T linearne kombinacije varijable y_{v+1}. Tada je $x_{v+1} = \alpha y_{v+1}$, $T = \beta y_{v+1}$ za neke $\alpha, \beta \in \mathbb{Q}$ (primijetimo da su koeficijenti svih linearnih kombinacija tijekom cijelog dokaza racionalni brojevi – ni jedan korak u dokazu nije za posljedicu imao gubitak racinalnosti koeficijenata). Izaberimo sada $y_{v+1} := 1$. Sada (12) povlači

$$n\alpha^2 = 1 + \beta^2 \quad \overset{\alpha \neq 0}{\Rightarrow} \quad n = \left(\frac{1}{\alpha}\right)^2 + \left(\frac{\beta}{\alpha}\right)^2, \quad \frac{1}{\alpha}, \frac{\beta}{\alpha} \in \mathbb{Q}.$$

Lema 9 povlači da je $n = m^2 + k^2$ za neke $m, k \in \mathbb{Z}$. □

Korolar 12 (Bruck–Ryser, alternativna formulacija)**.** *Ako je n prirodan broj za koji vrijedi $n \equiv 1$ ili $2 \pmod 4$ i ako nekvadratni dio[9] broja n u rastavu na proste faktore sadržava barem jedan prosti faktor p takav da je $p \equiv 3 \pmod 4$, tada ne postoji projektivna ravnina reda n.*

Dokaz. Pretpostavimo da postoji projektivna ravnina reda n te neka vrijedi $n \equiv 1$ ili $2 \pmod 4$. Tada je po teoremu 11 $n = m^2 + k^2$ za neke $m, k \in \mathbb{Z}$. Teorem 7 povlači da se u rastavu broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom. Očito tada nekvadratni dio broja n ne sadržava ni jedan prosti faktor p za koji je $p \equiv 3 \pmod 4$. Obratom po kontrapoziciji dobivamo tvrdnju korolara. □

Korolar 6 nam kaže da postoje projektivne ravnine redova 2, 3, 4, 5, 7, 8, 9, 11, ... Korolar 12 nam kaže da ne postoje projektivne ravnine redova 6, 14, 21, 22, ... Međutim, već za red 10, 12 ili 15 navedeni rezultati ne mogu nam dati odgovor. Može se lako pokazati da postoji beskonačno mnogo prirodnih brojeva za koje navedeni rezultati ne daju odgovor.
Krajem prošlog stoljeća uz pomoć računala je dokazano da ne postoji projektivna ravnina reda 10, dok je pitanje o postojanju projektivne ravnine reda 12 i dalje otvoren problem. Vidi [7].

5 Poopćenje

U ovom odjeljku iskazat ćemo poopćenje teorema 11, koje su našli H. J. Ryser i S. Chowla 1950. godine. No prije toga potrebno je definirati nešto općenitiju strukturu od konačne projektivne ravnine. Promatrat ćemo konačne projektivne ravnine s aspekta *teorije dizajna*.

Definicija. Neka su $v, k, \lambda \in \mathbb{N}$ takvi da je $v \geq k \geq 2$. Uređen par $(X, \mathcal{A})$, gdje je $\mathcal{A} \subseteq \mathcal{P}(X)$, zovemo (v, k, λ)-*balansiran nepotpun blok dizajn* (kraće ćemo pisati (v, k, λ)-*BIBD*[10]), ako vrijedi:

(B1) $\mathrm{card}(X) = v$;

(B2) Svaki *blok* (tj. element od $\mathcal{A}$) sadržava točno k elemenata;

[9] *Nekvadratni dio* broja $n \in \mathbb{N}$ je broj $\frac{n}{d^2}$, gdje je $d := \max\{k \in \mathbb{N} \, : \, k^2 \text{ dijeli } n\}$.
[10] Kratica BIBD dolazi od engleskog naziva "*balanced incomplete block design*".

(B3) Svaki neuređeni par različitih elemenata iz X nalazi se u točno λ blokova.

Nadalje, kažemo da je (v, k, λ)-BIBD *simetričan* ako je $\lambda(v-1) = k^2 - k$.

Sada nije teško vidjeti da je projektivna ravnina reda n zapravo $(n^2+n+1, n+1, 1)$-BIBD, uz identifikaciju: *pravac* $\leftrightarrow$ *blok* (tj. pravac smatramo skupom točaka koje na njemu leže). Štoviše, projektivna ravnina reda n simetričan je $(n^2+n+1, n+1, 1)$-BIBD. Sada smo u mogućnosti iskazati najavljeni teorem:

Teorem 13 (Bruck–Ryser–Chowla)**.** *Uzmimo da postoji simetričan* (v, k, λ)-*BIBD. Ako je* v *paran broj, tada je* $k - \lambda = w^2$ *za neki* $w \in \mathbb{Z}$. *Ako je* v *neparan broj, tada postoje* $x, y, z \in \mathbb{Z}$ *koji nisu svi nula, tako da vrijedi:*

$$x^2 = (k-\lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2. \tag{13}$$

Dokaz. Vidi [2], str. 30.–35. $\square$

Zašto je teorem 13 općenitiji slučaj teorema 11? Pretpostavimo da postoji projektivna ravnina reda n, tj. da postoji simetričan $(n^2+n+1, n+1, 1)$-BIBD, te primijetimo da je n^2+n+1 uvijek neparan broj.
Pretpostavimo prvo da je $n \equiv 0$ ili $3 \pmod 4$. Tada se jednakost (13) reducira na jednadžbu $x^2 = ny^2 + z^2$, koja uvijek ima netrivijalno rješenje $x = z = 1$, $y = 0$. Dakle, u slučaju $n \equiv 0$ ili $3 \pmod 4$ teorem Bruck–Ryser–Chowla ne daje odgovor o (ne)postojanju projektivne ravnine reda n.
Pretpostavimo sada da je $n \equiv 1$ ili $2 \pmod 4$. Tada se jednakost (13) reducira na $x^2 + z^2 = ny^2$, pa je (po lemi 9) $n = m^2 + k^2$ za neke $m, k \in \mathbb{Z}$, što je upravo tvrdnja teorema 11.

Literatura

[1] T. W. Hungerford, *Algebra*, Springer, 2003

[2] D. R. Stinson, *Combinatorial desings, construction and analysis*, Springer, 2004

[3] S. Radas, *Ortogonalni latinski kvadrati, magistarski rad*, PMF–Matematički odjel, Sveučilište u Zagrebu, 1988

[4] D. R. Huges, F. C. Piper, *Projective planes*, Springer, 1973

[5] D. Palman, *Projektivna geometrija*, Školska knjiga, 1984

[6] A. Dujella, *Uvod u teoriju brojeva, skripta*, PMF–Matematički odjel, Sveučilište u Zagrebu, `http://web.math.hr/~duje/utb/utblink.pdf`

[7] C. W. H. Lam, *The Search for a Finite Projective Plane of Order 10*, The American Mathematical Monthly Volume 98, Issue 4 (str. 305–318), 1991