

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

KONAČNE GEOMETRIJE

Predavanja

Juraj Šiftar
Vedran Krčadinac

Akadska godina 2012./2013.

Sadržaj

1	Uvod	1
2	Dizajni	7
3	Izomorfizam i automorfizmi	15
4	Simetrični dizajni i Hadamardove matrice	23
5	Projektivne i afine ravnine	31
5.1	Osnovno o konačnim poljima	31
5.2	Aksiomi i neki modeli projektivne ravnine	36
5.3	Desarguesova i Papposova konfiguracija	40
5.4	Automorfizmi (kolineacije) projektivnih ravnina	44
5.5	Afina ravnina	48
5.6	Primjer nedesarguesovske ravnine reda 9	51
6	Diferencijski skupovi	57
7	Teorem Brucka, Rysera i Chowle	65
8	Latinski kvadrati	73
9	Teorija kodiranja	79
9.1	Kodovi za ispravljanje pogrešaka	79
9.2	Linearni kodovi	82
9.3	Veze kodova i drugih konačnih struktura	89
10	Jedna primjena dizajna: algoritam za grupno testiranje	95
11	Rješenja nekih zadataka	99
	Bibliografija	101

Poglavlje 1

Uvod

Tema ove skripte su konačne pravilne matematičke strukture. Postoji više “jezika” kojim ih možemo opisati, npr. kao matrice ili grafove s određenim pravilnostima. Najviše ćemo koristiti jezik incidencijskih struktura i odgovarajuću geometrijsku terminologiju.

Definicija 1.1. Konačna incidencijska struktura je uređena trojka $(\mathcal{T}, \mathcal{B}, I)$. Pritom je $\mathcal{T}$ konačni skup čije elemente zovemo točkama, $\mathcal{B}$ je konačni skup čije elemente zovemo blokovima ili pravcima, a $I \subseteq \mathcal{T} \times \mathcal{B}$ je relacija koju zovemo incidencijom.

Ako je $(p, B) \in I$, pišemo $p I B$ i kažemo da točka p leži na bloku B ili da B prolazi kroz p . Skup svih točaka koje leže na B označavamo s $[B] = \{p \in \mathcal{T} \mid p I B\}$. Ako je pridruživanje $B \mapsto [B]$ injektivno, tj. ako su različiti blokovi incidentni s različitim skupovima točaka, blokove možemo identificirati s podskupovima od $\mathcal{T}$, a relaciju incidence s relacijom “biti element” $\in$. Takve incidencijske strukture nazivamo *jednostavnima*. Zanimaju nas konačne incidencijske strukture s dodatnim pravilnostima.

Definicija 1.2. Dizajn s parametrima (v, k, λ) je konačna incidencijska struktura sa svojstvima:

1. ukupan broj točaka je v ,
2. na svakom bloku leži točno k točaka,
3. kroz svake dvije točke prolazi točno λ blokova.

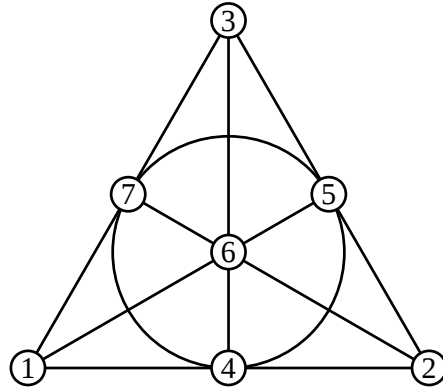
Puni naziv za ovakve strukture je *balansirani nepotpuni blokovni dizajn* ili BIBD (prema engleskom *balanced incomplete block design*).

Primjer 1.3. Neka je $\mathcal{T}$ bilo koji v -člani skup, a $\mathcal{B}$ skup svih k -članih podskupova od $\mathcal{T}$. Očito svake dvije točke možemo nadopuniti do k -članog podskupa na $\lambda = \binom{v-2}{k-2}$ načina. Prema tome, $(\mathcal{T}, \mathcal{B}, \in)$ je dizajn s parametrima $(v, k, \binom{v-2}{k-2})$. Zanimaju nas netrivialni dizajni, koji ne sadrže sve k -člane podskupove kao blokove.

Primjer 1.4. Neka je $\mathcal{T} = \{1, 2, 3, 4, 5, 6, 7\}$, a $\mathcal{B}$ sljedeći skup tročlanih podskupova:

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

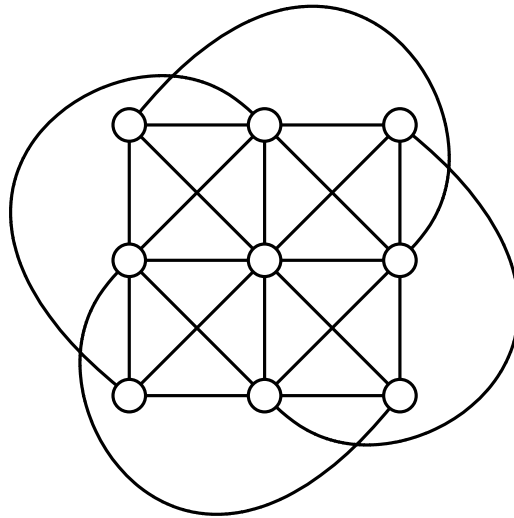
Tada je $(\mathcal{T}, \mathcal{B}, \in)$ dizajn s parametrima $(7, 3, 1)$ koji zovemo Fanovom ravninom ili projektivnom ravninom reda 2. Možemo ga prikazati na sljedeći način:



Slika 1.1: Projektivna ravnina reda 2.

Dizajn iz prethodnog primjera ima još jedno dobro svojstvo: ukupan broj točaka jednak je ukupnom broju blokova. Takve dizajne nazivamo *simetričnim dizajnima*.

Primjer 1.5. *Sljedeća slika predstavlja dizajn s parametrima $(9, 3, 1)$ koji nije simetričan. Nazivamo ga afinom ravninom reda 3.*



Slika 1.2: Afina ravnina reda 3.

Iz definicije dizajna slijede daljnje pravilnosti.

Propozicija 1.6. *Kroz svaku točku (v, k, λ) dizajna prolazi točno $r = \lambda \cdot \frac{v-1}{k-1}$ blokova.*

Dokaz. Označimo s r broj blokova koji prolaze kroz točku p_0 . Prebrojimo na dva načina elemente skupa

$$\{(p, B) \mid p \in \mathcal{T}, p \neq p_0, p, p_0 \text{ I } B\}.$$

Točku p možemo izabrati na $v - 1$ načina, a kad je zadamo postoji λ blokova B koji prolaze kroz p i p_0 . Prema tome, skup sadrži $(v - 1) \cdot \lambda$ parova. S druge strane, blok B kroz p_0 možemo izabrati na r načina, a na svakom leži $k - 1$ točaka p različitih od p_0 . Dakle, parova ima $r \cdot (k - 1)$. Izjednačavanjem dobivamo $r = \lambda \cdot \frac{v-1}{k-1}$. $\square$

Posebno, vidimo da kroz svaku točku (v, k, λ) dizajna prolazi isti broj blokova. Za Fanovu ravninu taj broj je $r = 3$, a za afinu ravninu reda 3 je $r = 4$.

Propozicija 1.7. *Ukupan broj blokova (v, k, λ) dizajna je $b = \lambda \cdot \frac{v(v-1)}{k(k-1)}$.*

Dokaz. Neka je b ukupan broj blokova. Prebrojimo na dva načina koliko parova sadrži relacija incidencije I . Kroz svaku od v točaka prolazi r blokova, pa incidentnih parova ima $v \cdot r$. Na svakom od b blokova leži k točaka, pa incidentnih parova ima $b \cdot k$. Izjednačavanjem i uvrštavanjem formule za r iz prethodne propozicije dobivamo $b = \lambda \cdot \frac{v(v-1)}{k(k-1)}$. $\square$

Fanova ravnina ima $b = 7$ blokova, a afina ravnina reda 3 ima $b = 12$ blokova. Ponekad brojeve r i b također navodimo kao parametre dizajna, tj. govorimo o (v, b, r, k, λ) dizajnu. Na kraju ovog poglavlja navodimo nekoliko primjera koji ilustriraju moguće primjene dizajna.

Degustacija vina (vinska proba)

Vrsta eksperimenta u kakvom se prirodno pojavljuje potreba za pravilnom strukturom kao što je dizajn često se ilustrira jednostavnim i slikovitim primjerom degustacije vina. Pretpostavimo da na nekoj izložbi vina treba ocijeniti 7 sorti vina, na temelju čega će se odrediti rang-lista i podijeliti nagrade. Organizator želi objektivno ocjenjivanje, ali i minimiziranje troškova plaćanja kvalificiranih stručnjaka - degustatora. Iako bi bilo idealno da svaki degustator kuša i rangira svih 7 vina, to nije dopušteno, nego je ograničenje najviše 3 vina po degustatoru (kušanjem više od 3 vina, stručnjak može izgubiti osjećaj za fine nijanse okusa). Radi objektivnosti i ujednačenosti, poželjno je da svako vino bude degustirano jednako mnogo puta, a također i da svaka dva vina budu izravno uspoređena međusobno (barem jedanput) i to jednako mnogo puta. Jasno je onda da je potrebno barem $\binom{7}{2} = 21$ usporedbi, to jest degustacija parova vina, a za to je onda nužno barem 7 degustatora i to maksimalno iskorištenih (svaki kuša 3 vina, koliko je i dopušteno).

Sad se može pokušati napisati shemu degustacije u kojoj će svaki od 7 degustatora kušati točno po 3 vina, s tim da se svaki par vina nađe točno jedanput zajedno kod jednog degustatora. Ukupni broj pokusa - degustacija jednak je broju uređenih parova (degustator, vino) te iznosi 21. Lako ćemo ustanoviti da se tražena shema doista može ostvariti. U primjeru 1.4 točke identificiramo s vinima, a blokove sa skupovima vina koje kušaju pojedini degustatori. Shemu kušanja vina daje nam $(7, 3, 1)$ dizajn, to jest projekтивna ravnina reda 2. Slične eksperimente možemo zamisliti i za drukčije izbore osnovnih parametara, no uočimo da su nam bitni bili uvjeti pravilnosti u smislu "balansiranosti" (jednaki broj usporedbi - pokusa) za svaka dva uzorka i ujednačenosti broja pokusa kojima je podvrgnut pojedini uzorak. Pitanje je onda za koje se vrijednosti zadanih parametara može ostvariti odgovarajući plan (dizajn) eksperimenta.

Povezivanje telefona

Još jedan primjer sasvim slične vrste odnosi se na povezivanje telefonskih linija u nekoj ustanovi ili firmi. Uzmimo da telefonskih aparata ima 21, a da se povezuju preko sklopki od kojih se na svaku može spojiti najviše 5 aparata. Koliko treba sklopki i kako rasporediti spajanje, a da svaka dva aparata budu povezana? Analognim razmišljanjem kao u prethodnom primjeru vidimo da za $\binom{21}{2} = 210$ parova trebamo barem 21 sklopku (jer se pomoću svake može ostvariti najviše $\binom{5}{2} = 10$ povezivanja parova), dakle opet jednako mnogo sklopki koliko i pojedinih aparata. Zbog većeg broja elemenata, shemu spajanja sad nije toliko lako napisati, ali je moguće. Navodimo jedno moguće “gotovo” rješenje. Neka su aparati označeni $1, 2, \dots, 21$. Na prvu sklopku spojimo aparate broj 1, 2, 5, 15, 17, a za svaku daljnju sklopku brojeve “ciklički” povećamo za 1, s tim da nakon 21 dolazi ponovno 1. To znači npr. da će na drugu sklopku biti spojeni aparati broj 2, 3, 6, 16, 18, a na posljednju, dvadeset i prvu, aparati broj 1, 4, 14, 16, 21. Nije teško provjeriti da su ovakvom shemom ispunjeni svi uvjeti, no naravno da će nas više zanimati opća metoda koja je ovdje primijenjena za konstrukciju simetričnog $(21, 5, 1)$ dizajna ili projektivne ravnine reda 4. To je metoda diferencijskih skupova, s kojom ćemo se поблиže upoznati u 6. poglavlju.

No, pretpostavimo da se broj telefonskih aparata u istoj ustanovi povećao na 31. Analogno rješenje sheme spajanja, pomoću simetričnog dizajna, bit će moguće ako se mogu upotrijebiti sklopke sa 6 priključaka, dakle ako konstruiramo $(31, 6, 1)$ dizajn. Međutim, daljnje povećanje na 43 aparata neće se moći riješiti istom metodom, pomoću sklopki sa 7 priključaka, jer simetrični dizajn $(43, 7, 1)$ (projektivna ravnina reda 6) ne postoji. Problem nije, dakako, u prevelikom broju aparata, nego u broju 6, budući da se daljnja povećanja u obliku simetričnih $(57, 8, 1)$ i $(73, 9, 1)$ mogu realizirati. Zanima nas, dakle, kakvi su početni parametri “dobri” u smislu mogućeg postojanja određene pravilne strukture.

Zabavna matematika: problem 15 učenica

Mnogi poticajni matematički problemi, od kojih su neki postali značajni za razvitak cijelih matematičkih disciplina, prvotno su bili formulirani u okvirima zabavne ili rekreativne matematike, kao zadaci ili zagonetke namijenjene širem krugu publike. Za konačne geometrije važan je tako Eulerov “problem 36 oficira” iz 1782. o kojem ćemo ovdje nešto više napisati u poglavlju o latinskim kvadratima. (U popularnoj igri SuDoKu također se pojavljuje latinski kvadrat s nekim dodatnim svojstvima). No, jedan kombinatorički zadatak iz sredine 19. stoljeća, objavljen kao nagradno pitanje u tadašnjem engleskom časopisu za razbibrigu, pokazao se karakterističnim za elementarnu teoriju dizajna. Petnaest učenica šeta svaki dan, u pet redova po tri učenice. Mogu li se učenice svrstati na taj način za šetnju, da se u 7 dana svake dvije učenice nađu zajedno u istom redu točno jedanput? Zadatak je 1844. potpisao W.S.B. Woolhouse, no rješenje i poopćenje (1847.-1850.) objavio je velečasni T.P. Kirkman, matematičar-amater, pa se i danas govori o “Kirkmanovom problemu 15 učenica”. U suvremenoj terminologiji, traži se zapravo $(15, 3, 1)$ dizajn s dodatnim svojstvom “paralelnosti” (inače u geometriji tipičnim za afnu ravninu) da se skup pravaca može rastaviti u 7 klasa disjunktnih pravaca. Kirkman je riješio i poopćenje kada je ukupni broj točaka v neparni višekratnik od 3, a broj dana za

šetnju, to jest broj klasa paralelnih pravaca, iznosi $\frac{v-1}{2}$.

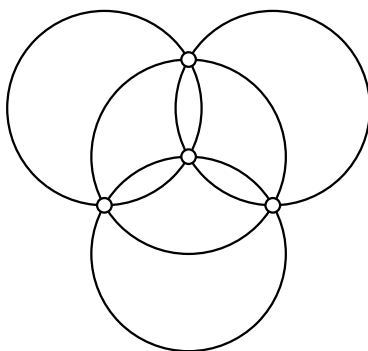
Dizajniranje eksperimenata

Britanski genetičar i statističar Ronald Fisher (1890.-1962.) najzaslužniji je za uvođenje suvremenih metoda planiranja eksperimenata na principima koji omogućuju statističku analizu rezultata. Svoj inovativni pristup Fisher je počeo razvijati u 20-im godinama 20. stoljeća, a njegovo ključno djelo je knjiga “The Design of Experiments” iz 1935. godine. Terminologiju i oznake poput v (varieties), r (replication) i t (treatment), koje su se zadržale do danas i u matematičkoj teoriji dizajna, uveo je pak F. Yates 1936. godine. Prvi problemi koje je razmatrao Fisher pripadaju području agronomije. Trebalo je ispitati djelotvornost v vrsta gnojiva na b tipova biljaka. “Potpuni eksperiment” zahtijevao bi raspolaganje s b parcela podijeljenih na po v dijelova kako bi se testirali svi parovi gnojivo - biljka, no to bi bilo preskupo u realnim uvjetima. Za “nepotpuni” eksperiment svaka se biljka “tretira” s k vrsti gnojiva, $k < v$, pri čemu treba ispuniti uvjet balansiranosti, da svaka dva gnojiva budu primijenjena na λ tipova biljaka (dakle, na jednako mnogo tipova). Na taj način osiguravaju se uvjeti za cjelovitu statističku analizu, što je također razradio Fisher. Primijetimo da je ideja pravilnog rasporeda i balansiranosti jednaka, dakako, kao u prethodnim primjerima, no da je u dizajniranju eksperimenata naglasak na statističkoj obradi podataka dobivenih “tretmanima” (što su u kombinatoričkoj strukturi samo “incidencije”).

Zadaci

Zadatak 1.1. Označite točke afine ravnine reda 3 brojevima $\{1, 2, \dots, 9\}$ i ispišite njezine blokove. Uvjerite se da je zaista riječ o dizajnu s parametrima $(9, 3, 1)$.

Zadatak 1.2. Na sljedećoj slici prikazan je dizajn kojem su točke kružići, a blokovi velike kružnice. Odredite njegove parametre i uvjerite se da je zaista riječ o dizajnu s tim parametrima.



Poglavlje 2

Dizajni

Ovo poglavlje započinjemo generalizacijom dizajna definiranih u uvodu.

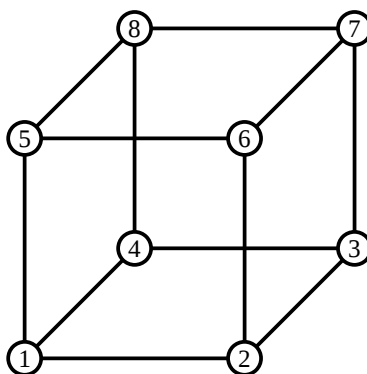
Definicija 2.1. *Neka su $v > k \geq t \geq 0$ i $\lambda > 0$ cijeli brojevi. Dizajn s parametrima t -(v, k, λ) je konačna incidencijska struktura sa svojstvima:*

1. *ukupan broj točaka je v ,*
2. *na svakom bloku leži točno k točaka,*
3. *svaki t -člani skup točaka sadržan je u točno λ blokova.*

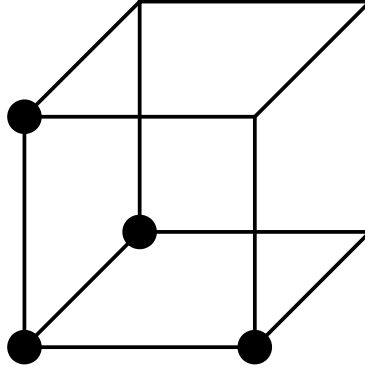
Za $t = 2$ imamo uvjete identične onima iz definicije 1.2. Kad želimo istaknuti parametar t , govorimo o t -dizajnu. Pod *dizajnom* podrazumijevamo 2-dizajn. Definicija ima smisla za $t = 1$ i $t = 0$, ali su to preslabe strukture da bi nam bile zanimljive. Incidencijska struktura je 1-(v, k, λ) dizajn ako ima v točaka, k točaka na svakom bloku i λ blokova kroz svaku točku (parametar koji se obično označava s r). Kod 0-dizajna λ je broj blokova koji sadrže prazan skup, tj. ukupan broj blokova b . Baviti ćemo se prvenstveno t -dizajnima za $t \geq 2$. U nastavku navodimo nekoliko primjera za $t > 2$.

Primjer 2.2. *Kao u primjeru 1.3, uzmimo bilo koji v -člani skup $\mathcal{T}$ i skup svih njegovih k -članih podskupova $\mathcal{B}$. Svaki t -člani podskup možemo nadopuniti do k -članog podskupa na $\lambda = \binom{v-t}{k-t}$ načina. Dakle, dizajn $(\mathcal{T}, \mathcal{B}, \in)$ ima parametre t -($v, k, \binom{v-t}{k-t}$).*

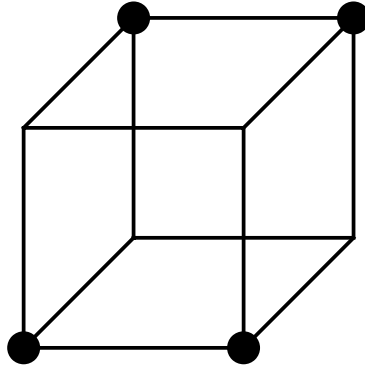
Primjer 2.3. *Skup točaka $\mathcal{T} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ možemo identificirati s vrhovima kocke:*



Blokove čine četveročlani podskupovi točaka dvije vrste. Osam blokova sastoji se od vrha kocke i tri njemu susjedna vrha:



To su blokovi $\mathcal{B}_1 = \{\{1, 2, 4, 5\}, \{1, 2, 3, 6\}, \{2, 3, 4, 7\}, \{1, 3, 4, 8\}, \{1, 5, 6, 8\}, \{2, 5, 6, 7\}, \{3, 6, 7, 8\}, \{4, 5, 7, 8\}\}$. Daljnjih šest blokova dobivamo kao vrhove na dva nasuprotna brida kocke:



To su blokovi $\mathcal{B}_2 = \{\{1, 2, 7, 8\}, \{3, 4, 5, 6\}, \{2, 3, 5, 8\}, \{1, 4, 6, 7\}, \{1, 3, 5, 7\}, \{2, 4, 6, 8\}\}$. Pokazuje se da su bilo koja tri vrha kocke sadržana u jedinstvenom bloku, tj. da je incidencijska struktura $(\mathcal{T}, \mathcal{B}_1 \cup \mathcal{B}_2, \in)$ dizajn s parametrima $3-(8, 4, 1)$.

Teorem 2.4. Neka je incidencijska struktura $\mathcal{D} = (\mathcal{T}, \mathcal{B}, I)$ dizajn s parametrima $t-(v, k, \lambda)$. Tada je $\mathcal{D}$ ujedno $s-(v, k, \lambda_s)$ dizajn, za svaki $s \in \{0, \dots, t\}$ i za

$$\lambda_s = \lambda \cdot \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

Dokaz. Neka je $S \subseteq \mathcal{T}$ proizvoljan s -člani skup točaka. Označimo s $\lambda(S)$ broj blokova koji ga sadrže i prebrojimo na dva načina parove u skupu

$$\{(T, B) \mid S \subseteq T \subseteq B, |T| = t, B \in \mathcal{B}\}.$$

Na $\binom{v-s}{t-s}$ načina možemo izabrati t -člani nadskup T od S , a blok B koji sadrži taj nadskup na λ načina. Prema tome, parova ima $\binom{v-s}{t-s} \cdot \lambda$. S druge strane, blok B koji sadrži S

možemo izabrati na $\lambda(S)$ načina, a t -člani “međuskup” T na $\binom{k-s}{t-s}$ načina. Dakle, parova ima $\lambda(S) \cdot \binom{k-s}{t-s}$. Izjednačavanjem dobivamo

$$\lambda(S) = \lambda \cdot \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}},$$

iz čega vidimo da $\lambda(S)$ ne ovisi o izboru skupa S , nego samo o njegovom broju elemenata s . Taj broj označavamo λ_s i time smo dokazali da je $\mathcal{D}$ dizajn s parametrima s -(v, k, λ_s). $\square$

Ovaj teorem je generalizacija propozicije 1.6 i propozicije 1.7 iz uvodnog poglavlja. Za $t = 2$ i $s = 1$ dobivamo broj blokova kroz proizvoljnu točku $r = \lambda_1 = \lambda \cdot \frac{\binom{v-1}{1}}{\binom{k-1}{1}} = \lambda \cdot \frac{v-1}{k-1}$. Za $t = 2$ i $s = 0$ dobivamo broj blokova koji sadrže prazan skup, tj. ukupan broj blokova $b = \lambda_0 = \lambda \cdot \frac{\binom{v}{2}}{\binom{k}{2}} = \lambda \cdot \frac{v(v-1)}{k(k-1)}$. Iz teorema također slijede nužni uvjeti djeljivosti na parametre da bi dizajni mogli postojati.

Korolar 2.5. *Ako postoji dizajn s parametrima t -(v, k, λ), onda $\binom{k-s}{t-s}$ dijeli $\lambda \cdot \binom{v-s}{t-s}$, za svaki $s \in \{0, \dots, t\}$.*

Dokaz. Parametri $\lambda_0, \dots, \lambda_t$ iz teorema 2.4 moraju biti prirodni brojevi. $\square$

Korolar 2.6. *Ako postoji 2-dizajn s parametrima (v, k, λ) , onda $k-1$ dijeli $\lambda(v-1)$ i $k(k-1)$ dijeli $\lambda v(v-1)$.*

U primjeru 3.17 konstruirat ćemo 5-(12, 6, 1) dizajn, koji je ujedno 4-(12, 6, 4) dizajn, 3-(12, 6, 12) dizajn, 2-(12, 6, 30) dizajn, 1-(12, 6, 66) dizajn i 0-(12, 6, 132) dizajn. Zadnje dvije tvrdnje znače da u tom dizajnu kroz svaku točku prolazi $r = 66$ blokova, a ukupan broj blokova je $b = 132$.

Iz korolara 2.5 slijedi da ne postoji 5-(13, 6, 1) dizajn, jer parametar $\lambda_4 = \frac{9}{2}$ nije prirodan broj. Slično, 5-(14, 6, 1) dizajn ne postoji zbog $\lambda_3 = \frac{55}{3}$, a 5-(15, 6, 1) dizajn zbog $\lambda_4 = \frac{11}{2}$. Parametri 5-(16, 6, 1) zadovoljavaju uvjete djeljivosti, ali dizajn s tim parametrima ipak ne postoji (što nije baš jednostavno dokazati). To pokazuje da uvjeti iz korolara 2.5 nisu dovoljni za postojanje dizajna. Parametri 2-(16, 6, 1) također zadovoljavaju uvjete djeljivosti, a dizajn ne postoji. U ovom slučaju nepostojanje lako slijedi iz sljedećeg teorema.

Teorem 2.7 (Fisherova nejednakost). *Ako postoji 2-dizajn s parametrima (v, b, r, k, λ) , onda je $v \leq b$.*

Za parametre 2-(16, 6, 1) dobivamo $r = 3$ i $b = 8$, pa oni očito ne zadovoljavaju Fisherovu nejednakost. Zato dizajn s tim parametrima ne postoji. Nejednakost nosi ime po već spomenutom britanskom statističaru Ronaldu Fisheru. Njezina važnost u statistici vidljiva je iz sljedećeg primjera.

Primjer 2.8. *Želimo testirati moguće interakcije između v lijekova. Svaki par lijekova treba testirati λ puta, tj. trebamo λ dobrovoljaca koji će istovremeno uzimati oba lijeka. Ukupan broj potrebnih dobrovoljaca je $\lambda \cdot \binom{v}{2}$ i on brzo raste s porastom broja lijekova v .*

Ideja za uštedu jest da svakom od dobrovoljaca damo $k > 2$ lijekova. Ideja je razumna ako su interakcije moguće isključivo između parova lijekova i ako se ne očekuje puno interakcija. Testiranje možemo provesti koristeći dizajn s parametrima (v, b, r, k, λ) , čije točke identificiramo s lijekovima, a blokove s dobrovoljcima. Tada parametar v označava broj lijekova, b broj dobrovoljaca, a r je broj dobrovoljaca koji uzimaju pojedini lijek. Već smo rekli da je k broj lijekova koje uzima pojedini dobrovoljac, a λ broj usporedbi parova lijekova. U toj interpretaciji Fisherova nejednakost kaže da broj dobrovoljaca ne može biti manji od broja lijekova koje testiramo.

Fisherova nejednakost može se dokazati primjenom linearne algebre. Za dokaz nam trebaju neki pomoćni rezultati. Prvo ćemo naučiti kako dizajne i druge konačne incidencijske strukture reprezentiramo matricama.

Definicija 2.9. Neka je $\mathcal{D}$ konačna incidencijska struktura sa skupom točaka $\mathcal{T} = \{p_1, \dots, p_v\}$ i skupom blokova $\mathcal{B} = \{B_1, \dots, B_b\}$. Incidencijska matrica od $\mathcal{D}$ je $v \times b$ matrica $A = [a_{ij}]$ definirana s

$$a_{ij} = \begin{cases} 1, & \text{ako je } p_i \in B_j, \\ 0, & \text{inače.} \end{cases}$$

Incidencijska matrica Fanove ravnine iz primjera 1.4 je

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix},$$

a incidencijska matrica 3-(8, 4, 1) dizajna iz primjera 2.3 je

$$A_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Označimo s I_n jediničnu matricu reda n :

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

S J_n označimo $n \times n$ matricu popunjenu jedinicama:

$$J_n = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}.$$

Konačno, neka j_n označava vektor-redak duljine n popunjen jedinicama:

$$j_n = [1 \quad 1 \quad \cdots \quad 1].$$

Tada incidencijske matrice 2-dizajna možemo karakterizirati na sljedeći način.

Teorem 2.10. *Neka je A matrica tipa $v \times b$ popunjena nulama i jedinicama. Matrica A je incidencijska matrica 2-dizajna s parametrima (v, b, r, k, λ) ako i samo ako vrijedi $j_v \cdot A = k j_b$ i $A \cdot A^T = \lambda J_v + (r - \lambda) I_v$.*

Dokaz. Množenjem matrica j_v i A dobivamo sume stupaca matrice A . Prema tome, jednakost $j_v \cdot A = k j_b$ ekvivalentna je činjenici da u incidencijskoj strukturi koju predstavlja A na svakom bloku leži točno k točaka. U produktu $A \cdot A^T$ na mjestu (i, j) nalazi se skalarni produkt i -tog i j -tog retka matrice A . On predstavlja broj blokova koji prolaze kroz i -tu i j -tu točku incidencijske strukture. Matrica $\lambda J_v + (r - \lambda) I_v$ na desnoj strani druge jednakosti ima brojeve r na dijagonali i λ izvan dijagonale. Druga jednakost vrijedi ako i samo ako kroz svaku točku incidencijske strukture prolazi točno r blokova, a kroz svake dvije točke prolazi točno λ blokova. Vidimo da su jednakosti ekvivalentne zahtjevima iz definicije 2-dizajna i propozicije 1.6. $\square$

Incidencijska matrica Fanove ravnine A_1 zadovoljava $j_7 \cdot A_1 = 3j_7$ i

$$A_1 \cdot A_1^T = \begin{bmatrix} 3 & 1 & \cdots & 1 \\ 1 & 3 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 3 \end{bmatrix}.$$

Dizajn 3-(8, 4, 1) s incidencijskom matricom A_2 ujedno je 2-dizajn s parametrima 2-(8, 4, 3), odnosno (8, 14, 7, 4, 3). Njegova incidencijska matrica zadovoljava $j_8 \cdot A_2 = 4j_{14}$ i

$$A_2 \cdot A_2^T = \begin{bmatrix} 7 & 3 & \cdots & 3 \\ 3 & 7 & \cdots & 3 \\ \vdots & \vdots & \ddots & \vdots \\ 3 & 3 & \cdots & 7 \end{bmatrix}.$$

U idućoj lemi izračunavamo determinantu matrice $\lambda J_v + (r - \lambda) I_v$.

Lema 2.11.

$$\begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{vmatrix} = (r - \lambda)^{v-1} (r + (v - 1)\lambda).$$

Dokaz. Od prvog retka determinante oduzmemo drugi, od drugog retka oduzmemo treći i tako dalje. Zatim izlučimo $r - \lambda$ iz svih redaka determinante osim zadnjeg:

$$\begin{vmatrix} r - \lambda & \lambda - r & 0 & \cdots & 0 & 0 \\ 0 & r - \lambda & \lambda - r & \cdots & 0 & 0 \\ 0 & 0 & r - \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & r - \lambda & \lambda - r \\ \lambda & \lambda & \lambda & \cdots & \lambda & r \end{vmatrix} = (r - \lambda)^{v-1} \begin{vmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ \lambda & \lambda & \lambda & \cdots & \lambda & r \end{vmatrix}.$$

Zbroj drugog do zadnjeg stupca dodamo prvom stupcu:

$$(r - \lambda)^{v-1} \begin{vmatrix} 0 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ r + (v - 1)\lambda & \lambda & \lambda & \cdots & \lambda & r \end{vmatrix}.$$

Sada razvijemo determinantu po prvom stupcu:

$$(r - \lambda)^{v-1} (-1)^{v-1} (r + (v - 1)\lambda) \begin{vmatrix} -1 & 0 & \cdots & 0 \\ 1 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{vmatrix}.$$

Zadnja determinanta jednaka je $(-1)^{v-1}$, pa dobivamo rezultat $(r - \lambda)^{v-1} (r + (v - 1)\lambda)$. $\square$

Ako su (v, b, r, k, λ) parametri dizajna, onda iz propozicije 1.6 dobivamo $(v - 1)\lambda = r(k - 1)$, tj. $r + (v - 1)\lambda = rk$. Tada je determinanta iz leme jednaka $rk(r - \lambda)^{v-1}$, posebno različita je od nule. Dokažimo sada Fisherovu nejednakost.

Dokaz teorema 2.7. Neka je A incidencijska matrica 2-dizajna s parametrima (v, b, r, k, λ) . Vidjeli smo da je determinanta matrice $A \cdot A^T$ različita od nule, pa je ta matrica punog ranga v . Rang od A također je jednak v jer kod množenja matrica rang ne može narasti. Rang je manji ili jednak od broja stupaca b matrice A i time smo dokazali $v \leq b$. $\square$

Dokaz Fisherove nejednakosti primjer je korištenja linearne algebre za dokazivanje kombinatoričkih nejednakosti. Naš dokaz je iskazan jezikom matrica, ali osnovna ideja te metode sadržana je u sljedećim lemapa.

Lema 2.12. *Neka je $f : S \rightarrow T$ funkcija s konačnom domenom S i kodomenom T . Ako je f injekcija, onda je $|S| \leq |T|$. Ako je f surjekcija, onda je $|S| \geq |T|$.*

Analogna lema vrijedi za linearne operatore.

Lema 2.13. *Neka je $f : V \rightarrow W$ linearni operator kojem su domena i kodomena konačnodimenzionalni vektorski prostori V i W . Ako je f monomorfizam (tj. injekcija), onda je $\dim V \leq \dim W$. Ako je f epimorfizam (tj. surjekcija), onda je $\dim V \geq \dim W$.*

Linearnoalgebarska metoda u kombinatorici bazirana je na svojevrsnoj kombinaciji prethodne dvije leme.

Lema 2.14. *Neka je $f : S \rightarrow V$ funkcija kojoj je domena konačan skup S , a kodomena konačnodimenzionalni vektorski prostor V . Ako je slika od f linearno nezavisni podskup od V , onda je $|S| \leq \dim V$. Ako je slika od f skup izvodnica za V , onda je $|S| \geq \dim V$.*

Funkcije poput ove dobivamo iz incidencijske matrice dizajna. Točkama dizajna pridružujemo odgovarajuće retke incidencijske matrice, tj. vektore iz prostora $\mathbb{R}^b$. U dokazu teorema 2.7 pokazali smo da su ti vektori linearno nezavisni, pa je broj točaka $v \leq \dim \mathbb{R}^b = b$. Dualno, blokovima dizajna pridružujemo stupce incidencijske matrice, vektore iz $\mathbb{R}^v$. Pokazat ćemo da stupci čine skup izvodnica za $\mathbb{R}^v$, pa je broj blokova $b \geq \dim \mathbb{R}^v = v$.

Drugi dokaz teorema 2.7. Neka je $A = [a_1 \cdots a_b]$ incidencijska matrica 2-dizajna s parametrima (v, b, r, k, λ) , pri čemu su $a_1, \dots, a_b \in \mathbb{R}^v$ njezini stupci. Iz definicije dizajna i propozicije 1.6 slijedi $S = \sum_{i=1}^b a_i = rj_v$ i $S_p = \sum_{\{i|a_{pi}=1\}} a_i = (r - \lambda)e_p + \lambda j_v$, za $p \in \{1, \dots, v\}$. Pritom je $j_v = (1, \dots, 1)$ vektor jedinica, a $e_p = (0, \dots, 0, 1, 0, \dots, 0)$ je vektor kanonske baze od $\mathbb{R}^v$. Vektore kanonske baze možemo izraziti kao linearnu kombinaciju stupaca incidencijske matrice: $e_p = \frac{1}{r-\lambda}S_p - \frac{\lambda}{r(r-\lambda)}S$. Prema tome, stupci incidencijske matrice razapinju $\mathbb{R}^v$, pa iz leme 2.14 slijedi $b \geq \dim \mathbb{R}^v = v$. $\square$

Za simetrične dizajne vrijedi $v = b$, tj. oni dostižu Fisherovu nejednakost. Simetrični dizajni čine važnu klasu dizajna. Njima ćemo se baviti u 4., 5., 6. i 7. poglavlju.

Korolar 2.15. *Incidencijska matrica simetričnog dizajna je regularna.*

Dokaz. Rječ je o kvadratnoj $v \times v$ matrici. U prvom dokazu Fisherove nejednakosti vidjeli smo da je ta matrica ranga v , pa je regularna. $\square$

Postoje razne generalizacije Fisherove nejednakosti na t -dizajne. D. Raghavarao je 1970. dokazao da u t -(v, k, λ) dizajnu s $v > k + 1$ vrijedi $b \geq (t - 1)(v - t + 2)$. R.M. Wilson i D.K. Ray-Chaudhuri dokazali su 1971. da u t -(v, k, λ) dizajnu s $v \geq k + s$, $s = \lfloor t/2 \rfloor$ vrijedi $b \geq \binom{v}{s}$. Iz tih nejednakosti slijedi da t -dizajni s $t \geq 3$ ne mogu biti simetrični.

Na kraju ovog poglavlja promotrit ćemo familiju dizajna s parametrima $t = 2$, $k = 3$ i $\lambda = 1$. To su takozvani *Steinerovi sustavi trojki*; umjesto 2-($v, 3, 1$) parametre zapisujemo $STS(v)$ (prema engleskom *Steiner triple system*).

Propozicija 2.16. *Ako postoji $STS(v)$ dizajn, onda je $v \equiv 1$ ili $3 \pmod{6}$ i $v \geq 7$.*

Dokaz. Iz uvjeta djeljivosti $k - 1 \mid \lambda(v - 1)$ slijedi da je v neparan, a iz uvjeta $k(k - 1) \mid \lambda v(v - 1)$ slijedi da je $v \equiv 1$ ili $0 \pmod{3}$ (korolar 2.6). Stoga je $v \equiv 1$ ili $3 \pmod{6}$, a uvjet $v \geq 7$ dobijemo iz Fisherove nejednakosti. $\square$

Zadaci

Zadatak 2.1. *Dokažite leme 2.12, 2.13 i 2.14.*

Zadatak 2.2. *Dokažite da su reci incidencijske matrice 2-dizajna linearno nezavisni.*

Zadatak 2.3. *Odredite skup svih prirodnih brojeva v za koje su parametri 2 -($v, 4, 1$) dizajna dopustivi (tj. zadovoljavaju uvjete djeljivosti i Fisherovu nejednakost).*

Poglavlje 3

Izomorfizam i automorfizmi

Incidencijske strukture koje možemo dobiti jedne od drugih promjenom oznaka točaka i blokova u biti su jednake. Pojam izomorfizma omogućuje nam da ih identificiramo.

Definicija 3.1. *Neka su $\mathcal{D}_1 = (\mathcal{T}_1, \mathcal{B}_1, I_1)$ i $\mathcal{D}_2 = (\mathcal{T}_2, \mathcal{B}_2, I_2)$ konačne incidencijske strukture. Kažemo da su one izomorfne ako postoje bijekcije $\varphi : \mathcal{T}_1 \rightarrow \mathcal{T}_2$ i $\psi : \mathcal{B}_1 \rightarrow \mathcal{B}_2$ takve da vrijedi $p I_1 B \iff \varphi(p) I_2 \psi(B)$, za sve $p \in \mathcal{T}_1$, $B \in \mathcal{B}_1$. Uređen par (φ, ψ) nazivamo izomorfizmom između $\mathcal{D}_1$ i $\mathcal{D}_2$.*

Izomorfne incidencijske strukture imaju identična svojstva. Naprimjer, jedna od njih je t -(v, k, λ) dizajn ako i samo ako je druga dizajn s istim parametrima. Izomorfnost možemo karakterizirati preko incidencijskih matrica i takozvanih *permutacijskih matrica*. To su kvadratne matrice koje imaju točno jednu jedinicu u svakom retku i stupcu, a svi ostali unosi su nule.

Propozicija 3.2. *Neka su A_1 i A_2 incidencijske matrice incidencijskih struktura $\mathcal{D}_1$ i $\mathcal{D}_2$. Strukture $\mathcal{D}_1$ i $\mathcal{D}_2$ su izomorfne ako i samo ako postoje permutacijske matrice P i Q takve da je $A_1 = P \cdot A_2 \cdot Q$.*

Dokaz. Množenje s lijeva permutacijskom matricom P odgovara permutiranju redaka incidencijske matrice, odnosno točaka incidencijske strukture. Množenje zdesna s Q odgovara permutiranju stupaca incidencijske matrice, odnosno blokova incidencijske strukture. $\square$

Ako je (φ, ψ) izomorfizam između jednostavnih incidencijskih struktura $\mathcal{D}_1 = (\mathcal{T}_1, \mathcal{B}_1, \in)$ i $\mathcal{D}_2 = (\mathcal{T}_2, \mathcal{B}_2, \in)$, onda bijekcija $\varphi : \mathcal{T}_1 \rightarrow \mathcal{T}_2$ jednoznačno određuje bijekciju $\psi : \mathcal{B}_1 \rightarrow \mathcal{B}_2$. Naime, blok B iz $\mathcal{B}_1$ preslikava se u blok $\psi(B) = \{\varphi(p) \mid p \in B\}$ iz $\mathcal{B}_2$. Za jednostavne incidencijske strukture izomorfizam možemo definirati kao bijekciju $\varphi : \mathcal{T}_1 \rightarrow \mathcal{T}_2$ koja blokove iz $\mathcal{B}_1$ preslikava u blokove iz $\mathcal{B}_2$.

Definicija 3.3. *Izomorfizam s incidencijske strukture $\mathcal{D}$ na samu sebe nazivamo automorfizmom od $\mathcal{D}$.*

Neki automorfizmi $(7, 3, 1)$ dizajna vidljivi su sa slike iz primjera 1.4. Izometrije euklidske ravnine koje preslikavaju trokut na samoga sebe induciraju automorfizme dizajna. Naprimjer, simetrija obzirom na pravac na kojem leže točke 3, 4, 6 inducira automorfizam $\alpha = (1, 2)(5, 7)$, a rotacija oko točke 6 za 120° u pozitivnom smjeru inducira automorfizam

$\beta = (1, 2, 3)(4, 5, 7)$. Ovdje navodimo samo permutacije točaka, jer je $(7, 3, 1)$ dizajn jednostavan. Postoje automorfizmi tog dizajna koji nisu inducirani izometrijama ravnine, naprimjer $\gamma = (1, 2, 3, 4, 5, 6, 7)$.

Propozicija 3.4. *Skup svih automorfizama incidencijske strukture $\mathcal{D}$ čini grupu obzirom na kompoziciju. Nazivamo je punom grupom automorfizama od $\mathcal{D}$ i označavamo s $\text{Aut } \mathcal{D}$.*

Dokaz. Slijedi iz činjenice da je kompozicija automorfizama automorfizam i inverz automorfizma automorfizam. Ako na automorfizam gledamo kao na par permutacija (φ, ψ) skupa točaka i skupa blokova, onda je njegov inverz $(\varphi^{-1}, \psi^{-1})$, a kompozicija automorfizama je $(\varphi_1, \psi_1) \circ (\varphi_2, \psi_2) = (\varphi_1 \circ \varphi_2, \psi_1 \circ \psi_2)$. $\square$

Puna grupa automorfizama $(7, 3, 1)$ dizajna generirana je automorfizmima α, β, γ , tj. $\text{Aut } \mathcal{D} = \langle (1, 2)(5, 7), (1, 2, 3)(4, 5, 7), (1, 2, 3, 4, 5, 6, 7) \rangle$. Uz pomoć programskog sustava GAP [9] ili nekog drugog sustava za računalnu algebru lako se provjeri da je red te grupe 168. Za bilo koju podgrupu $G \leq \text{Aut } \mathcal{D}$ kažemo da je *grupa automorfizama* dizajna $\mathcal{D}$. Naprimjer, grupa $G = \langle (1, 2)(5, 7), (1, 2, 3)(4, 5, 7) \rangle$ generirana s α i β je grupa automorfizama reda 6. Izomorfna je diedralnoj grupi D_3 , tj. grupi izometrija euklidske ravnine koje preslikavaju jednakostranični trokut na samog sebe. Grupu G čine automorfizmi $(7, 3, 1)$ dizajna sa slike koji su inducirani izometrijama euklidske ravnine.

Za iskazivanje tvrdnji o izomorfizmima i automorfizmima često se koristi terminologija djelovanja grupa na skupove.

Definicija 3.5. *Neka je G grupa s neutralnim elementom 1 i X skup. Kažemo da G djeluje na X ako je zadana funkcija $G \times X \rightarrow X$ (koja se zapisuje bez oznake, kao množenje: $(g, x) \mapsto gx$) takva da vrijedi*

1. $1x = x$, za svaki $x \in X$,
2. $g(hx) = (gh)x$, za sve $g, h \in G, x \in X$.

Djelovanje je vjerno ako je neutralni element jedini element iz G koji zadovoljava prvo svojstvo.

Primjer 3.6. *Neka je V vektorski prostor nad poljem F . To znači da je V Abelova grupa i zadano je množenje vektora skalarom $F \times V \rightarrow V$ koje ima svojstva*

1. $1x = x$, za svaki $x \in V$,
2. $\alpha(\beta x) = (\alpha \cdot \beta)x$, za sve $\alpha, \beta \in F, x \in V$.

Dakle, multiplikativna grupa polja F djeluje na V . Aksiomi distributivnosti kažu da je to djelovanje "usklađeno" sa zbrajanjem u polju F i s binarnom operacijom u grupi V .

Primjer 3.7. *Neka je $G \leq S(X)$ podgrupa grupe svih permutacija skupa X . Grupa G na prirodan način djeluje na X : za permutaciju $\alpha : X \rightarrow X$ i $x \in X$ definiramo $\alpha x = \alpha(x)$. Djelovanje je vjerno jer je identiteta (neutralni element u G) jedina permutacija koja svaki $x \in X$ preslikava u samoga sebe.*

Sljedeća propozicija pokazuje da svako vjerno djelovanje možemo shvatiti kao djelovanje iz primjera 3.7.

Propozicija 3.8. *Neka grupa G djeluje na skup X . Tada postoji homomorfizam grupa $\Phi : G \rightarrow S(X)$ takav da je $gx = \Phi(g)(x)$, za svaki $g \in G$ i $x \in X$. Homomorfizam Φ je injektivan ako i samo ako je djelovanje vjerno.*

Dokaz. Za proizvoljni element $g \in G$ definiramo funkciju $\Phi(g) : X \rightarrow X$ sa $\Phi(g)(x) = gx$, $\forall x \in X$. Funkcija $\Phi(g)$ je bijekcija zato što ima inverznu funkciju $\Phi(g^{-1})$:

$$[\Phi(g) \circ \Phi(g^{-1})](x) = \Phi(g)[\Phi(g^{-1})(x)] = g(g^{-1}x) = (gg^{-1})x = 1x = x, \quad \forall x \in X.$$

Vidimo da je kompozicija $\Phi(g) \circ \Phi(g^{-1})$ identiteta, a slično se vidi da je i $\Phi(g^{-1}) \circ \Phi(g)$ identiteta. Tako smo dobili funkciju $\Phi : G \rightarrow S(X)$ za koju ćemo sada pokazati da je homomorfizam grupa. Treba provjeriti da za sve $g, h \in G$ vrijedi $\Phi(gh) = \Phi(g) \circ \Phi(h)$:

$$\Phi(gh)(x) = (gh)x = g(hx) = \Phi(g)[\Phi(h)(x)] = [\Phi(g) \circ \Phi(h)](x), \quad \forall x \in X.$$

Homomorfizam je injekcija ako i samo ako mu je jezgra trivijalna, tj. ako se samo neutralni element $1 \in G$ preslika u neutralni element $id \in S(X)$. To je očito ekvivalentno vjernom djelovanju G na X . $\square$

Ako je djelovanje vjerno, Φ je monomorfizam, tj. ulaganje grupe G u grupu permutacija $S(X)$. Tada je grupa G izomorfna sa slikom $\Phi(G)$, koja je podgrupa od $S(X)$ i djeluje na X kao u primjeru 3.7.

Primjer 3.9. *Vidjeli smo da $(7, 3, 1)$ dizajn ima grupu automorfizama izomorfnu s diedralnom grupom D_3 . Koristeći terminologiju djelovanja možemo jednostavno reći da D_3 jest grupa automorfizama tog dizajna. Apstraktna grupa G je grupa automorfizama incidencijske strukture $(\mathcal{T}, \mathcal{B}, I)$ ako ona djeluje vjerno na skupu točaka $\mathcal{T}$ i na skupu blokova $\mathcal{B}$ i ako su ta dva djelovanja usklađena s relacijom incidencije: $p I B \iff gp I gB$, za sve $g \in G$, $p \in \mathcal{T}$ i $B \in \mathcal{B}$. Alternativno, za jednostavnu incidencijsku strukturu $(\mathcal{T}, \mathcal{B}, \in)$ grupu automorfizama možemo definirati kao apstraktnu grupu G koja djeluje na skupu točaka $\mathcal{T}$ tako da djelovanje vjerno i "čuva blokove". Točnije, za svaki blok $B \in \mathcal{B}$ i za svaki $g \in G$ skup $gB = \{gx \mid x \in B\}$ je također blok iz $\mathcal{B}$.*

Definicija 3.10. *Neka grupa G djeluje na skup X i neka je $x \in X$. Stabilizator elementa x je skup $G_x = \{g \in G \mid gx = x\} \subseteq G$. Orbita ili staza elementa x je skup $x^G = \{gx \mid g \in G\} \subseteq X$.*

Lako se provjeri da je stabilizator zapravo podgrupa od G : za $g, h \in G_x$ vrijedi $gh^{-1} \in G_x$. Na skupu X možemo definirati relaciju ekvivalencije na sljedeći način: $x \sim y \iff (\exists g \in G) y = gx$. Pokazuje se da su klase ekvivalencije te relacije orbite, pa skup X možemo prikazati kao disjunktну uniju orbita.

Primjer 3.11. *Neka je X skup svih 0-1 matrica tipa $v \times b$, ili skup svih incidencijskih matrica $t(v, k, \lambda)$ dizajna. Direktni produkt simetričnih grupa $G = S_v \times S_b$ djeluje na X permutiranjem redaka i stupaca: za $(\varphi, \psi) \in G$ i $A = [a_{ij}] \in X$ matricu $(\varphi, \psi)A$ definiramo kao $[a_{\varphi(i)\psi(j)}]$. Očito vrijede uvjeti iz definicije djelovanja. U slučaju kad X sadrži samo*

incidencijske matrice dizajna, treba još provjeriti zatvorenost skupa X na permutiranje redaka i stupaca. Incidencijske strukture ili dizajni $\mathcal{D}_1$ i $\mathcal{D}_2$ su izomorfni ako i samo ako njihove incidencijske matrice A_1 i A_2 pripadaju istoj orbiti pri ovom djelovanju. Puna grupa automorfizama incidencijske strukture $\mathcal{D}$ podudara se sa stabilizatorom odgovarajuće incidencijske matrice.

Teorem 3.12. *Neka grupa G djeluje na skup X i neka je $x \in X$. Kardinalni broj orbite od x jednak je indeksu stabilizatora: $|x^G| = [G : G_x]$.*

Dokaz. Označimo stabilizator s $H = G_x \leq G$. Prisjetimo se da je indeks podgrupe $[G : H]$ broj lijevih (ili desnih) susjednih klasa od H . Lijeve susjedne klase su skupovi oblika $gH = \{gh \mid h \in H\}$, koji se dobiju kao klase ekvivalencije relacije $g_1 \sim g_2 \iff g_1^{-1}g_2 \in H$. Treba dokazati da je kardinalni broj orbite $|x^G|$ jednak broju lijevih susjednih klasa.

Definiramo funkciju $\Phi : x^G \rightarrow \{gH \mid g \in G\}$ sa $\Phi(gx) = gH$, za svaki $gx \in x^G$. Funkcija je dobro definirana: ako je $g_1x = g_2x$, onda je $(g_1^{-1}g_2)x = x \Rightarrow g_1^{-1}g_2 \in G_x = H \Rightarrow g_1H = g_2H$. Funkcija Φ je bijekcija jer možemo definirati inverznu funkciju $\Psi : \{gH \mid g \in G\} \rightarrow x^G$, $\Psi(gH) = gx$. Lako se provjeri da je i Ψ dobro definirana te da su kompozicije $\Psi \circ \Phi$ i $\Phi \circ \Psi$ identiteta na orbiti x^G , odnosno na skupu lijevih susjednih klasa $\{gH \mid g \in G\}$. Dakle, Φ je bijekcija, pa slijedi $|x^G| = [G : G_x]$. $\square$

Korolar 3.13. *Neka grupa G djeluje na skup X i neka je $x \in X$. Tada je $|x^G| \cdot |G_x| = |G|$.*

Dokaz. Slijedi iz prethodnog teorema i $[G : G_x] = |G|/|G_x|$. $\square$

Ako znamo red pune grupe automorfizama dizajna $\mathcal{D}$, iz teorema možemo izračunati koliko ima dizajna izomornih s $\mathcal{D}$. Kardinalni broj orbite $|\mathcal{D}^{S_v \times S_b}|$ jednak je $[(S_v \times S_b) : \text{Aut } \mathcal{D}] = \frac{v! \cdot b!}{|\text{Aut } \mathcal{D}|}$. Problem klasifikacije dizajna sa zadanim parametrima t - (v, k, λ) sastoji se od određivanja po jednog predstavnika iz svake klase izomorfizma. Tada možemo izračunati ukupan broj t - (v, k, λ) dizajna.

Problem klasifikacije je vrlo težak i rješava se samo za male parametre, uz pomoć računala. Za mnoge parametre nije riješen ni problem egzistencije, tj. pitanje postoje li uopće t - (v, k, λ) dizajni? Ako je odgovor pozitivan dovoljno je konstruirati jedan primjer, za što se često koriste grupe automorfizama dizajna. Da bismo konstruirali $(7, 3, 1)$ dizajn s automorfizmom $\gamma = (1, 2, 3, 4, 5, 6, 7)$ dovoljno je naći samo jedan blok, naprimjer $B = \{1, 2, 4\}$. Ostale blokove dobivamo djelovanjem s γ na B .

Definicija 3.14. *Neka grupa G djeluje na skup X . Kažemo da je djelovanje tranzitivno ako za svaka dva elementa $x, y \in X$ postoji $g \in G$ takav da je $gx = y$.*

Tranzitivnost djelovanja znači da se cijeli X sastoji samo od jedne orbite. Djelovanje grupe G možemo prirodno proširiti sa skupa X na njegove podskupove: $gS = \{gx \mid x \in S\}$, $S \subseteq X$ i na uređene t -torke elemenata iz X : $g(x_1, \dots, x_t) = (gx_1, \dots, gx_t)$. Pri djelovanju na podskupove čuva se broj elemenata u S .

Definicija 3.15. *Neka grupa G djeluje na skup X . Kažemo da je djelovanje t -homogeno ako za svaka dva t -člana podskupa $S_1, S_2 \subseteq X$ postoji $g \in G$ takav da je $gS_1 = S_2$. Kažemo da je djelovanje t -tranzitivno ako za svake dvije uređene t -torke $(x_1, \dots, x_t)$, $(y_1, \dots, y_t)$ postoji $g \in G$ takav da je $g(x_1, \dots, x_t) = (y_1, \dots, y_t)$.*

Pojam t -homogenosti zapravo znači tranzitivnost induciranog djelovanja na skupu svih t -članih podskupova od X , a t -tranzitivnosti na skupu svih uređenih t -torki elemenata iz X . Očito iz t -tranzitivnosti slijedi t -homogenost. “Obična” tranzitivnost ekvivalentna je 1-homogenosti i 1-tranzitivnosti. Od višestruko homogenih permutacijskih grupa lako dobivamo dizajne.

Teorem 3.16. *Neka grupa G djeluje t -homogeno na v -člani skup X i neka je $K \subseteq X$ bilo koji k -člani podskup. Onda je incidencijska struktura $\mathcal{D} = (X, K^G, \in)$ dizajn s parametrima t -(v, k, λ), za $\lambda = [G : G_K] \cdot \binom{k}{t} / \binom{v}{t}$. Pritom je $G_K = \{g \in G \mid gK = K\}$ stabilizator. Ako je djelovanje G na X vjerno, onda je G grupa automorfizama od $\mathcal{D}$.*

Dokaz. Incidencijska struktura $\mathcal{D}$ sastoji se od $v = |X|$ točaka. Blokovi su k -člani podskupovi iz orbite $K^G = \{gK \mid g \in G\}$. Zbog t -homogenosti, za bilo koja dva t -člana podskupa $T_1, T_2 \subseteq X$ postoji $g_0 \in G$ takav da je $g_0 T_1 = T_2$. Neka je $\mathcal{B}_1 = \{gK \mid g \in G, T_1 \subseteq gK\}$ skup svih blokova koji sadrže T_1 i analogno $\mathcal{B}_2 = \{hK \mid h \in G, T_2 \subseteq hK\}$. Nije teško provjeriti da je $\mathcal{B}_2 = \{g_0 B \mid B \in \mathcal{B}_1\}$, pa su $\mathcal{B}_1$ i $\mathcal{B}_2$ jednakobrojni. Prema tome, svaki t -člani podskup sadržan je u istom broju blokova. Ako taj broj označimo λ , vidimo da je $\mathcal{D}$ dizajn s parametrima t -(v, k, λ). Dvostrukim prebrojavanjem parova iz skupa $\{(T, B) \mid B \in K^G, T \subseteq B, |T| = t\}$ dobivamo jednakost $[G : G_K] \cdot \binom{k}{t} = \binom{v}{t} \cdot \lambda$, iz koje slijedi formula za λ . Grupa G očito preslikava blokove u blokove, pa je u slučaju vjernog djelovanja grupa automorfizama od $\mathcal{D}$. $\square$

Ako djelovanje nije vjerno, dizajn iz prethodnog teorema ima grupu automorfizama G/N za normalnu podgrupu $N = \{g \in G \mid gx = x, \forall x \in X\}$. Ilustrirat ćemo teorem konstrukcijom takozvanog *malog Wittovog dizajna* u programskom sustavu GAP [9].

Primjer 3.17. *Dizajn s parametrima 5-(12, 6, 1) možemo konstruirati od Mathieuove grupe M_{12} . U GAP-u je dobijemo ovako:*

```
gap> G:=MathieuGroup(12);
Group([ (1,2,3,4,5,6,7,8,9,10,11), (3,7,11,8)(4,10,5,6),
(1,12)(2,11)(3,6)(4,8)(5,9)(7,10) ])
```

Riječ je o permutacijskoj grupi na skupu $\{1, \dots, 12\}$ generiranoj permutacijama $\alpha = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)$, $\beta = (3, 7, 11, 8)(4, 10, 5, 6)$ i $\gamma = (1, 12)(2, 11)(3, 6)(4, 8)(5, 9)(7, 10)$. Ovako dobijemo njezin red:

```
gap> Order(G);
95040
```

Provjerimo najprije tranzitivnost. Svih 12 točaka leže u jednoj orbiti:

```
gap> Orbits(G, [1..12]);
[ [ 1, 2, 12, 3, 11, 4, 7, 6, 8, 5, 10, 9 ] ]
gap> Size(last);
1
```

Višestruku homogenost provjeravamo prebrojavanjem orbita na t -članim podskupovima:

```

gap> Size(Orbits(G,Combinations([1..12],2),OnSets));
1
gap> Size(Orbits(G,Combinations([1..12],3),OnSets));
1
gap> Size(Orbits(G,Combinations([1..12],4),OnSets));
1
gap> Size(Orbits(G,Combinations([1..12],5),OnSets));
1
gap> Size(Orbits(G,Combinations([1..12],6),OnSets));
2

```

Grupa je t -homogena za $t = 2, 3, 4, 5$, ali nije za $t = 6$ jer postoje dvije orbite 6-članih podskupova. Ovako dobijemo predstavnike tih orbita:

```

gap> orb:=Orbits(G,Combinations([1..12],6),OnSets);;
gap> K1:=orb[1][1];
[ 1, 2, 3, 4, 5, 6 ]
gap> K2:=orb[2][1];
[ 1, 2, 3, 4, 5, 7 ]

```

Izračunajmo indekse stabilizatora ta dva podskupa:

```

gap> Order(G) / Order(Stabilizer(G,K1,OnSets));
792
gap> Order(G) / Order(Stabilizer(G,K2,OnSets));
132

```

Prema teoremu 3.16, orbita K_1^G je skup blokova 5-(12, 6, λ_1) dizajna s $\lambda_1 = 792 \cdot \binom{6}{5} / \binom{12}{5} = 6$, a K_2^G čini 5-(12, 6, λ_2) dizajn s $\lambda_2 = 132 \cdot \binom{6}{5} / \binom{12}{5} = 1$. Blokovi se u GAP-u dobiju sa `orb[1]` i `orb[2]`. Ovako vidimo da drugi dizajn ima $b = 132$ blokova, što se slaže s parametrima 5-(12, 6, 1) i s teoremom 2.4.

```

gap> Size(orb[2]);
132

```

Još jedna važna formula za djelovanje grupa na konačne skupove dana je u sljedećoj lemi.

Lema 3.18 (Cauchy-Frobenius-Burnside). *Neka grupa G djeluje na skup X . Označimo s $f(g) = |\{x \in X \mid gx = x\}|$ broj točaka iz X fiksiranih elementom $g \in G$. Broj orbita pri djelovanju G na X jednak je prosječnom broju točaka koje fiksiraju elementi iz G ,*

$$\frac{1}{|G|} \sum_{g \in G} f(g).$$

Dokaz. Na dva načina prebrojimo parove $\{(g, x) \in G \times X \mid gx = x\}$. Za čvrsti $g \in G$ broj parova je $f(g)$, pa je ukupan broj parova $\sum_{g \in G} f(g)$. Za čvrsti $x \in X$ broj parova jednak je redu stabilizatora $|G_x|$, koji je prema korolaru 3.13 jednak $\frac{|G|}{|x^G|}$. Ukupan broj

parova je stoga $|G| \cdot \sum_{x \in X} \frac{1}{|xG|}$. Rezultat slijedi izjednačavanjem, ako primijetimo da suma $\sum_{x \in X} \frac{1}{|xG|}$ daje broj orbita pri djelovanju G na X . Za svaki x sumiramo recipročnu vrijednost veličine orbite kojoj pripada, pa u sumi dobivamo po jednu jedinicu za svaku orbitu. $\square$

Pomoću ove leme možemo dokazati neke činjenice o grupama automorfizama simetričnih dizajna, koje će nam trebati kasnije.

Lema 3.19. *Ako automorfizam simetričnog dizajna fiksira točno f točaka, onda fiksira i točno f blokova.*

Dokaz. Neka automorfizam α simetričnog (v, k, λ) dizajna $\mathcal{D} = (\mathcal{T}, \mathcal{B}, \in)$ fiksira f točaka i F blokova. Dokazujemo da je $f = F$. Prebrojimo na dva načina skup parova $\{(p, B) \in \mathcal{T} \times \mathcal{B} \mid p \in B, \alpha(p) \in B\}$. Ako je p fiksna točka automorfizma (tj. $\alpha(p) = p$), onda imamo par za svaki od k blokova kroz p . U tom slučaju broj parova je fk . Ako p nije fiksna točka, imamo λ blokova kroz p i $\alpha(p)$, pa takvih parova ima $(v - f)\lambda$. Ukupan broj parova je $fk + (v - f)\lambda$. Brojanjem parova tako da prvo biramo blok B dobivamo analogni rezultat $Fk + (v - F)\lambda$, jer je dualna struktura simetrični dizajn s istim parametrima (vidi korolar 4.3). Izjednačavanjem dobivamo $(f - F)(k - \lambda) = 0$, iz čega slijedi $f = F$ (u netrivialnom simetričnom dizajnu je $k > \lambda$). $\square$

Propozicija 3.20. *Neka je G grupa automorfizama simetričnog dizajna. Broj orbita grupe G na točkama dizajna jednak je broju orbita na blokovima dizajna.*

Dokaz. Za automorfizam $g \in G$ označimo s $f(g)$ broj fiksnih točaka, a s $F(g)$ broj fiksnih blokova. Po lemi 3.18 broj orbita na točkama je $\frac{1}{|G|} \sum_{g \in G} f(g)$. Po lemi 3.19 to je jednako $\frac{1}{|G|} \sum_{g \in G} F(g)$, što je ponovo po lemi 3.18 broj orbita na blokovima. $\square$

Korolar 3.21. *Ako grupa automorfizama djeluje tranzitivno na točke simetričnog dizajna, onda djeluje tranzitivno i na blokove tog dizajna.*

Dokaz. Tranzitivno djelovanje znači da imamo samo jednu orbitu, a po prethodnoj propoziciji broj orbita na točkama jednak je broju orbita na blokovima. $\square$

Zadaci

Zadatak 3.1. *Uvjerite se da je svaki $(7, 3, 1)$ dizajn izomorfan dizajnu iz primjera 1.4. Izračunajte koliko ukupno ima $(7, 3, 1)$ dizajna na skupu točaka $\{1, \dots, 7\}$.*

Zadatak 3.2. *Neka grupa G djeluje na skup X i neka je $N = \{g \in G \mid gx = x, \forall x \in X\}$. Dokažite da je N normalna podgrupa od G .*

Zadatak 3.3. *Svaka grupa G djeluje na samu sebe lijevim translacijama: za $g \in G$ i $x \in G$ definiramo $gx = g \cdot x$ ("točkica" $\cdot$ je binarna operacija u grupi). Provjerite da je time zadano vjerno djelovanje i dokažite Cayleyev teorem, koji kaže da je svaka grupa izomorfna nekoj grupi permutacija.*

Zadatak 3.4. *Drugi način na koji grupa G djeluje na samu sebe je konjugiranjem: za $g \in G$ i $x \in G$ definiramo $gx = g \cdot x \cdot g^{-1}$. Provjerite da je time zadano djelovanje i ispitajte kada je ono vjerno. Stablizatore pri ovom djelovanju nazivamo centralizatorima elemenata iz G . Koju ulogu ima centar grupe $Z(G) = \{g \in G \mid g \cdot x = x \cdot g, \forall x \in G\}$?*

Zadatak 3.5. *Konstruirajte veliki Wittov $5-(24, 8, 1)$ dizajn. Upotrijebite Mathieuovu grupu M_{24} , koja se u GAP-u dobije s `MathieuGroup(24)`. Provjerite da M_{24} djeluje 5-homogeno na skup $\{1, \dots, 24\}$ i nađite orbitu 8-članih podskupova koja čini 5-dizajn s parametrom $\lambda = 1$.*

Poglavlje 4

Simetrični dizajni i Hadamardove matrice

Kao što smo spomenuli u uvodu, dizajne koji imaju jednako mnogo točaka i blokova ($v = b$) nazivamo *simetričnim dizajnima*. Uvjet je ekvivalentan s $k = r$, tj. s uvjetom da je broj točaka na bilo kojem bloku jednak broju blokova kroz bilo koju točku. Simetrični dizajni nužno imaju parametar $t = 2$, tj. riječ je o 2-dizajnima (vidi primjedbu na kraju 2. poglavlja). Iz propozicija 1.6 i 1.7 proizlazi nuždan uvjet za postojanje simetričnog (v, k, λ) dizajna:

$$k(k-1) = \lambda(v-1). \quad (4.1)$$

Simetrični dizajni imaju još jednu pravilnost: svaka dva bloka sijeku se točno u λ točaka. Kod nesimetričnih dizajna pojavljuju se i druge veličine presjeka.

Teorem 4.1. *Neka je $\mathcal{D}$ simetrični (v, k, λ) dizajn sa skupom blokova $\mathcal{B} = \{B_1, \dots, B_b\}$. Tada za svaka dva bloka $B_i \neq B_j$ vrijedi $|[B_i] \cap [B_j]| = \lambda$.*

Dokaz. Neka je A incidencijska matrica dizajna $\mathcal{D}$. Riječ je o kvadratnoj matrici reda v , koja je prema korolaru 2.15 regularna. Pomnožimo relaciju $A \cdot A^T = \lambda J_v + (k - \lambda)I_v$ iz teorema 2.10 s lijeva inverznom matricom A^{-1} :

$$A^T = \lambda A^{-1} J_v + (k - \lambda) A^{-1}.$$

Iz teorema 2.10 također slijedi $A J_v = k J_v$ (sume redaka od A su k), iz čega množenjem s A^{-1} dobivamo $A^{-1} J_v = \frac{1}{k} J_v$. Uvrštavanjem u prethodnu relaciju slijedi

$$A^T = \frac{\lambda}{k} J_v + (k - \lambda) A^{-1},$$

iz čega množenjem s A zdesna i uvrštavanjem $J_v A = k J_v$ dobivamo

$$A^T \cdot A = \lambda J_v + (k - \lambda) I_v.$$

Ova relacija znači da je skalarni produkt bilo koja dva stupca incidencijske matrice A jednak λ , tj. broj točaka koje leže na oba odgovarajuća bloka je λ . $\square$

Korolar 4.2. *Simetrični (v, k, λ) dizajni s $k < v$ su jednostavne incidencijske strukture.*

Dokaz. Kad bi različiti blokovi B_i, B_j bili incidentni s istim skupom točaka, vrijedilo bi $|[B_i] \cap [B_j]| = k$. Iz prethodnog teorema dobili bismo $k = \lambda$, a iz nužnog uvjeta (4.1) slijedilo bi $v = k$. $\square$

Dual incidencijske strukture $\mathcal{D} = (\mathcal{T}, \mathcal{B}, I)$ je incidencijska struktura $\mathcal{D}^\tau = (\mathcal{B}, \mathcal{T}, I^\tau)$ koju dobijemo zamjenom uloge točaka i blokova. Pritom je $I^\tau = \{(B, p) \mid (p, B) \in I\}$. Ako je A incidencijska matrica od $\mathcal{D}$, onda je incidencijska matrica od $\mathcal{D}^\tau$ transponirana matrica A^τ . Dual nesimetričnog dizajna ne može biti dizajn jer ne zadovoljava Fisherovu nejednakost. Za simetrične dizajne iz teorema 4.1 slijedi:

Korolar 4.3. *Dual simetričnog (v, k, λ) dizajna je simetrični dizajn s istim parametrima.*

Dualni dizajn $\mathcal{D}^\tau$ ne mora biti izomorfan polaznom simetričnim dizajnu $\mathcal{D}$. Ako to vrijedi, kažemo da je $\mathcal{D}$ *samodualan*. Fanova ravnina je očito samodualna jer su svaka dva $(7, 3, 1)$ dizajna izomorfna, a najmanji primjer dizajna koji nije samodualan ima parametre $(15, 7, 3)$.

Za dizajn s parametrima (v, b, r, k, λ) broj $n = r - \lambda$ nazivamo njegovim *redom*. Za simetrične dizajne je $r = k$, pa je red $n = k - \lambda$.

Teorem 4.4. *Broj točaka simetričnog (v, k, λ) dizajna reda $n \geq 2$ zadovoljava*

$$4n - 1 \leq v \leq n^2 + n + 1.$$

Dokaz. Uvrštavanjem $k = n + \lambda$ u nuždan uvjet (4.1) dobivamo kvadratnu jednadžbu u varijabli λ :

$$\lambda^2 + (2n - v)\lambda + n(n - 1) = 0. \quad (4.2)$$

Jednadžba ima rješenje, pa je njezina diskriminanta nenegativna:

$$(2n - v)^2 - 4n(n - 1) \geq 0 \implies (v - 2n)^2 \geq (2n - 1)^2 - 1.$$

Za $n \geq 2$ broj na desnoj strani $(2n - 1)^2 - 1$ nije potpun kvadrat, pa je nejednakost stroga:

$$(v - 2n)^2 > (2n - 1)^2 - 1 \implies (v - 2n)^2 \geq (2n - 1)^2 \implies v - 2n \geq 2n - 1 \implies v \geq 4n - 1.$$

Drugu nejednakost dobivamo iz rješenja jednadžbe (4.2):

$$\lambda_{1,2} = \frac{v - 2n \pm \sqrt{(2n - v)^2 - 4n(n - 1)}}{2}. \quad (4.3)$$

Iz $\lambda \geq 1$ slijedi $v - 2n \pm \sqrt{(2n - v)^2 - 4n(n - 1)} \geq 2$, tj. $v - 2n - 2 \geq \pm \sqrt{(2n - v)^2 - 4n(n - 1)}$. Kvadriranjem i sređivanjem dobivamo $v \leq n^2 + n + 1$. $\square$

Proučit ćemo pobliže simetrične dizajne s parametrima koji dostižu ocjene iz prethodnog teorema. Trebat će nam konstrukcija komplementiranja dizajna.

Propozicija 4.5. *Neka je $\mathcal{D} = (\mathcal{T}, \mathcal{B}, I)$ dizajn s parametrima (v, b, r, k, λ) , ne nužno simetričan. Tada je komplementarna incidencijska struktura $\mathcal{D}^c = (\mathcal{T}, \mathcal{B}, I^c)$, gdje je $I^c = (\mathcal{T} \times \mathcal{B}) \setminus I$, dizajn s parametrima $(v, b, b - r, v - k, b - 2r + \lambda)$.*

Dokaz. Broj točaka v i broj blokova b ne mijenjaju se komplementiranjem. Za bilo koju točku p u dizajnu $\mathcal{D}$ postoji r blokova koji su incidentni s p i $b - r$ blokova koji nisu incidentni s p . U komplementarnoj strukturi ti blokovi zamijene uloge, pa u $\mathcal{D}^c$ imamo $b - r$ blokova kroz p . Analogno, u $\mathcal{D}^c$ na bilo kojem bloku leži točno $v - k$ točaka. Prebrojimo sada blokove u $\mathcal{D}^c$ koji prolaze kroz proizvoljne dvije točke p_1 i p_2 . To su blokovi u $\mathcal{D}$ koji nisu incidentni niti s jednom od te dvije točke. Od ukupno b blokova, r je incidentno s p_1 , r je incidentno s p_2 , a λ je incidentno s p_1 i p_2 . Prema tome, $b - 2r + \lambda$ blokova nije incidentno niti s p_1 niti s p_2 . $\square$

Komplementiranjem možemo postići da bude $k \leq \frac{v}{2}$, pa se obično proučavaju samo takvi dizajni. Promotrimo sada simetrične dizajne reda n s najvećim mogućim brojem točaka $v = n^2 + n + 1$. Uvrštavanjem u (4.3) i sređivanjem dobivamo $\lambda_1 = 1$, $\lambda_2 = n^2 - n$. Iz $k = n + \lambda$ dobivamo odgovarajuće parametre $k_1 = n + 1$, $k_2 = n^2$. Dakle, simetrični dizajni reda n s najvećim mogućim brojem točaka imaju parametre $(n^2 + n + 1, n + 1, 1)$ i $(n^2 + n + 1, n^2, n^2 - n)$. Prva familija su *konačne projektivne ravnine* kojima je posvećeno iduće poglavlje, a druga familija su njihovi komplementi.

Na drugom kraju su simetrični dizajni reda n s najmanjim mogućim brojem točaka, $v = 4n - 1$. Uvrštavanjem u (4.3) slijedi $\lambda_1 = n$, $\lambda_2 = n - 1$ i $k_1 = 2n$, $k_2 = 2n - 1$. Dakle, takvi dizajni imaju parametre $(4n - 1, 2n, n)$ i $(4n - 1, 2n - 1, n - 1)$, koji su također komplementarni. U ostatku ovog poglavlja bavit ćemo se s familijom $(4n - 1, 2n - 1, n - 1)$ dizajna, takozvanim *Hadamardovim dizajnima*.

Jaques Hadamard (1865.-1963.) bio je poznati francuski matematičar koji je dao značajne doprinose u nekoliko područja matematike. Jedan od problema kojima se bavio bilo je pitanje ekstremnih vrijednosti determinante kvadratne matrice s ograničenim unosima.

Teorem 4.6 (Hadamard). *Neka je $A = [a_{ij}]$ realna $m \times m$ matrica čiji elementi zadovoljavaju $|a_{ij}| \leq 1$. Tada je $|\det A| \leq m^{m/2}$, pri čemu jednakost vrijedi ako i samo ako su svi elementi $a_{ij} \in \{1, -1\}$ i vrijedi $A \cdot A^T = mI_m$.*

Geometrijski dokaz ovog teorema dan je na str. 267 knjige [4]. Matrice za koje vrijedi jednakost nazivaju se *Hadamardovim matricama* i imaju zanimljiva kombinatorna svojstva. To su $\{1, -1\}$ -matrice kojima su reci međusobno ortogonalni.

Definicija 4.7. Hadamardova matrica reda m je kvadratna matrica H s unosima iz skupa $\{1, -1\}$ takva da je $H \cdot H^T = mI_m$.

Primjer 4.8. Množenjem se lako provjeri da su $H_1 = [1]$, $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ i

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Hadamardove matrice.

Množenje bilo kojeg retka ili stupca Hadamardove matrice s -1 neće pokvariti svojstva iz definicije. Na taj način možemo postići da u prvom retku i stupcu svi unosi budu jedinice; za takve Hadamardove matrice kažemo da su u *standardnom obliku*. Transponiranje također ne kvari svojstva Hadamardove matrice, tj. njezini stupci su također ortogonalni.

Lema 4.9. *Ako je H Hadamardova matrica, onda je i H^T Hadamardova matrica.*

Dokaz. Matrica H je očito regularna i vrijedi $H^T = mH^{-1}$. Množenjem te relacije zdesna s H dobivamo $H^T \cdot H = mI_m$, pa je i H^T Hadamardova matrica. $\square$

Propozicija 4.10. *Ako postoji Hadamardova matrica reda $m > 2$, onda je m djeljiv s 4.*

Dokaz. Množenjem redaka s -1 možemo postići da u prvom stupcu matrice budu samo jedinice, tj. da svaki redak počinje jedinicom. Neka je a broj redaka oblika $[1 \ 1 \ 1 \ \dots]$, b broj redaka oblika $[1 \ 1 \ -1 \ \dots]$, c broj redaka oblika $[1 \ -1 \ 1 \ \dots]$ i d broj redaka oblika $[1 \ -1 \ -1 \ \dots]$. Očito vrijedi

$$a + b + c + d = m,$$

a iz ortogonalnosti prva tri stupca dobivamo jednakosti

$$a + b - c - d = 0,$$

$$a - b + c - d = 0,$$

$$a - b - c + d = 0.$$

Sustav ove četiri jednadžbe ima jedinstveno rješenje $a = b = c = d = \frac{m}{4}$. Budući da su a, b, c, d cijeli brojevi, m mora biti djeljiv s 4. $\square$

Sljedeći teorem uspostavlja vezu između Hadamardovih matrica, spomenute serije simetričnih $(4n - 1, 2n - 1, n - 1)$ dizajna i jedne serije 3-dizajna koji se također nazivaju Hadamardovim dizajnima. Treba nam još jedna konstrukcija koja od dizajna pravi dizajne.

Propozicija 4.11. *Neka je $\mathcal{D} = (\mathcal{T}, \mathcal{B}, \in)$ dizajn s parametrima t -(v, k, λ) i $p \in \mathcal{T}$ njegova točka. Neka je $\text{der}_p \mathcal{D} = (\mathcal{T} \setminus \{p\}, \{B \setminus \{p\} \mid B \in \mathcal{B}, p \in B\}, \in)$ incidencijska struktura koju dobijemo brisanjem točke p i uzimanjem svih blokova kroz p (bez te točke). Tada je $\text{der}_p \mathcal{D}$ dizajn s parametrima $(t - 1)$ -($v - 1, k - 1, \lambda$).*

Dokaz. Ukupan broj točaka i broj točaka na svakom bloku smanji se za 1. Ako uzmemo proizvoljnih $t - 1$ točaka iz $\mathcal{T} \setminus \{p\}$, onda u $\mathcal{D}$ imamo λ blokova koji sadrže p i te točke. Dakle, u $\text{der}_p \mathcal{D}$ imamo λ blokova kroz bilo kojih $t - 1$ točaka. $\square$

Dizajn $\text{der}_p \mathcal{D}$ zovemo *deriviranim dizajnom* od $\mathcal{D}$ u točki p .

Teorem 4.12. *Ekvivalentno je:*

(a) *postoji Hadamardova matrica reda $m = 4n$,*

(b) postoji $3-(4n, 2n, n-1)$ dizajn,

(c) postoji simetrični $2-(4n-1, 2n-1, n-1)$ dizajn.

Dokaz. $[a \Rightarrow b]$ Neka je $H = [h_{ij}]$ Hadamardova matrica reda $m = 4n$. Možemo pretpostaviti da je u standardnom obliku, tj. da su u prvom retku i stupcu jedinice. Definiramo incidencijsku strukturu sa skupom točaka $\mathcal{T} = \{1, \dots, m\}$ i s blokovima $B_i^+ = \{j \in \mathcal{T} \mid h_{ij} = 1\}$, $B_i^- = \{j \in \mathcal{T} \mid h_{ij} = -1\}$. Tvrdimo da je $(\mathcal{T}, \mathcal{B}, \in)$ dizajn s parametrima $3-(4n, 2n, n-1)$, gdje je $\mathcal{B} = \{B_2^+, \dots, B_m^+, B_2^-, \dots, B_m^-\}$. Očito je ukupan broj točaka $m = 4n$, a zbog ortogonalnosti i -tog retka s prvim retkom vrijedi $|B_i^+| = |B_i^-| = 2n$, za $i = 2, \dots, m$. Uzmimo tri različite točke $j_1, j_2, j_3 \in \{1, \dots, m\}$ i prebrojimo koliko blokova sadrži sve tri. Blok B_i^+ ih sadrži ako je $h_{ij_1} = h_{ij_2} = h_{ij_3} = 1$, a blok B_i^- ako je $h_{ij_1} = h_{ij_2} = h_{ij_3} = -1$. Prema tome, dobivamo jedan blok kroz j_1, j_2 i j_3 za svaki redak u kojemu se unosi u ta tri stupca slažu. U propoziciji 4.10 vidjeli smo da se unosi u prva tri stupca matrice H slažu za točno n redaka (jer je $a = \frac{m}{4} = n$). Jasno je da bi se isto moglo dokazati za bilo koja tri stupca. Jedno slaganje nastupa u prvom retku (koji sadrži same jedinice), a preostala slaganja daju nam točno $n-1$ blokova kroz točke j_1, j_2 i j_3 . Dakle, dobili smo $3-(4n, 2n, n-1)$ dizajn.

$[b \Rightarrow c]$ Ako postoji dizajn s parametrima $3-(4n, 2n, n-1)$, onda derivirani dizajn (u bilo kojoj točki) ima parametre $2-(4n-1, 2n-1, n-1)$. Derivirani dizajni su simetrični jer parametri zadovoljavaju uvjet (4.1).

$[c \Rightarrow a]$ Neka je A incidencijska matrica simetričnog $(4n-1, 2n-1, n-1)$ dizajna. Matricu H dobijemo od A tako da zamijenimo sve nule s -1 i dodamo redak i stupac popunjen jedinicama. Prvi redak (popunjen jedinicama) ortogonalan je s ostalima jer matrica A u svakom retku ima $2n-1$ jedinica i $2n$ nula. Nakon zamjene $0 \rightarrow -1$ i dodavanja jedinice na početak imamo točno $2n$ jedinica i nula u ostalim recima. Ostali reci od H su međusobno ortogonalni jer u A u bilo koja dva retka imamo unose $(1, 1)$ na $n-1$ mjesta, a unose $(0, 0)$, $(0, 1)$ i $(1, 0)$ na n mjesta. Zamjenom $0 \rightarrow -1$ i dodavanjem jedinica svaka od kombinacija $(1, 1)$, $(-1, -1)$, $(1, -1)$ i $(-1, 1)$ javlja se točno n puta, pa skalarnim množenjem redaka od H dobivamo $2n \cdot 1 + 2n \cdot (-1) = 0$. Dakle, H je Hadamardova matrica reda $4n$. $\square$

Postavlja se pitanje za koje prirodne brojeve n postoji Hadamardova matrica reda $4n$. Prema takozvanoj Hadamardovoj hipotezi, koja nije dokazana do današnjeg dana, takve matrice postoje za svaki n . Poznate su mnoge konstrukcije beskonačnih serija i pojedinačnih Hadamardovih matrica. Upoznat ćemo jednu rekurzivnu konstrukciju.

Definicija 4.13. Neka je $A = [a_{ij}]$ matrica tipa $m \times n$ i B matrica tipa $p \times q$. Kroneckerov ili tenzorski produkt matrica A i B je sljedeća blok matrica tipa $mp \times nq$:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}.$$

Primjer 4.14. Kroneckerov produkt matrica H_2 i H_3 iz primjera 4.8 je matrica

$$H_2 \otimes H_3 = \begin{bmatrix} H_3 & H_3 \\ H_3 & -H_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Provjerite množenjem da je $H_2 \otimes H_3$ također Hadamardova matrica!

Lema 4.15. Ako su A, C i B, D dva para ulančanih matrica (koje se mogu množiti), onda vrijedi $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$. Pritom je $\cdot$ uobičajeni produkt matrica, a $\otimes$ je Kroneckerov produkt.

Dokaz. Neka su matrice A, B, C, D redom tipa $m \times n, p \times q, n \times o, q \times r$ s elementima $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}], D = [d_{ij}]$. Matrice $A \otimes B$ i $C \otimes D$ su tipa $mp \times nq$ i $nq \times or$; ulančane su i njihov produkt je tipa $mp \times or$. Matrice $A \cdot C$ i $B \cdot D$ su tipa $m \times o$ i $p \times r$, a njihov Kroneckerov produkt $(A \cdot C) \otimes (B \cdot D)$ je tipa $mp \times or$. Vidimo da su $(A \otimes B) \cdot (C \otimes D)$ i $(A \cdot C) \otimes (B \cdot D)$ istog tipa $mp \times or$. Indekse $i \in \{1, \dots, mp\}$, $j \in \{1, \dots, or\}$ možemo identificirati s parovima $i \equiv (i_1, i_2) \in \{1, \dots, m\} \times \{1, \dots, p\}$, $j \equiv (j_1, j_2) \in \{1, \dots, o\} \times \{1, \dots, r\}$. Tada je element na mjestu (i, j) matrice $(A \otimes B) \cdot (C \otimes D)$ dan izrazom $\sum_{k=1}^n \sum_{l=1}^q a_{i_1 k} b_{i_2 l} c_{k j_1} d_{l j_2}$, a matrice $(A \otimes B) \cdot (C \otimes D)$ izrazom $(\sum_{k=1}^n a_{i_1 k} c_{k j_1})(\sum_{l=1}^q b_{i_2 l} d_{l j_2})$. Izrazi su očito jednaki, pa su i matrice jednake. $\square$

Propozicija 4.16. Neka su H_1 i H_2 Hadamardove matrice reda m_1 i m_2 . Tada je $H_1 \otimes H_2$ Hadamardova matrica reda $m_1 m_2$.

Dokaz. Matrica $H_1 \otimes H_2$ ima unose ± 1 i zadovoljava $(H_1 \otimes H_2) \cdot (H_1 \otimes H_2)^\tau = (H_1 \otimes H_2) \cdot (H_1^\tau \otimes H_2^\tau) = (H_1 \cdot H_1^\tau) \otimes (H_2 \cdot H_2^\tau) = (m_1 I_{m_1}) \otimes (m_2 I_{m_2}) = m_1 m_2 I_{m_1 m_2}$. $\square$

Iz primjera 4.8 znamo da postoji Hadamardova matrica reda 2, pa iz ove propozicije slijedi postojanje Hadamardovih matrica reda $m = 2^l$ za sve $l \geq 2$. U primjeru 6.13 vidjet ćemo da postoji Hadamardova matrica reda 12. Iz propozicije 4.16 tada slijedi postojanje Hadamardovih matrica reda $m = 3 \cdot 2^l$ za sve $l \geq 2$. Direktnim konstrukcijama Hadamardovih matrica dobivamo druge nizove Hadamardovih matrica, ali beskonačno mnogo redova ostaje “nepokriveno”. Za te redove ne zna se postoje li Hadamardove matrice. Do nedavno najmanji otvoreni red je bio $m = 428$, a nakon rada [13] to je $m = 668$.

Zadaci

Zadatak 4.1. Dokažite obrat teorema 4.1: ako se svaka dva bloka (v, k, λ) dizajna sijeku u λ točaka, onda je taj dizajn simetričan.

Zadatak 4.2.* Konstruirajte simetrični $(15, 7, 3)$ dizajn koji nije samodualan.

Zadatak 4.3. Dokažite da se permutiranjem točaka i blokova $(7, 3, 1)$ dizajna može postići da njegova incidencijska matrica bude simetrična. Simetrični dizajni s tim svojstvom nazivaju se samopolarnim dizajnima.

Zadatak 4.4. Dokažite da je svaki samopolarni dizajn ujedno i samodualan.

Zadatak 4.5.* Nađite primjer samodualnog dizajna koji nije samopolaran.

Zadatak 4.6. Ako je $\mathcal{D} = (\mathcal{T}, \mathcal{B}, \in)$ dizajn s parametrima t -(v, k, λ) i $p \in \mathcal{T}$ njegova točka, dokažite da je incidencijska struktura $\text{res}_p \mathcal{D} = (\mathcal{T} \setminus \{p\}, \{B \mid B \in \mathcal{B}, p \notin B\})$ dizajn s parametrima $(t-1)$ -($v-1, k, \lambda_{t-1} - \lambda$). Zovemo ga rezidualnim dizajnom od $\mathcal{D}$ u točki p . Parametar λ_{t-1} dobijemo iz teorema 2.4.

Zadatak 4.7. Neka je $\mathcal{D}$ simetrični (v, k, λ) dizajn s $\lambda \geq 2$ i neka je p njegova točka. Dokažite da je tada dualna struktura deriviranog dizajna $(\text{der}_p \mathcal{D})^\tau$ dizajn s parametrima 2 -($k, \lambda, \lambda - 1$).

Zadatak 4.8. Neka je $\mathcal{D}$ simetrični (v, k, λ) dizajn s $k \geq \lambda + 2$ i neka je p njegova točka. Dokažite da je tada dualna struktura rezidualnog dizajna $(\text{res}_p \mathcal{D})^\tau$ dizajn s parametrima 2 -($v - k, k - \lambda, \lambda$).

Poglavlje 5

Projektivne i afine ravnine

U području konačnih geometrija posebno mjesto zauzimaju projektivne i afine ravnine, naročito kad se ističu upravo neki geometrijski aspekti promatranih incidencijskih struktura, poput podstruktura (konfiguracije, podravnine, ovali, krivulje 2. reda) i automorfizama - kolineacija. Koordinatizacija projektivnih ravnina pomoću prikladnih algebarskih struktura također ima ključnu ulogu u konstrukcijama i proučavanju svojstava takvih ravnina. Projektivne i afine ravnine zasad smo spomenuli samo usputno, a u ovom poglavlju posvetit ćemo im nešto više pozornosti, premda će to biti samo minimalni uvod u tu tematiku. Uobičajenu geometrijsku terminologiju ovdje smo već dosad primjenjivali na dizajne i srodne incidencijske strukture, no još važnije su motivacija i ideje koje se u značajnoj mjeri prenose iz “klasične” geometrije na konačne geometrije. I sličnosti i razlike koje se pritom pojavljuju vrlo su korisne za bolje razumijevanje promatranih struktura te poticajne za različita istraživanja.

Euklidska ravnina zapravo je afina ravnina s bogatstvom dodatne strukture (uređaj, metrika). Projektivna geometrija razvijala se postupno, prvotno s idejom proširivanja euklidske geometrije “neizmjereno dalekim” elementima (točkama i pravcem, odnosno pravcima i ravninom ako je riječ o trodimenzionalnom prostoru) kako bi se euklidski paralelni pravci mogli tretirati zajednički i ravnopravno s pravcima koji se sijeku. Takvo “upotpunjenje” omogućuje objedinjeni uvid u mnoge geometrijske činjenice, a pripadna preslikavanja, karakteristična za ovakav pristup, proizlaze iz centralnog projiciranja, kao vrlo jednostavnog i prirodnog pridruživanja među točkama, pravcima i ravninama koje općenito “čuva” samo incidenciju. (Invarijantnost kutova, djelišnog omjera ili pogotovo udaljenosti nije svojstvena projektivnoj geometriji nego njezinim specijalnim podgeometrijama.) Stoga je razumljivo da je upravo projektivna geometrija bliska incidencijskim strukturama kakve su nam ovdje od interesa.

5.1 Osnovno o konačnim poljima

Najprije navodimo nekoliko bitnih činjenica o konačnim poljima, budući da se mnoge konstrukcije konačno-geometrijskih struktura, a posebno projektivnih i afinih ravnina, temelje upravo na konačnim poljima i njihovim svojstvima.

Ovdje je korisno vladati barem najosnovnijim pojmovima i činjenicama iz teorije grupa, kao što su ciklička grupa, red elementa u grupi, Lagrangeov teorem (red podgrupe

konačne grupe nužno je djelitelj reda grupe), pojam homomorfizma i izomorfizma grupa te prvi teorem o izomorfizmu, no mi ćemo nastojati “prepričati” ono najvažnije o konačnim poljima navodeći samo naputke o povezanosti s drugim algebarskim strukturama.

Podsjetimo da je polje $(F, +, \cdot)$ algebarska struktura koja se sastoji od nepraznog skupa F i dvije binarne operacije, standardno označene kao zbrajanje $+$ i množenje $\cdot$, takve da je $(F, +)$ komutativna (Abelova) grupa, $(F^*, \cdot)$ uz oznaku $F^* = F \setminus \{0\}$ također Abelova grupa te vrijedi distributivnost operacije $\cdot$ u odnosu na $+$: $a(b + c) = a \cdot b + a \cdot c$ za sve $a, b, c \in F$. Pritom je 0 neutralni element za zbrajanje, 1 neutralni element za množenje, a oznaka za operaciju $\cdot$ izostavlja se kad god je to praktično i nedvosmisleno ($a \cdot b = ab$).

Elemente bilo kojeg polja često zovemo skalari, osobito u kontekstu vektorskog prostora nad poljem. Vektorski prostor V dimenzije n nad poljem F , za bilo koji $n \in \mathbb{N}$, jednostavno konstruiramo kao skup F^n svih uređenih n -torki $(x_1, \dots, x_n)$ s $x_i \in F$, uz zbrajanje n -torki i množenje n -torki skalarom iz F po komponentama. Iz linearne algebre znamo da je svaki n -dimenzionalni vektorski prostor nad poljem F izomorfan prostoru F^n . (Izomorfizam se jednostavno uspostavlja prikazom vektora u odabranoj bazi vektorskog prostora).

U matematici se najčešće služimo poljem racionalnih brojeva $\mathbb{Q}$, poljem realnih brojeva $\mathbb{R}$ i poljem kompleksnih brojeva $\mathbb{C}$. No, vektorski prostor isto tako možemo definirati nad bilo kojim poljem. Valja istaknuti da ako je polje F konačno te ima q elemenata, onda je i vektorski prostor F^n konačan skup i ima q^n elemenata – vektora.

Spomenimo da se algebarska struktura $(K, +, \cdot)$ naziva *tijelom* ako ima sva svojstva kao polje, osim možda komutativnosti množenja. Vrijedi teorem da je svako konačno tijelo komutativno, to jest da je polje. Štoviše, vrijedi teorem (Wedderburn, 1905.) da je svaka konačna integralna domena (prsten s jedinicom, bez djelitelja nule) tijelo pa stoga i polje. Ovo je između ostalog važno zato što nam u konstrukcijama, primjerice konačnih projektivnih ravnina s “nestandardnim” svojstvima trebaju upravo algebarske strukture koje nisu tijelo ili polje (npr. kvazipolje, skoropolje) pa je korisno znati koja će dodatna algebarska svojstva proizaći iz uvjeta konačnosti.

Primjer beskonačnog nekomutativnog tijela je tijelo kvaterniona (vidi poglavlje 7, tekst iza teorema 7.6).

Uočimo da svako polje mora sadržavati barem elemente 0 i 1 , tj. neutralni element za svaku od operacija. Moguće je da polje sadrži isključivo ta dva elementa: na skupu $\{0, 1\}$ definiramo množenje standardno, kao u cijelim brojevima, dok za zbrajanje, uz očigledno $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, stavimo $1 + 1 = 0$. Tako dobivamo najmanje polje od svega dva elementa, a možemo ga interpretirati kao skup $\mathbb{Z}_2$ cjelobrojnih ostataka po modulu 2 s operacijama zbrajanja i množenja modulo 2. Ovo se daje poopćiti i tako dobivamo polje $\mathbb{Z}_p$ s točno p elemenata za svaki primbroj p . Naime, za cijeli broj $m \geq 2$ operacije modulo m ($\text{mod } m$) definiramo tako da dva cijela broja zbrojimo odnosno pomnožimo “obično”, kao u $\mathbb{Z}$, a zatim uzmemo ostatak rezultata te operacije pri dijeljenju s m . Skup $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ svih ostataka pri dijeljenju s m ima strukturu komutativnog prstena s jedinicom s obzirom na operacije zbrajanja i množenja mod m . Posebno, taj prsten bit će integralna domena (tj. neće imati djelitelja nule) ako i samo ako je m primbroj. U tom slučaju $\mathbb{Z}_m$ je i polje.

Primjer 5.1.

- (a) U polju $\mathbb{Z}_3 = \{0, 1, 2\}$ elementi 1 i 2 međusobno su suprotni (inverzni pri zbrajanju) pa se često umjesto 2 piše -1 . Svaki od elemenata 1 i 2 vlastiti je inverz za množenje. Općenito se u $\mathbb{Z}_p$ može identificirati $p - 1$ i -1 . Elementi 1 i $p - 1$ uvijek su sami sebi inverzni za množenje.
- (b) U polju $\mathbb{Z}_{11}$ za operaciju množenja međusobno su inverzni parovi elemenata 2 i 6, 3 i 4, 5 i 9, 7 i 8, dok su 1 i 10 sami sebi inverzni.

Primjer 5.2. U svakom polju F jednadžbe oblika $a + x = b$ i $a \cdot x = b$, potonja uz uvjet $a \neq 0$, imaju jedinstveno rješenje. Nadalje, sve činjenice o rješivosti i strukturi skupa rješenja sustava linearnih jednadžbi, poznate iz linearne algebre, također vrijede nad bilo kojim poljem F . Naravno, ako je skup rješenja neprazan pa čini k -dimenzionalni potprostor prostora F^n (za homogeni sustav) odnosno linearnu mnogostrukost (za nehomogeni sustav), onda je taj skup rješenja konačan kada je i polje F konačno te se sastoji od q^k elemenata.

Osnovne rezultate o egzistenciji konačnih polja izložiti ćemo u sljedećem teoremu. Za konačno polje kažemo da je reda q ako se sastoji od točno q elemenata te pišemo $|F| = q$. Konačna polja još se nazivaju i Galoisovim poljima, prema francuskom matematičaru E. Galoisu te se polje reda q najčešće označava $GF(q)$, od *Galois field*.

Teorem 5.3.

- (1) Konačno polje reda q postoji ako i samo ako je $q \in \mathbb{N}$ oblika $q = p^d$, pri čemu je p primbroj, a $d \in \mathbb{N}$.
- (2) Polje reda $q = p^d$ ima jedinstveno potpolje reda p . Primbroj p je karakteristika polja F , u oznaci $\text{char } F = p$. To je najmanji prirodan broj m za koji je

$$\underbrace{1 + 1 + \dots + 1}_{m \text{ puta}} = 0.$$

- (3) Svaka dva polja jednakog reda q su izomorfna.

Ovaj teorem nećemo dokazivati, no evo djelomične skice dokaza i nekoliko napomena kako bismo bolje razumijeli njegov sadržaj. Ako je F neko polje i K njegovo potpolje, dakle podskup koji je i sam polje s obzirom na operacije naslijeđene iz F (npr. $\mathbb{Q}$ je potpolje od $\mathbb{R}$, a $\mathbb{R}$ od $\mathbb{C}$), onda je F ujedno i vektorski prostor nad poljem K . U slučaju da je F konačno polje, a time i K konačno potpolje, F je prostor konačne dimenzije, recimo d , nad K pa je $|F| = |K|^d$. Najmanje potpolje konačnog polja F dobivamo kao potpolje generirano elementom 1. Ono se sastoji od svih elemenata oblika $1 + 1 + \dots + 1 = m \cdot 1$, a nije teško pokazati da postoji najmanji $m \in \mathbb{N}$ takav da je $m \cdot 1 = 0$ i da je taj m primbroj. Tako se zapravo izvodi tvrdnja (2) u teoremu, a odatle slijedi i nužnost oblika $q = p^d$ za red q konačnog polja. Uočimo da u polju karakteristike p za svaki element a vrijedi $pa = 0$. (Za polje F reda p , gdje je p primbroj, nema drugih potpolja pa je

neposredno ispunjeno (2)). Dovoljnost uvjeta $q = p^d$, p primbroj, da bi postojalo polje reda q u slučaju $d = 1$ vidimo iz već navedenog primjera polja $\mathbb{Z}_p$ ostataka mod p .

Preostaje izgradnja polja reda p^d za vrijednosti $d \geq 2$. Samo ćemo naznačiti kako se to može učiniti. Ideja je slična kao za cjelobrojne ostatke mod p , samo što treba uzeti skup polinoma stupnja najviše $d - 1$, s koeficijentima iz polja $\mathbb{Z}_p$ (takvih polinoma očito ima upravo p^d) te, uz standardno zbrajanje polinoma, definirati novu operaciju množenja tako da budu ispunjena svojstva polja. Ulogu analognu onoj primbroja p kod operacija mod p ovdje će imati odabrani ireducibilni polinom $f(x)$ stupnja d ; polinomi će se pomnožiti standardno pa će se onda uzeti ostatak pri dijeljenju umnoška polinomom $f(x)$ (vidi primjer 5.4). (Preciznije algebarski formulirano, imamo kvocijentni prsten prstena polinoma po prostom idealu generiranom ireducibilnim polinomom $f(x)$).

Što se pak tiče tvrdnje (3), izomorfizam svaka dva konačna polja jednakog reda, dakle postojanje bijekcije koja "čuva" obje operacije, za operaciju $+$ proizlazi odatle što: (i) jednakost redova uključuje jednakost karakteristika, a polje prim reda p očito je izomorfno polju $\mathbb{Z}_p$; (ii) Abelove grupe dotičnih polja izomorfne su, kao odgovarajuće grupe u vektorskim prostorima jednakih dimenzija nad potpoljem reda p , dakle u izomorfnim prostorima. "Prenošenje" izomorfizma aditivnih grupa i na multiplikativne grupe nije sasvim jednostavno, a lakše se vidi nešto drukčijim pristupom za koji je potrebno znati da je multiplikativna grupa konačnog polja ciklička (a svake dvije cikličke grupe jednakog reda su izomorfne).

Polje $GF(q)$ može se opisati i kao proširenje polja $GF(p)$ koje sadrži sve nultočke polinoma $x^q - x$.

Primjer 5.4. *Konstrukcija polja reda 4 i reda 9.*

- (1) *Polje reda 4 dovoljno je maleno da ga možemo konstruirati i izravno, uzimajući npr. skup $\{0, 1, a, b\}$ i definirajući operacije tako da pazimo na ispunjavanje potrebnih svojstava. I ovdje mora biti $1 + 1 = 0$, dok dalje lako ustanovimo da treba definirati $a + a = b + b = 0$, $a + 1 = b$, $aa = b$, $ab = 1$ itd. No, ako se poslužimo navedenim principom konstrukcije pomoću polinoma, imamo svega 4 polinoma: $0, 1, x, 1 + x$, a za operaciju množenja treba nam ireducibilni polinom stupnja 2. Taj polinom nema nultočaka u polju $\mathbb{Z}_2$ pa lako vidimo da to mora biti $f(x) = x^2 + x + 1$. Sada je npr. $(x + 1) \cdot (x + 1) = x^2 + 1 \equiv x \pmod{f(x)}$. (Dakako, $x + x = 0$ jer računamo u polju karakteristike 2, gdje je $1 + 1 = 0$).*
- (2) *Malo više posla imamo za red 9. Sada je broj elemenata toliko velik da je bolje odmah primijeniti konstrukciju pomoću polinoma. Imamo 9 polinoma oblika $ax + b$, gdje su a, b iz polja $\mathbb{Z}_3$ (dakle, koeficijenti polinoma su 0, 1 i 2, odnosno -1), a za ireducibilni polinom možemo uzeti $g(x) = x^2 + 1$. Primjer umnoška sada je $(x + 1) \cdot (x + 2) = x^2 + 2 \equiv 1 \pmod{g(x)}$, jer $x + 2x = 0$ u ovom polju.*

U različitim konstrukcijama u konačnim geometrijama vrlo korisna su i sljedeća svojstva konačnih polja.

Propozicija 5.5. *Neka je $F = GF(q)$ i $F^\square = \{a^2 \mid a \in F^*\}$ skup svih kvadrata u F različitih od 0. Tada vrijedi:*

- (1) *za $\text{char } F = 2$, $F^\square = F^*$;*

- (2) za $\text{char } F = p > 2$, $F^\square$ je podgrupa multiplikativne grupe F^* , reda $|F^\square| = (q-1)/2$. Pritom je $-1 \in F^\square$ ako i samo ako je $q \equiv 1 \pmod{4}$.

Skica dokaza (uz malo teorije grupa). Promatramo kvadriranje na $F^\square$: preslikavanje koje svakom $a \neq 0$ pridružuje a^2 . Za elemente a i b vrijedi $a^2 = b^2$ ako i samo ako je $(a+b)(a-b) = 0$. U slučaju karakteristike 2, $a+b = a-b$ pa slijedi $(a-b)^2 = 0$, to jest $a = b$ pa je kvadriranje u tom slučaju injektivno, dakle i bijektivno te je $F^\square = F^*$. Za neparnu karakteristiku p , jednake kvadrate imaju će točno po dva međusobno suprotna elementa pa će kvadrata biti upola manje od svih $q-1$ elemenata. (Kvadriranje, označimo to preslikavanje s φ , zapravo je homomorfizam grupe F^* na njezinu podgrupu $F^\square$, jer je $\varphi(ab) = (ab)^2 = a^2b^2$, pa se može primijeniti prvi teorem o izomorfizmu i na taj način odrediti $|F^\square|$, budući da je jezgra $\text{Ker } \varphi = \{1, -1\}$ pa je $|F^\square| = |F^* / \text{Ker } \varphi| = (q-1)/2$. Napokon, da bi -1 bio u $F^\square$ nužno je i dovoljno da red te grupe bude paran, tj. $q-1 \equiv 0 \pmod{4}$, jer tada i samo tada je $\{1, -1\}$ podgrupa grupe $F^\square$. (Općenito vrijedi da je konačna grupa parnog reda ako i samo ako sadrži podgrupu reda 2, što se lako pokaže npr. tako da se promatra koliko ima elemenata koji su sami sebi inverzni, budući da ostali elementi dolaze u parovima uzajamno inverznih). $\square$

Primjer 5.6. U polju $F = GF(11)$, $F^\square = \{1, 3, 4, 5, 9\}$, a 10 (odnosno -1) nije u tom podskupu kvadrata. U polju $F = GF(3^2)$ iz primjera 5.4 $x^2 \equiv -1 \pmod{g(x)}$ jer $g(x) = x^2 + 1$ pa polinomi x i $-x$ kao elementi polja kvadriranjem daju -1 .

Ovaj kratki pregled svojstava konačnih polja završit ćemo tvrdnjama o strukturi aditivne i multiplikativne grupe polja.

Propozicija 5.7. Neka je $F = GF(q)$, $q = p^d$. Tada je grupa $(F, +)$ elementarno Abelova p -grupa, a grupa $(F^*, \cdot)$ je ciklička.

Strukturu grupe $(F, +)$ razabiremo već odatle što je F vektorski prostor nad svojim potpoljem reda p . Svaki element od F može se prikazati kao uređena d -torka elemenata tog potpolja, a to zapravo znači da je $(F, +)$ direktna suma d podgrupa reda p (cikličkih, dakako). To upravo govori da je $(F, +)$ elementarno Abelova p -grupa. Argument da je multiplikativna grupa ciklička zahtijeva malo više pojedinosti iz teorije konačnih grupa, u što nećemo ulaziti. Primijetimo samo da za svaki element a polja, $a \neq 0$, vrijedi $a^{q-1} = 1$ pa je a nultočka polinoma $x^{q-1} - 1$. Broj nultočaka polinoma nije veći od njegova stupnja, a malo detaljnije razmatranje pokazalo bi da ako grupa $(F^*, \cdot)$ ne bi bila ciklička onda bi svi njezini elementi bili nultočke polinoma stupnja manjeg od $q-1$ što nije moguće. Primjerice, ako je $q = 9$, Abelova grupa reda 8 može biti ili ciklička reda 8 ili direktna suma cikličkih grupa reda 4 i 2 ili direktna suma tri cikličke grupe reda 2, to jest elementarno Abelova 2-grupa. U drugom i trećem slučaju za sve elemente vrijedi $a^4 = 1$, što bi značilo da bi polinom $x^4 - 1$ imao 8 različitih nultočaka u polju, nemoguće. Svaki generator grupe $(F^*, \cdot)$ naziva se *primitivni element* polja F . Za primitivni element ω vrijedi, dakle, da je $F^* = \{1, \omega, \omega^2, \dots, \omega^{q-2}\}$, jer je $\omega^{q-1} = 1$. Ovakav prikaz često je vrlo praktičan za računanje u konačnom polju.

5.2 Aksiomi i neki modeli projektivne ravnine

Već smo definirali konačnu projektivnu ravninu kao simetrični (v, k, λ) dizajn u kojem je $\lambda = 1$ pa se onda v i k izražavaju s pomoću parametra $n = k - \lambda$, reda dizajna, u obliku $v = n^2 + n + 1$, $k = n + 1$ te govorimo o projektivnoj ravnini *reda* n .

Sad ćemo pristupiti definiranju projektivne ravnine putem općenitih aksioma, bez uvjeta konačnosti. Ovdje izabiremo “sažeti” popis osnovnih aksioma koji je i najpogodniji za naše svrhe, ne vodeći dakle računa o mogućem “izlasku” u prostor dimenzije veće od 2, što je inače svakako od interesa. Uz to, dakako, izbjegavamo aksiome koji bi nužno vodili na beskonačnu ravninu. U ovom poglavlju elemente skupa $\mathcal{B}$ nazivat ćemo pravcima, a ne blokovima.

Definicija 5.8. *Incidencijska struktura $\mathcal{P} = (\mathcal{T}, \mathcal{B}, I)$ naziva se projektivna ravnina, ako su zadovoljeni aksiomi:*

- (P1) *za svake dvije točke p, q postoji točno jedan pravac B tako da vrijedi $p I B$ i $q I B$;*
- (P2) *za svaka dva različita pravca B, C postoji točka p tako da vrijedi $p I B$ i $p I C$;*
- (P3) *postoje četiri različite točke takve da nikoje tri od njih nisu kolinearne, to jest da nisu sve tri incidentne s nekim pravcem.*

Želimo, dakle, da naša geometrija bude ovakva: Svake dvije (različite) točke spojene su jednim jedinim pravcem (u skladu s našim pojmovima iz euklidske geometrije), što nam je poznato kao uvjet balansiranosti s $\lambda = 1$ za dizajne. No, i svaka dva različita pravca imat će zajedničku točku, “sjecište”. Ovo je bitna novost u odnosu na euklidsku planimetriju: nema (različitih) paralelnih pravaca, a to da je “sjecište” dvaju pravaca jedinstveno ne moramo uključiti u iskaz aksioma, budući da to neposredno slijedi iz aksioma (P1) (postojanje dva sjecišta očito bi povlačilo dvije različite spojnice za te dvije točke, suprotno zahtjevu).

Napokon, treći aksiom samo će nam osiguravati da u toj ravnini imamo dovoljno točaka i pravaca, kako ne bismo morali voditi brigu o trivijalnim slučajevima, npr. o “ravnini” od svega jednog pravca i dvije točke na njemu ili slično. Lako se može zaključiti kako to vodi na postojanje barem 6 različitih pravaca (spojnica 6 parova točaka), no zapravo je zajamčeno postojanje barem 7 točaka i 7 pravaca, a u jednom mogućem rasporedu oni čine najmanju projektivnu ravninu, onu reda 2.

Naglasimo također kako se projektivna ravnina nikad ne može “nacrtati” u euklidskoj ravnini, to jest vjerno prikazati unutar euklidske ravnine na način da neke točke i neki pravci (ili dijelovi pravaca) euklidske ravnine budu u bijektivnoj korespondenciji s točkama i pravcima projektivne ravnine, a da pritom incidencija (točka pripada ili ne pripada pravcu) bude u cijelosti sačuvana. Nešto kasnije, ovu nemogućnost smještanja u euklidsku ravninu dokazat ćemo za sve konačne ravnine. Ipak, to ne znači da se pri konstrukciji modela raznih projektivnih ravnina nećemo poslužiti elementima euklidske geometrije, uz određene modifikacije. Već je spomenuto da se problem sjecišta za paralelne (euklidske) pravce rješava uvođenjem novih, “neizmjereno dalekih” točaka, što pripada uobičajenoj terminologiji npr. u nacrtnoj geometriji.

Propozicija 5.9. *Neka je $\mathcal{P} = (\mathcal{T}, \mathcal{B}, I)$ projektivna ravnina. Tada vrijedi:*

- (a) svaka dva pravca imaju jedinstvenu zajedničku točku (sjecište);
- (b) postoje četiri pravca tako da nikoja tri od njih ne prolaze zajedničkom točkom (nemaju zajedničko sjecište);
- (c) skupovi $\mathcal{T}$ i $\mathcal{B}$ imaju barem po 7 elemenata, pri čemu je svaka točka incidentna s barem 3 pravca, a svaki pravac incidentan je s barem 3 točke.

Radi jednostavnosti, pravac koji prolazi točkama p i q (aksiom (P1)) nazivamo spojnicom tih točaka i po potrebi označavamo s pq , dok jedinstvenu zajedničku točku pravaca B i C (aksiom (P2) i propozicija 5.9) zovemo sjecištem tih pravaca i označavamo BC . Skup od četiri točke sa svojstvom iz aksioma (P3) nazivamo *četverovrh*, a skup od četiri pravca sa svojstvom iz propozicije 5.9 (c) nazivamo *četverostran*.

Skicirajmo bitni dio dokaza propozicije. Neka su p, q, r, s točke sa svojstvom iz aksioma (P3), dakle vrhovi jednog četverovrha. Promatrajući spojnice pq i rs , pr i qs te ps i qr uočavamo da se ta tri para pravaca sijeku u trima točkama – označimo ih redom s t, u i w , koje su sve različite od p, q, r i s (u suprotnom bi dobili proturječje s početnom pretpostavkom o četverovrhu). Na taj način imamo već 7 točaka i 6 pravaca. No, i svake dvije od točaka t, u i w imaju svoju spojnicu. To mogu biti tri različita pravca, ali u našim aksiomima nema zapreke da točke t, u i w budu kolinearne. Time dobivamo sedmi pravac, a daljnjih pravaca može i ne mora biti, budući da u slučaju kolinearne t, u i w imamo potpunu projektivnu ravninu čiji su pravci (skraćeno pisano): $pqt, rst, pru, qsu, psw, qrw$ i tuw . To je tzv. Fanova ravnina, kakvu već poznajemo.

Ako t, u i w nisu kolinearne, imamo barem 9 pravaca koji onda imaju i daljnja sjecišta. (Sljedeće “zatvaranje” projektivne ravnine može se dogoditi za 13 točaka i 13 pravaca, jer će broj točaka konačne projektivne ravnine nužno biti oblika $n^2 + n + 1$ za $n \in \mathbb{N}$).

Napomena 5.10. *Primijetimo još stanovitu ravnopravnost tj. simetriju u svojstvima točaka i pravaca koja proizlazi kombiniranjem definicije 5.8 i propozicije 5.9 (a) i (b). Riječ je o tzv. principu dualnosti koji ima važnu ulogu u projektivnoj geometriji. Ne sasvim formalno iskazano, princip dualnosti zapravo je teorem koji govori kako se iz svake istinite tvrdnje projektivne geometrije ravnine dobiva također istinita, dualna tvrdnja tako da se međusobno zamijene pojmovi “točka” – “pravac” i svi termini koji se odnose na relaciju incidencije između njih, npr. “leži na” zamjenjuje se s “prolazi kroz” (i obrnuto), “spojnica” sa “sjecište” (i obrnuto) itd. Posve je jasno kako bismo “dualiziranjem” neke tvrdnje i njezina dokaza dobili dualnu tvrdnju i njezin dokaz. (Uočimo vezu s pojmom dualne incidencijske strukture iz poglavlja 4 i korolarom 4.3).*

Nadalje, uvest ćemo jednostavna preslikavanja pomoću kojih možemo uspostaviti i neke kvantitativne odnose među skupovima točaka pojedinih pravaca (u projektivnoj geometriji katkad se govori o nizovima točaka) i, dualno, skupovima pravaca koji imaju zajedničko sjecište (tzv. pramenovi pravaca). U slučaju konačne ravnine, time ćemo zapravo dobiti svojstva simetričnog dizajna. Prisjetimo se da smo skup svih točaka incidentnih s pravcem B označavali s $[B]$, a analognu tj. dualnu oznaku $[p]$ uvodimo za točku p . Ne ulazeći sada, radi sažetijeg izlaganja, u punu terminologiju projektivne geometrije (perspektivitet, projektivitet itd.) definirat ćemo tip preslikavanja koji ćemo jednostavno nazivati centralnim projiciranjem.

Definicija 5.11. *Neka su B i C različiti pravci projektivne ravnine $\mathcal{P}$, a s točka koja ne leži ni na jednom od tih pravaca. Centralno projiciranje pravca B na pravac C je preslikavanje koje točki $x \in [B]$ pridružuje $x' \in [C]$ kao sjecište pravaca sx i C . Točka s je pritom centar projiciranja.*

Zahvaljujući aksiomima (P1) i (P2), odnosno propoziciji 5.9 (a), lako se dokazuje da je projiciranje dobro definirano i pritom bijektivno preslikavanje. Stoga su skupovi $[B]$ i $[C]$ ekvipotentni (jednakobrojni) čim za pravce B i C postoji centar projiciranja (bilo koja točka koja ne leži ni na jednom od njih), no to je ispunjeno u svakoj projektivnoj ravnini, kao što se vidi jednostavnom primjenom aksioma i propozicije 5.9. Nadalje, spajanjem bilo koje točke p sa svim točkama nekog pravca B koji s njom nije incidentan, uspostavljamo bijekciju između skupova $[p]$ i $[B]$. Stoga su svi skupovi oblika $[p]$ odnosno $[B]$ u projektivnoj ravnini međusobno ekvipotentni, bez ikakvih ograničenja na konačnost skupova točaka i pravaca. Uz uvjet konačnosti (ili cijelog skupa točaka $\mathcal{T}$ ili skupa točaka barem jednog pravca), dobivamo uniformnost, regularnost i simetričnost te incidencijske strukture:

Propozicija 5.12. *Neka je $\mathcal{P}$ projektivna ravnina u kojoj barem za jedan pravac L vrijedi da je skup $[L]$ konačan te označimo $|[L]| = k$. Tada je $k \geq 3$ te za svaki pravac B i za svaku točku p vrijedi $|[B]| = |[p]| = k$. Nadalje, ukupni broj točaka ravnine $\mathcal{P}$ je konačan, jednak je ukupnom broju pravaca ravnine te iznosi $k^2 - k + 1$. Drugim riječima, $\mathcal{P}$ je simetrični $(v, k, 1)$ dizajn s $v = k^2 - k + 1 = n^2 + n + 1$, uz oznaku $n = k - 1$ za red dizajna.*

Na ovaj način došli smo, dakle, do tumačenja projektivne ravnine kao simetričnog dizajna, ali započevši od geometrijskog pristupa bez unaprijed postavljenog uvjeta konačnosti incidencijske strukture. Dakako, jedno od glavnih pitanja u vezi s konačnim projektivnim ravninama je problem postojanja ravnine reda n za neki $n \in \mathbb{N}$, $n \geq 2$. Taj problem nije još u cijelosti riješen, no sve dosad poznate konačne projektivne ravnine imaju red oblika potencije primbroja, $n = p^s$ (p primbroj). Pitanjem uvjeta egzistencije ravnine za pojedine vrijednosti n baviti ćemo se opširnije u 7. poglavlju, a već sada možemo navesti cijelu seriju konačnih projektivnih ravnina izgrađenih pomoću linearne algebre nad konačnim poljima, za svaki red oblika $n = p^s$. To su projektivne ravnine koje predstavljaju najvažniju i najbolje istraženu klasu ravnina, po svojstvima umnogome srodnu klasičnoj, realnoj projektivnoj geometriji ravnine.

Teorem 5.13. *Neka je V vektorski prostor dimenzije 3 nad poljem F . Definiramo incidencijsku strukturu $\mathcal{P} = (\mathcal{T}, \mathcal{B}, I)$ tako da je $\mathcal{T}$ skup svih 1-dimenzionalnih potprostora, a $\mathcal{B}$ skup svih 2-dimenzionalnih potprostora prostora V , dok je $I = \subseteq$ relacija inkluzije među skupovima. Tada je $\mathcal{P}$ projektivna ravnina koju označavamo s $PG(2, F)$. Posebno, ako je $F = GF(q)$ konačno polje, onda je $PG(2, F) = PG(2, q)$ projektivna ravnina reda q .*

Dokaz. Formalno je lako provjeriti valjanost aksioma (P1)-(P3) za ovako definiranu strukturu $\mathcal{P}$, služeći se jednostavnim činjenicama iz linearne algebre, no korisno je također predočiti si tu strukturu onako kao što bismo to učinili u intuitivnom, trodimenzionalnom euklidskom prostoru: skup svih pravaca (to su naše “točke”) i svih ravnina (to su sada “pravci”) koje prolaze jednom odabranom točkom (ishodište - nulvektor). Ukratko,

svaka dva od tih pravaca sadržana su u točno jednoj ravnini (jer se sijeku), a svake dvije ravnine sijeku se po jedinstvenom zajedničkom pravcu (jer nisu paralelne). U terminima linearne algebre, dva različita 1-dimenzionalna potprostora S i T sadržana su u svojoj sumi $S + T$, a to je jedini 2-dimenzionalni potprostor koji ih sadrži, dok svaka dva različita 2-dimenzionalna potprostora L i M imaju za presjek 1-dimenzionalni potprostor $L \cap M$ (možemo primijeniti jednakost $\dim(L + M) + \dim(L \cap M) = \dim L + \dim M$, u kojoj je $\dim(L + M) = \dim V = 3$). Za (P3) dostatno je uočiti točke - potprostore razapete vektorima $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ i $(1, 1, 1)$ koji postoje nad bilo kojim poljem. Svaka tri od ova četiri vektora linearno su nezavisna pa pripadni 1-dimenzionalni potprostori nisu sadržani u istom 2-dimenzionalnom potprostoru. Time je dokazan prvi dio tvrdnje. Projektivna ravnina $\mathcal{P}$ konstruirana na ovaj način standardno se označava s $PG(2, F)$ (projektivna geometrija dimenzije 2 nad poljem F).

Uzimimo sada konačno polje reda q . Trebamo samo prebrojati točke na bilo kojem pravcu kako bismo ustanovili red pripadne ravnine. Kako u 2-dimenzionalnom potprostoru ukupno ima $q^2 - 1$ vektora različitih od nulvektora, a svaki 1-dimenzionalni potprostor sadrži točno $q - 1$ takvih vektora (i različiti 1-dimenzionalni potprostori nemaju zajedničkih vektora osim 0), vidimo da ima točno $(q^2 - 1)/(q - 1) = q + 1$ potprostora dimenzije 1 sadržanih u bilo kojem 2-dimenzionalnom potprostoru. Dakle, red projektivne ravnine $\mathcal{P}$ jednak je $(q + 1) - 1 = q$. $\square$

Na temelju prethodnog teorema možemo konstruirati projektivne ravnine reda 2, 3, 4, 5, 7, 8, 9, 11, 13 itd. Posebno je jednostavna konstrukcija ravnine reda 2, jer nad poljem $GF(2)$ svaki 1-dimenzionalni vektorski prostor sastoji se samo od nulvektora $(0, 0, 0)$ i još jednog vektora s koordinatama 0 ili 1 (ima ih, dakako, sedam). Pravci, tj. 2-dimenzionalni potprostori, mogu se jednostavno zadati homogenim linearnim jednadžbama poput $x_1 = 0$ (sadrži točke $(0, 1, 0)$, $(0, 0, 1)$ i $(0, 1, 1)$).

Napomena 5.14. U poglavlju 7 bit će dokazano da ne postoji projektivna ravnina reda 6. Za $n = 2, 3, 4, 5, 7$ i 8 poznato je da je svaka projektivna ravnina reda n izomorfna ravnini $PG(2, n)$. Za $n = 9$ postoje točno četiri međusobno neizomorfne ravnine tog reda, među kojima je, dakako, i $PG(2, 9)$.

Napomena 5.15. Konstrukcijom iz teorema 5.13 možemo dobiti različite beskonačne projektivne ravnine ako za polje F izaberemo npr. $\mathbb{R}$ ili $\mathbb{C}$. Nadalje, moguće je konstrukciju provesti i pomoću vektorskog prostora nad (nekomutativnim) tijelom, poput tijela kvaterniona. Kako je već spomenuto, konačno tijelo uvijek je komutativno, dakle nužno je to i polje.

Pokažimo, kako je i najavljeno, da se konačna projektivna ravnina ne može “nacrtati” u euklidskoj ravnini koristeći samo točke i pravce. Tvrdnja vrijedi i općenitije, za bilo koji $2-(v, k, 1)$ dizajn s $k \geq 3$. Argument će biti jasan i bez strogog formaliziranja. Pretpostavimo suprotno, da smo dizajn $\mathcal{D}$ uspjeli nacrtati u euklidskoj ravnini, to jest da postoji injekcija sa skupa točaka i blokova (pravaca) dizajna u odgovarajuće skupove u euklidskoj ravnini pri čemu je sačuvana incidencija (kolinearnost). Kako neincidentnih parova točka-pravac (u slici dizajna) ima konačno mnogo, možemo izabrati onaj par za koji je udaljenost točke i pravca minimalna, ali pozitivna. Neka su to točka p i pravac L . Spustimo okomicu iz p na L i nožište označimo s p' . Točka p' može i ne mora pripadati slici

dizajna. Ako joj ne pripada, koristimo činjenicu da na L imamo barem tri točke dizajna. Barem dvije od njih, označimo ih q_1 i q_2 , su s iste strane točke p' . Tada pravci pq_1 i pq_2 pripadaju slici dizajna, a trokut pq_1q_2 je tupokutan. Ako je npr. q_1 vrh uz tupi kut, onda je udaljenost od q_1 do pravca pq_2 strogo manja od udaljenosti p i p' (jer ta udaljenost je duljina visine spuštenu q_1q_2 kao stranicu trokuta kraću od pq_2). To je u proturječju s izborom p i L . Slično, ako p' pripada slici dizajna $\mathcal{D}$, neka je q bilo koja od ostalih točaka dizajna na L pa imamo pravokutni trokut $pp'q$ čije sve tri stranice odgovaraju pravcima dizajna, no udaljenost p' od pq strogo je manja od udaljenosti p i p' čime opet dobivamo proturječje. Time smo se uvjerali da slike $2-(v, k, 1)$ dizajna poput onih iz primjera 1.4 i 1.5 nužno moraju sadržati kružnice ili druge krivulje.

5.3 Desarguesova i Papposova konfiguracija

Za strukturu projektivnih ravnina poseban značaj imaju određene konfiguracije i svojstva povezana s njima. Spomenut ćemo dvije najvažnije, Desarguesovu i Papposovu konfiguraciju. Najprije trebamo nekoliko definicija.

Definicija 5.16. *Konačnu incidencijsku strukturu koja je uniformna i regularna, a bilo koje dvije točke imaju najviše jednu spojnicu nazivamo konfiguracijom. Uz uobičajene dosadašnje oznake, govorimo o (v_r, b_k) konfiguraciji. Posebno, simetrična (v_r) konfiguracija sastoji se od jednakog broja točaka i pravaca ($v = b$, a tada i $r = k$).*

Uočavamo da je svaki $2-(v, k, 1)$ dizajn konfiguracija, no konfiguracija ne mora imati ispunjeno svojstvo balansiranosti.

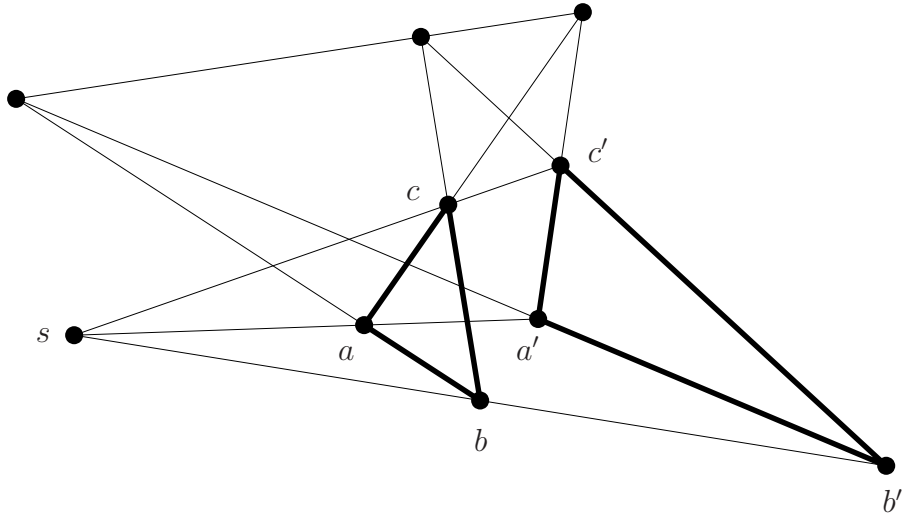
Ako npr. u projektivnoj ravnini imamo podskup od m točaka takvih da nikoje tri nisu kolinearne, tih m točaka i njihovih $\binom{m}{2} = \frac{m(m-1)}{2}$ spojnica čine $(m_{m-1}, \binom{m}{2}_2)$ konfiguraciju, takozvani *potpuni m -terovrh*. Najjednostavnije takve konfiguracije su trovrh i potpuni četverovrh, za $m = 3$ odnosno $m = 4$. Drukčije, ako u podskup od m točaka uvedemo uređaj, dakle oznake poput $a_1, a_2, \dots, a_m$, kažemo da te točke određuju *obični m -terovrh* ako nikoje tri uzastopne točke nisu kolinearne, pri čemu uređaj shvaćamo ciklički pa su uzastopne trojke točaka također i a_{m-1}, a_m, a_1 kao i a_m, a_1, a_2 . Spojnice uzastopnih točaka nazivamo stranama tog običnog m -terovrha pa time dobivamo jednostavnu simetričnu (m_2) konfiguraciju. Primijetimo da je (samo) trovrh i obični i potpuni m -terovrh pa možemo ukratko govoriti o trovrhu.

Definicija 5.17. *Neka su abc i $a'b'c'$ dva trovrha u projektivnoj ravnini. Kažemo da su ti trovrsi centralno perspektivni ako spojnice odgovarajućih vrhova – aa' , bb' i cc' – prolaze jednom točkom, označimo je s , koja se tada naziva centrom perspektiviteta naznačenih trovrha. Dualno, kažemo da su abc i $a'b'c'$ osno perspektivni ako su sjecišta odgovarajućih stranica – ab i $a'b'$, bc i $b'c'$ te ca i $c'a'$ – kolinearne točke. Pravac koji prolazi tim točkama, označimo ga s L , naziva se tada os perspektiviteta naznačenih trovrha.*

U ovoj definiciji riječ je o posebnom položaju dva trovrha u projektivnoj ravnini. Ako izbjegnemo neke posebne slučajeve u kojima se pojedine od naznačenih točaka podudaraju, za par centralno perspektivnih trovrha imat ćemo ukupno 10 različitih točaka (6

vrhova dva trovrha, centar perspektiviteta i tri sjecišta odgovarajućih stranica) te, najprije, barem 9 različitih pravaca (6 stranica dva trovrha i spojnice odgovarajućih vrhova). Ako su sjecišta pravaca ab i $a'b'$, bc i $b'c'$ te ca i $c'a'$ kolinearne točke onda one određuju deseti pravac i time se “zatvara” jedna simetrična (10_3) konfiguracija. To je tzv. Desarguesova konfiguracija, koja proizlazi iz dva trovrha koji su i centralno i osno perspektivni. Ako sjecišta pravaca ab i $a'b'$, bc i $b'c'$ te ca i $c'a'$ nisu kolinearne točke, njihovim spajanjem u parovima dobivamo tri nova pravca. Tada trovrsi nisu osno perspektivni i ne zatvara se konfiguracija. No, ako pokušamo nacrtati sve navedene točke i pravce u euklidskoj ravnini, učinit će nam se posve uvjerljivim da vrijedi osna perspektivnost, to jest da će tri sjecišta uvijek biti kolinearna. To nije slučajno, naime, ne ovisi o načinu izbora točaka i “urednosti” crtanja. Euklidska ravnina “dio” je realne projektivne ravnine $PG(2, \mathbb{R})$ (o tome još nešto kasnije), a u njoj vrijedi sljedeći važan teorem:

Teorem 5.18 (Desargues). *Dva trovrha su centralno perspektivni ako i samo ako su osno perspektivni.*



Slika 5.1: Desarguesova (10_3) konfiguracija.

To je klasični Desarguesov¹ teorem, no ista tvrdnja vrijedi i u projektivnoj ravnini $PG(2, F)$ nad bilo kojim poljem, štoviše nad bilo kojim tijelom. (Naravno, u najmanjoj ravnini $PG(2, 2)$ ne može se ostvariti pripadna (10_3) konfiguracija jer nema dovoljno točaka). Uputa za dokaz Desarguesova teorema dana je u zadatku 5.7.

Međutim, Desarguesov teorem ne samo što vrijedi u svakoj ravnini $PG(2, F)$, nego upravo i karakterizira, na posve geometrijski način, cijelu klasu projektivnih ravnina nad tijelima. Vrijedi, naime, sljedeći ključni teorem.

Teorem 5.19. *Projektivna ravnina $\mathcal{P}$ izomorfna je ravnini $PG(2, F)$ nad nekim tijelom F ako i samo ako u ravnini $\mathcal{P}$ vrijedi Desarguesov teorem.*

¹Girard Desargues (1591.-1661.), francuski matematičar, arhitekt i inženjer.

Dokaz onog smjera koji nije sadržan u zadatku 5.7, dakle tvrdnje da je u biti zatvaranje Desarguesove konfiguracije za bilo koji par perspektivnih trovrha dovoljan uvjet da bi ravnina bila tipa $PG(2, F)$, opsežan je i nimalo lagan.

Projektivna ravnina naziva se Desarguesovom (dezargovskom) ako u njoj vrijedi teorem 5.18. Dakle, projektivne ravnine mogu se razvrstati na dezargovske i nedezargovske, a dezargovske su upravo ravnine tipa $PG(2, F)$. To je jedna od bitnih činjenica iz teorije projektivnih ravnina. Vratimo li se na napomenu 5.14, možemo je dopuniti primjedbom kako su sve projektivne ravnine reda najviše 8 dezargovske, dok za red 9 postoji dezargovska i tri međusobno neizomorfne nedezargovske ravnine.

Zasad je još otvorena, ni dokazana ni opovrgnuta, hipoteza: *svaka projektivna ravnina, čiji red je primbroj, dezargovska je*. Podsjetimo se ovdje i ključne, još otvorene slutnje u vezi s egzistencijom projektivnih ravnina: *red svake konačne projektivne ravnine nužno je oblika potencije primbroja*.

Može se učiniti da nije lako naći nedezargovske projektivne ravnine, no i za njih postoji obilje modela. Mi ćemo na kraju ovog poglavlja izložiti konstrukciju jedne nedezargovske afine ravnine reda 9. Spomenimo još da postoji točno 10 međusobno neizomorfnih (10_3) konfiguracija.

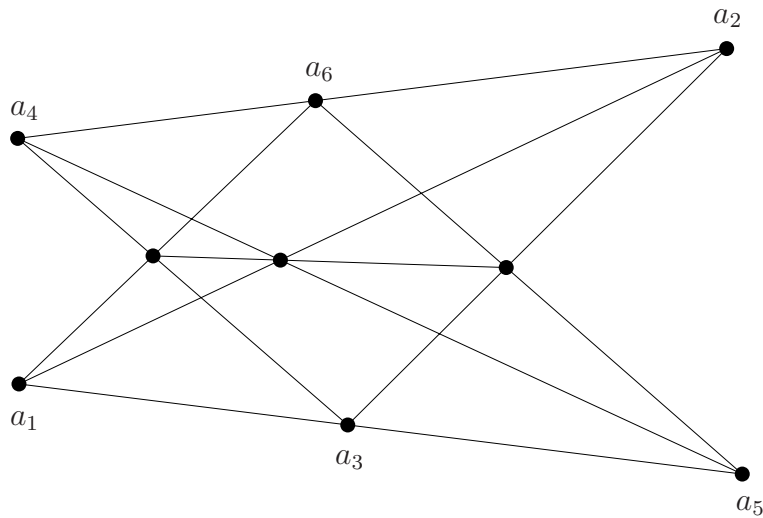
Primjer 5.20 (Ostromov teorem). *Svaka konačna projektivna ravnina reda $n \geq 5$ sadrži bar jednu Desarguesovu konfiguraciju.*

Ova tvrdnja zapravo vrijedi i za projektivne ravnine reda manjeg od 5, budući da su to sve dezargovske ravnine (s tim da za red $n = 2$ nema dovoljno točaka pravaca za pravu, nedegeneriranu (10_3) konfiguraciju), no zanimljivi argument kojim se dokazuje tvrdnja može se primijeniti općenito uz pretpostavku dostatno velikog reda ravnine. Skicirajmo samo glavnu ideju. Neka su L_1 , L_2 i L_3 tri pravca koji se sijeku u točki s (ta točka imat će ulogu centra perspektiviteta) i neka je M pravac koji ne prolazi kroz s . Na M izaberimo čvrste točke p i q , različite od sjecišta M s pravcima L_i , $i = 1, 2, 3$. Definira se preslikavanje sa skupa točaka pravca L_1 , različitih od s i sjecišta L_1 s M , u skup točaka pravca M na sljedeći način: za točku x_1 na L_1 neka je najprije x_2 sjecište pravaca px_1 i L_2 , zatim neka je točka x_3 sjecište pravaca qx_2 i L_3 te napokon označimo s x' sjecište pravca x_1x_3 s pravcem M . Na taj način za točku x dobivamo trovrh $x_1x_2x_3$ čiji su vrhovi redom na L_1 , L_2 i L_3 te imamo sjecišta p , q i x' njegovih strana s pravcem M . Za zatvaranje jedne Desarguesove konfiguracije trebaju nam dvije točke x i y na pravcu L_1 kojima bi se pridružene slike x' i y' podudarale. Postojanje takvih točaka slijedi odatle što preslikavanje x u x' nije injektivno, budući da se x bira iz skupa od $n - 1$ točaka na L_1 , dok za x' ima svega $n - 3$ mogućnosti, jer, kako se pokazuje, ta točka svakako je različita od p , q i sjecišta L_1 i L_3 s pravcem M .

Prelazimo na osnovne činjenice u vezi s Papposovom² konfiguracijom. Promatra se posebna vrsta običnog šesterovrha $a_1a_2 \dots a_6$ takvog da su po tri točke naizmjenično kolinearne: neka a_1 , a_3 i a_5 leže na pravcu L , dok a_2 , a_4 i a_6 leže na pravcu M , različitom od L te pretpostavimo da se nijedan od šest vrhova a_i ne podudara sa sjecištem pravaca L i M . Takav šesterovrh naziva se *Papposovim šesterovrhom*. Parove stranica a_1a_2 i a_4a_5 , a_2a_3 i a_5a_6 te a_3a_4 i a_6a_1 nazivamo nasuprotnim stranicama tog šesterovrha.

²Pappos ili Pappus iz Aleksandrije (oko 290.-350.), istaknuti grčki matematičar.

Teorem 5.21 (Papposov teorem). *Parovi nasuprotnih stranica Papposovog šesterovrha sijeku se u tria kolinearnim točkama. Pravac na kojem leže ta tri sjecišta naziva se Papposovim pravcem dotičnog Papposovog šesterovrha.*



Slika 5.2: Papposova (9_3) konfiguracija.

Slično kao kod Desarguesove konfiguracije i pripadnog teorema 5.18, ako nacrtamo Papposov šesterovrh u euklidskoj ravnini, kolinearnost sjecišta nasuprotnih stranica izgledat će potpuno uvjerljivom, a time će se ujedno “zatvoriti” jedna (9_3) konfiguracija koju čine šest vrhova i tri spomenuta sjecišta te šest stranica, pravci L i M i napokon Papposov pravac P . I opet, to nije slučajno jer Papposov teorem doista vrijedi i u proširenoj euklidskoj ravnini i u ravnini $PG(2, F)$ nad bilo kojim poljem F (uputu za dokaz vidi u zadatku 5.8). No, ovaj put bitna je i komutativnost množenja, dakle teorem ne vrijedi u ravnini nad nekomutativnim tijelom. Kako je konačno tijelo uvijek komutativno, spomenuta distinkcija ne dolazi do izražaja u konačnim projektivnim ravninama. Sljedeća tvrdnja analogna je teoremu 5.19.

Teorem 5.22. *Projektivna ravnina $\mathcal{P}$ izomorfna je ravnini $PG(2, F)$ nad nekim poljem F ako i samo ako u ravnini $\mathcal{P}$ vrijedi Papposov teorem.*

Iz prethodnog je onda jasno da izravno slijede:

Korolar 5.23. *Ako u projektivnoj ravnini vrijedi Papposov teorem, onda vrijedi i Desarguesov teorem.*

Korolar 5.24. *U konačnoj projektivnoj ravnini vrijedi Desarguesov teorem ako i samo ako vrijedi Papposov teorem. Svaka takva ravnina izomorfna je ravnini $PG(2, q)$ nad konačnim poljem $GF(q)$, pri čemu je q red ravnine.*

Uvodeći pojam Papposove ravnine kao projektivne ravnine u kojoj vrijedi Papposov teorem, možemo neke od prethodnih činjenica formulirati na uobičajeniji, malo sažetiji način:

- Svaka Papposova ravnina je i Desarguesova, ali obrat ne vrijedi.
- Konačna projektivna ravnina je Desarguesova ako i samo ako je Papposova.

Sad razabiremo snagu ovih “konfiguracijskih” teorema u određivanju strukture projektivne ravnine (dakako, mi zasad u ovom opsegu izlaganja uopće nemamo jasniju ideju o mogućim “odstupanjima” od strukture ravnine nad poljem, no kao što je već istaknuto, postoje mnogi primjeri nedezargovskih ravnina, što s “malenim” što s “vrlo velikim” odstupanjima od svojstava Desarguesovih odnosno Papposovih ravnina, npr. Andréove ravnine, Hughesove ravnine itd).

Još nekoliko napomena u vezi s prethodnim pojmovima i činjenicama, a pojedinosti se mogu naći npr. u [15]. Kao što je Desarguesova konfiguracija samo jedna od deset neizomorfni (10₃) konfiguracija, Papposova konfiguracija jedna je od svega tri moguće neizomorfne (9₃) konfiguracije. Nadalje, postoji čisto geometrijski (“sintetički”) dokaz (G. Hessenberg, 1903.) da je svaka Papposova ravnina ujedno i Desarguesova (neovisno o konačnosti i beskonačnosti, dakako). U [15] također se može naći najpoznatiji primjer nedezargovske beskonačne projektivne ravnine (Moultonova ravnina). Papposov teorem navodi se često i kao Pappos-Pascalov teorem, budući da analogna tvrdnja vrijedi ako su vrhovi šesterovrha raspoređeni ne na dvama pravcima nego na krivulji 2. reda (konicu), što je iznimno važan rezultat u projektivnoj geometriji (vidi također [15]).

Primjer 5.25 (Podravnine projektivne ravnine). *Za strukturu konačnih projektivnih ravnina važne su i podravnine. Ako je $\mathcal{P} = (\mathcal{T}, \mathcal{B}, I)$ projektivna ravnina i $\mathcal{T}' \subseteq \mathcal{T}$, $\mathcal{B}' \subseteq \mathcal{B}$, a I' restrikcija relacije I na $\mathcal{T}' \times \mathcal{B}'$, to jest $I' = I \cap (\mathcal{T}' \times \mathcal{B}')$, kažemo da je $\mathcal{P}' = (\mathcal{T}', \mathcal{B}', I')$ podravnina projektivne ravnine $\mathcal{P}$ ako je $\mathcal{P}'$ i sama projektivna ravnina. Za podravninu $\mathcal{P}'$ reda m u ravnini $\mathcal{P}$ reda n moguće je pokazati da vrijedi ili $n = m^2$ ili $m^2 + m \leq n$. Za drugi slučaj nije poznat niti jedan primjer u kojem vrijedi jednakost, ali ta mogućnost nije ni opovrgnuta. No, podravnine reda m kakve mogu postojati u ravninama reda $n = m^2$ imaju važnu ulogu. To su tzv. Baerove ili guste podravnine, karakterizirane svojstvom da je svaka točka ravnine incidentna s nekim pravcem podravnine i , dualno, svaki pravac ravnine prolazi nekom točkom podravnine. Nije teško npr. naći podravninu reda 2 u ravnini reda 4 i provjeriti navedeno svojstvo.*

5.4 Automorfizmi (kolineacije) projektivnih ravnina

Ovdje ćemo navesti samo neke najvažnije činjenice u vezi s automorfizmima, odnosno kolineacijama kako je uobičajenije govoriti, projektivnih ravnina. Ta tematika dobro je istražena, naročito za kolineacije ravnina tipa $PG(2, F)$ to jest dezargovskih ravnina, a osnovna svojstva nisu nužno ograničena na konačne projektivne ravnine, nego vrijede općenito. Grupu svih kolineacija projektivne ravnine $\mathcal{P} = (\mathcal{T}, \mathcal{B}, I)$ označavat ćemo, u skladu s već uvedenim, s $\text{Aut } \mathcal{P}$.

Najprije razmotrimo slučaj ravnine $\mathcal{P} = PG(2, F)$ budući da znatan dio grupe $\text{Aut } \mathcal{P}$ ovdje možemo identificirati pomoću linearnih operatora. S obzirom da su točke ovdje 1-dimenzionalni potprostori, a pravci 2-dimenzionalni potprostori vektorskog prostora F^3 , neke kolineacije svakako su određene preslikavanjima vektorskog prostora koja potprostore preslikavaju u potprostore i pritom čuvaju dimenziju. Regularni (bijektivni) linearni

operatori, tj. izomorfizmi prostora F^3 na sebe imaju upravo tražena svojstva. (Incidencija je inkluzija potprostora, sačuvana za bilo kakve linearne operatore). Takvi operatori čine opću linearnu grupu $GL(3, F)$, no ona nije izomorfna s odgovarajućom podgrupom grupe $\text{Aut } \mathcal{P}$, jer različiti linearni operatori zadaju istu kolineaciju ako su međusobno linearno zavisni, tj. ako se razlikuju samo za skalarni faktor (naime, ne promatra se djelovanje na pojedine vektore nego na 1-dimenzionalne potprostore). Zato $\text{Aut } \mathcal{P}$ sadrži podgrupu izomorfnu kvocijentnoj grupi $GL(3, F)$ po podgrupi skalarnih operatora (odnosno matrica, ako sve gledamo matrično). Jednostavno rečeno, jednoj klasi međusobno proporcionalnih regularnih matrica odgovara neka kolineacija projektivne ravnine $PG(2, F)$ i na taj način nije teško “izračunavati” sve u vezi s djelovanjem ove vrste kolineacija na točke i pravce ravnine $PG(2, F)$. Spomenuta kvocijentna grupa označava se $PGL(3, F)$ i naziva se projektivna linearna grupa. U slučaju konačnog polja $F = GF(q)$ puna grupa $\text{Aut } \mathcal{P}$ može biti ili izomorfna upravo s grupom $PGL(3, F)$ i to ako je q primbroj, ili je izomorfna s većom grupom koja sadrži $PGL(3, F)$ kao podgrupu, ako je q oblika p^s , gdje je p primbroj, a $s > 1$. Ta veća grupa, u oznaci $PTL(3, F)$ odgovara takozvanim regularnim semilinearnim operatorima, a to su kompozicije regularnih linearnih operatora s netrivialnim automorfizmima samog polja F . Za $q = p^s$ grupa $\text{Aut } F$ je ciklička, reda s .

Prethodnim činjenicama ukratko je prepričan, dakako bez dokaza, sadržaj teorema koji se često naziva temeljnim teoremom projektivne geometrije (u ovoj varijanti, za konačne dezargovske ravnine). Mi ćemo tvrdnje koje su nam od najvećeg interesa sažeti sljedećom formulacijom:

Teorem 5.26. *Neka je $\mathcal{P} = PG(2, F)$ nad poljem $F = GF(q)$, $q = p^s$. Tada je puna grupa kolineacija $\text{Aut } \mathcal{P}$ izomorfna projektivnoj semilinearnoj grupi $PTL(3, F)$, reda $s q^3(q^3 - 1)(q^2 - 1)$. Grupa $\text{Aut } \mathcal{P}$ sadrži podgrupu izomorfnu projektivnoj linearnoj grupi $PGL(3, F)$, reda $q^3(q^3 - 1)(q^2 - 1)$.*

Red grupe $PGL(3, F)$ možemo lako izračunati, prebrojavanjem regularnih matrica reda 3 nad poljem $GF(q)$. Prvi stupac matrice možemo izabrati na $q^3 - 1$ načina (sve dolazi u obzir osim nulstupca), drugi stupac na $q^3 - q$ načina (jer izuzimamo stupce linearno zavisne s već izabranim stupcem, a takvih ima q) i treći stupac na $q^3 - q^2$ načina (izuzimamo linearne kombinacije već izabranih stupca). Napokon, umnožak $(q^3 - 1)(q^3 - q)(q^3 - q^2)$, što je jednako redu grupe $GL(3, F)$, treba podijeliti s $q - 1$ (broj skalara različitih od 0) jer pojedinoj kolineaciji odgovara klasa proporcionalnih regularnih matrica. Sređivanjem dobivamo $|PGL(3, F)| = q^3(q^3 - 1)(q^2 - 1)$.

Primjerice, za projektivnu ravninu reda 2 imamo točno $2^3(2^3 - 1)(2^2 - 1) = 168$ kolineacija (među ukupno $7! = 5040$ permutacija skupa od 7 točaka). To se slaže s komentarom iza propozicije 3.4, gdje smo s pomoću GAP-a dobili 168 kao red pune grupe automorfizama.

Napomena 5.27. *U skici dokaza teorema 5.21 (Pappos) u zadatku 5.8 spomenuto je da se bez smanjenja općenitosti za četiri točke od kojih po tri nisu kolinearne mogu uzeti koordinate (tj. vektori koji razapinju pripadne potprostore) upravo $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ i $(1, 1, 1)$. Da pritom, ili u svakoj takvoj situaciji, doista nismo smanjili općenitost može se sada opravdati poznavanjem grupe kolineacija ravnine $PG(2, F)$ budući da se svaki četverovrh može prikladnom kolineacijom preslikati na taj najjednostavniji, a incidencija je, dakako, sačuvana.*

Dosadašnje razmatranje kolineacija odnosilo se samo na projektivne ravnine nad poljima, no tvrdnje o automorfizmima simetričnih dizajna općenito iz poglavlja 4 možemo, dakako, primijeniti i na konačne projektivne ravnine. Primjerice, svaka kolineacija fiksira jednako mnogo točaka i pravaca (moguće nijednu točku i nijedan pravac). Grupa kolineacija ima jednako mnogo orbita na skupu točaka i na skupu pravaca; posebno, grupa kolineacija djeluje tranzitivno na skupu točaka ako i samo ako djeluje tranzitivno na skupu pravaca. Sad ćemo se ukratko baviti samo nekim tipovima kolineacija s relativno velikim brojem fiksnih točaka i pravaca, jer takve su među geometrijski najzanimljivijima. Naime, preslikavanja poznata iz affine geometrije kao što su translacije, homotetije i zrcaljenja zapravo su posebni slučajevi takozvanih centralnih kolineacija kojima je os “neizmjereno daleki pravac”. (Također, u slučaju konačne projektivne ravnine reda n , kao “relativno veliki broj” može se uzeti upravo n).

Neka je $\mathcal{P}$ konačna projektivna ravnina reda n i $\varphi \in \text{Aut } \mathcal{P}$. Incidencijska struktura koja se sastoji od fiksnih točaka i fiksnih pravaca za φ (moguće prazni skupovi ili jednočlani skupovi), s incidencijom restringiranom iz $\mathcal{P}$, očito je zatvorena na operacije spajanja i presijecanja, tj. spojnica fiksnih točaka je fiksni pravac i, dualno, sjecište fiksnih pravaca je fiksna točka. (Primijetimo da za simetrične dizajne s $\lambda > 1$ to nije doslovce tako).

Definicija 5.28. *Kolineacija φ naziva se centralnom ako postoji točka c (centar kolineacije) takva da je svaki pravac kroz c fiksna za φ , odnosno, dualno, osnom kolineacijom ako postoji pravac L na kojem je svaka točka fiksna za φ .*

Propozicija 5.29. *Kolineacija ima centar ako i samo ako ima os.*

Dokaz. Uzmimo na primjer da je φ osna kolineacija s osi L . Ako postoji fiksna točka izvan L , očito je to centar jer je njezina spojnica sa svakom točkom na L fiksna pravac. Ako nema fiksnih točaka izvan L , za bilo koju točku x izvan L i njezinu sliku $\varphi(x)$ spojnica $x\varphi(x)$ je fiksna pravac, jer siječe L u nekoj točki c , a pravac cx preslikava se u pravac $c\varphi(x)$. Sad točka c mora biti zajedničko sjecište svih spojnica točaka izvan L s njihovim slikama, jer u protivnom za neke dvije takve točke fiksni pravci $x\varphi(x)$ i $y\varphi(y)$ sijekli bi se u fiksnoj točki izvan L , a takve nema. Obrnuta implikacija dokazuje se dualno. $\square$

Centralne kolineacije možemo, dakle, ravnopravno nazivati osnima, jer su ti pojmovi ekvivalentni, no obično biramo prvu varijantu. Kolineaciju s centrom c i osi L nazivamo (c, L) -kolineacijom. U slučaju kad je centar na osi, kolineaciju nazivamo *elacija*, a ako je centar izvan osi, nazivamo je *homologija*. Elacija ima po $n + 1$ fiksnih točaka i pravaca, dok homologija ima po $n + 2$ fiksnih točaka i pravaca.

Postojanje centralnih kolineacija u projektivnoj ravnini usko je povezano sa svojstvom zatvaranja Desarguesovih konfiguracija za pojedine točke i pravce kao centre odnosno osi kolineacija. Ovdje ćemo navesti samo najvažniji rezultat koji se odnosi na postojanje “svih mogućih” centralnih kolineacija, premda se može formulirati odgovarajuća tvrdnja koja se odnosi na pojedine centre i osi.

Teorem 5.30. *U projektivnoj ravnini postoje sve moguće centralne kolineacije tj. postoji (c, L) -kolineacija za bilo koju točku c i bilo koji pravac L , takva da zadanu točku x preslikava u zadanu točku x' (uz uvjet da su c , x , x' različite i kolinearne te da ni x ni x' nije incidentna s L) ako i samo ako je ravnina dezargovska.*

Skica dokaza. Za razumijevanje tvrdnje teorema, a ujedno i njegova dokaza, važno je uočiti sljedeće (svakako uz skicu!). Želimo li konstruirati (c, L) -kolineaciju koja preslikava x u x' , sliku bilo koje točke y (koja ne pripada pravcu cx) konstruirat ćemo kao sjecište pravca cy i pravca koji je slika pravca xy , a taj se s xy siječe na osi L . No, ako ponovimo odgovarajući postupak za neku daljnju točku z , dobivena točka z' ne smije ovisiti o tome jesmo li je odredili pomoću x i x' ili pomoću y i y' . Lako se vidi da ta jednoznačnost rezultata ovisi o tome sijeku li se sva tri para pravaca xy i $x'y'$, yz i $y'z'$ te zx i $z'x'$ u točkama pravca L , što znači da ovisi o valjanosti Desarguesovog teorema. (Imamo trovrhe xyz i $x'y'z'$ koji su centralno perspektivni, a trebaju biti i osno perspektivni). Uzimajući to u obzir, lako se dokaže i obrnuta tvrdnja, da iz postojanja “svih mogućih” centralnih kolineacija slijedi valjanost Desarguesova teorema. $\square$

Ako identičku kolineaciju smatramo (trivijalnom) centralnom i osnom kolineacijom, različiti skupovi centralnih kolineacija sa zajedničkim centrom ili zajedničkom osi činit će podgrupe grupe svih kolineacija $\text{Aut } \mathcal{P}$. Ovdje nećemo ulaziti u pojedinosti. No, istaknut ćemo jednu važnu klasu projektivnih ravnina, takozvane translacijske ravnine.

Definicija 5.31. *Kažemo da je pravac L translacijski pravac u projektivnoj ravnini $\mathcal{P}$ ako je grupa svih elacija s osi L tranzitivna na skupu svih točaka izvan L . Ravnina $\mathcal{P}$ se naziva translacijskom ravninom ako u njoj postoji bar jedan translacijski pravac.*

Može začuditi uporaba pojma “translacijski” koji pripada afinoj geometriji, a ne projektivnoj, no on je uobičajen iz razloga što se izuzimanjem takvog pravca iz projektivne ravnine dobiva afina ravnina s punom grupom translacija. Za nju se također upotrebljava termin translacijska ravnina.

Primijetimo sljedeće: elacija s osi L zadana je slikom bilo koje točke a izvan pravca L , jer centar elacije je tada sjecište L sa spojnicom a i njezine slike. Stoga, u slučaju konačne ravnine reda n , red grupe svih elacija s osi L može biti najviše n^2 i to ako i samo ako je L translacijski pravac. Tada je grupa svih elacija s osi L strogo tranzitivna (regularna) na skupu točaka izvan L .

Po teoremu 5.30, u dezargovskoj ravnini svaki je pravac translacijski. S druge strane, translacijska ravnina ne mora biti dezargovska, no nije teško dokazati da ako u ravnini postoje tri translacijska pravca koji ne prolaze jednom točkom, onda je ta ravnina dezargovska. Naprotiv, vrlo je težak teorem da u konačnoj projektivnoj ravnini postojanje dva translacijska pravca povlači da je ta ravnina dezargovska. Vrijedi i sljedeći važan rezultat:

Teorem 5.32. *Ako je $\mathcal{P}$ konačna translacijska ravnina, njezin red je potencija primbroja.*

Iz svega navedenog jasno je koliko je translacijska ravnina “bliska” dezargovskoj, ali ipak ne mora biti dezargovska. Posljednji teorem dokazuje se pomoću teorije grupa; naime, za grupu svih elacija čija je os translacijski pravac pokazuje se da je elementarna abelova p -grupa, p primbroj, a s druge strane, kako smo već uočili, red te grupe jednak je n^2 .

Nakon kraćeg razmatranja afinih ravnina, ovo poglavlje zaključit ćemo primjerom nedezargovske translacijske ravnine.

5.5 Afina ravnina

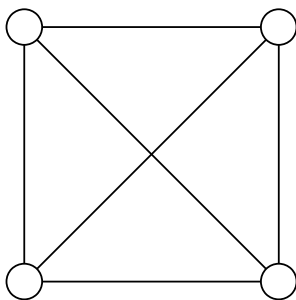
Već smo istaknuli da je afina ravnina najbliža našem uobičajenom poimanju geometrije ravnine, jer euklidska ravnina zapravo je posebna afina ravnina s bogatom dodatnom strukturom. S aspekta teorije dizajna, afina ravnina ključni je primjer rastavljivog dizajna (eng. *resolvable design*), a njezina povezanost s projektivnom ravninom glavni je primjer proširivanja nesimetričnog dizajna do simetričnog.

Definicija 5.33. *Incidencijska struktura $\mathcal{A} = (\mathcal{T}, \mathcal{B}, I)$ naziva se afinom ravninom, ako su zadovoljeni aksiomi:*

- (A1) *za svake dvije točke p, q postoji točno jedan pravac B tako da vrijedi $p I B$ i $q I B$;*
- (A2) *za svaki pravac L i svaku točku a koja nije incidentna s L postoji točno jedan pravac M takav da je $a I M$ i M nema zajedničkih točaka s L ;*
- (A3) *postoje tri različite nekolinearne točke.*

Naravno, prvi aksiom identičan je aksiomu (P1) za projektivnu ravninu, a pravac L iz aksioma (A2) nazivat ćemo pravcem kroz točku a paralelnim s pravcem M . Preciznije, na skupu pravaca $\mathcal{B}$ zadaje se relacija paralelnosti $\parallel$ tako da je $L \parallel M$ ako i samo ako je $L = M$ ili je $[L] \cap [M] = \emptyset$ (tj. ako pravci nemaju zajedničkih točaka). Lako se provjeri da je $\parallel$ relacija ekvivalencije, pri čemu je ključno mjesto primjena aksioma (A2) kod dokaza tranzitivnosti. Klase ekvivalencije su, dakle, klase paralelnih pravaca i svaku klasu nazivamo *smjerom* (katkad i pramenom paralelnih pravaca). Očito je da svakom točkom afine ravnine prolazi po jedan pravac svakog pojedinog smjera. Tako je svakim smjerom definirana jedna particija skupa $\mathcal{T}$ na skupove točaka paralelnih pravaca.

Primjer 5.34. *Iz aksioma afine ravnine nije teško izvesti da takva ravnina na svakom pravcu ima barem 2 točke te da ukupno ima barem 4 točke i barem 6 pravaca, što ujedno odgovara najmanjoj afinoj ravnini od 4 točke i 6 “spojnica” po dvije od njih. Možemo to skicirati kao paralelogram s “dijagonalama” koje se ne sijeku već također predstavljaju par paralelnih pravaca.*



Slika 5.3: Afina ravnina reda 2.

Različita svojstva afine ravnine možemo izvoditi izravno iz aksioma ili najprije ustanoviti vezu s projektivnim ravninama pa se poslužiti već poznatim svojstvima projektivnih ravnina. Navedimo ipak najprije standardni model $AG(2, F)$ afine ravnine nad poljem F (konačnim ili beskonačnim).

Teorem 5.35. *Neka je V vektorski prostor dimenzije 2 nad poljem F . Definiramo incidencijsku strukturu $\mathcal{A} = (\mathcal{T}, \mathcal{B}, I)$ tako da je $\mathcal{T} = V$, a $\mathcal{B}$ skup svih 1-dimenzionalnih linearnih mnogostrukosti prostora V , dok je I relacija “biti element” $\in$. Tada je $\mathcal{A}$ afina ravnina.*

Dokaz. Prisjetimo se da je linearna mnogostrukost dimenzije k skup vektora oblika $a + L = \{a + v \mid v \in L\}$ pri čemu je L k -dimenzionalni potprostor. Dakle, to je skup vektora dobiven translacijom potprostora L za neki vektor a . Potprostori su ujedno linearne mnogostrukosti kroz nulvektor 0 . Time definirana incidencijska struktura potpuno odgovara našem poimanju ravnine – svakoj točki odgovara vektor (“radijvektor”), a paralelni pravci dobivaju se translacijom jednog pravca (potprostora) za različite vektore. Primijetimo da su pravci ovdje paralelni ako i samo ako su definirani istim 1-dimenzionalnim potprostorom, budući da se različiti potprostori L i M sijeku (samo) u nulvektoru, a presjek linearnih mnogostrukosti $x + L$ i $y + M$ odredi se pomoću (jednoznačnog) prikaza vektora $y - x$ kao linearne kombinacije vektora koji razapinju L odnosno M . Nadalje, pravac koji spaja točke (vektore) x i y zadan je potprostorom razapetim vektorom $y - x$. Stavimo $L = [y - x]$ pa je $x = x + 0$ i $y = x + (y - x)$, dakle x i y su u linearnoj mnogostrukosti $x + L$ (i to je jedinstvena takva jer je $x + L = y + L$). Aksiom (A2) ispunjen je, jer za pravac $v + L$ i točku (vektor) a , koji mu ne pripada, pronalazimo pravac $a + L$ kao jedini kroz a koji je paralelan s $v + L$. $\square$

Primjer 5.36. *Prethodnu konstrukciju afine ravnine možemo jednostavno interpretirati tako da su točke uređeni parovi $(x, y) \in F^2$, dok su pravci skupovi točaka oblika $\{(x, y) \mid x = \text{const.}\}$ (pravci paralelni s “osi y ”) i skupovi točaka oblika $\{(x, y) \mid y = kx + l\}$, za neke $k, l \in F$ (pravci koeficijenta smjera k , uključivo 0). Sve se tada izračunava analogno kao u realnoj afinoj ravnini. Ipak, dobro je konstrukciju opisati i pomoću vektorskog prostora kao u teoremu 5.35, jer to otvara mogućnost definicije afinih prostora viših dimenzija, nad poljem.*

U zadatku 4.6 navedeno je kako se iz bilo kojeg t -dizajna dobiva tzv. rezidualni $(t-1)$ -dizajn, uklanjanjem jedne točke i svih blokova koji sadrže tu točku. Ovdje nam treba “dualni” pristup, gdje se iz simetričnog dizajna uklanja jedan blok i sve njegove točke.

Propozicija 5.37. *Neka je $\mathcal{D}$ simetrični (v, k, λ) dizajn i B bilo koji njegov blok. Incidencijska struktura dobivena uklanjanjem bloka B i svih točaka incidentnih s njim tada je nesimetrični $2-(v-k, k-1, \lambda)$ dizajn.*

Označimo s $\text{res}_B \mathcal{D}$ dizajn dobiven kao u propoziciji (rezidualni dizajn dizajna $\mathcal{D}$ u bloku B). Uzmemo li za $\mathcal{D}$ simetrični $(v, k, 1)$ dizajn, tj. konačnu projektivnu ravninu reda $n = k - 1$, kao rezidualni dizajn u bilo kojem bloku dobit ćemo $2-(n^2, n, 1)$ dizajn i to će biti afina ravnina (reda n). No, ovakav postupak nije ograničen samo na konačne projektivne ravnine – vidi zadatak 5.10. Jasno je da su pravcima projektivne ravnine koji se sijeku u nekoj od uklonjenih točaka zadani paralelni pravci u afinoj ravnini, a svaka uklonjena točka definira jedan smjer u afinoj ravnini. Ovo je ujedno uputa kako iz bilo koje afine ravnine proširivanjem dobiti projektivnu ravninu. Konstrukcija vrijedi bez obzira na pretpostavke o konačnosti ili beskonačnosti afine ravnine.

Neka je $\mathcal{A} = (\mathcal{T}, \mathcal{B}, I)$ afina ravnina. Definirat ćemo “proširene” skupove $\mathcal{T}^+$, $\mathcal{B}^+$ i I^+ kako slijedi. Uz sam $\mathcal{T}$, skup $\mathcal{T}^+$ obuhvaća sve smjerove (klase paralelnosti) kao nove “neizmjerljivo daleke” točke. Skup $\mathcal{B}^+$ sastoji se od $\mathcal{B}$ i samo jednog novog pravca, označenog s L_∞ (“neizmjerljivo daleki pravac”, “pravac u beskonačnosti”), čiji skup točaka je upravo skup svih novih točaka, tj. smjerova. Incidencijska relacija I^+ dobiva se proširivanjem I s “novim incidencijama”, a to su svi parovi koje čine pojedini smjer i bilo koji pravac tog smjera te svi parovi koje čini pojedini smjer i novi pravac L_∞ . Pokazuje se da je upravo definirana proširena incidencijska struktura projektivna ravnina – vidi zadatak 5.11.

Tvrđnje zadataka 5.10 i 5.11 pokazuju kako se proširivanjem svake afine ravnine može dobiti projektivna ravnina te kako se iz svake projektivne ravnine može dobiti afina ravnina. Pritom očito vrijedi da se uzastopnom primjenom dvaju postupaka (najprije proširivanja pa uklanjanja jednog pravca) dobiva početna afina ravnina $\mathcal{A}$. Napomenimo da se, općenito, uklanjanjem različitih pravaca iz neke projektivne ravnine neće dobiti uvijek jednake (točnije, međusobno izomorfne) afine ravnine, jer neki pravac projektivne ravnine može imati posebna svojstva koja nemaju drugi pravci. Ovakva veza također postoji između ravnina $AG(2, F)$ i $PG(2, F)$, iako to nije sasvim očito. Zapravo, proširivanjem $AG(2, F)$ dobiva se ravnina izomorfna s $PG(2, F)$, što nije sasvim trivijalno, kao ni obrnuti smjer – “redukcija” do afine ravnine izomorfne s $AG(2, F)$. “Obostrani prijelaz” između projektivne i afine ravnine omogućuje nam sljedeći zaključak:

Teorem 5.38. *Ako je $\mathcal{A}$ afina ravnina sa svojstvom da je jedan njezin pravac incidentan s točno n točaka, $n \geq 2$, onda se njezinim proširivanjem dobiva projektivna ravnina $\mathcal{P}$ reda n . Rezidualni dizajn ravnine $\mathcal{P}$ u bilo kojem njezinom pravcu je afina ravnina, koja je time $2-(n^2, n, 1)$ dizajn.*

Primjer 5.39. *U primjeru 1.5 vidjeli smo $2-(9, 3, 1)$ dizajn, tj. afinu ravninu reda $n = 3$.*

Posebno, vidimo da konačnost skupa točaka bilo kojeg pravca afine ravnine povlači konačnost čitavog njezinog skupa točaka i jednakobrojnost skupova točaka incidentnih s bilo kojim pravcem. (Kao i kod projektivnih ravnina, ovo smo mogli izvesti i izravno iz aksioma, što je korisna vježba). Možemo stoga govoriti o afinoj ravnini reda n . Ravnina $AG(2, F)$ nad poljem $F = GF(q)$ očito je reda q . Nadalje, izravno dobivamo da afina ravnina reda n ima $n+1$ klasa paralelnih pravaca, a svaka se sastoji od n pravaca. Svakom točkom afine ravnine prolazi po jedan pravac iz svake klase.

Korolar 5.40. *Konačna projektivna ravnina reda n postoji ako i samo ako postoji afina ravnina reda n . Afina ravnina reda n postoji za svaki n oblika potencije primbroja.*

Napomena 5.41. *Dizajn s parametrima $2-(v, k, \lambda)$ naziva se rastavljivim ako postoji particija njegovog skupa blokova na familije blokova takve da je svaka točka incidentna s točno jednim blokom iz svake od tih familija. Jasno je onda da tih familija mora biti točno $r = \lambda \cdot \frac{v-1}{k-1}$, a svaka se sastoji od točno $\frac{b}{r} = \frac{v}{k}$ blokova koji nemaju zajedničkih točaka. Afina ravnina reda n tipični je rastavljivi dizajn, s particijom skupa pravaca na klase paralelnosti. U uvodnom poglavlju spomenuli smo klasični Kirkmanov “problem 15 učenica” kao pitanje postojanja rastavljivog $2-(15, 3, 1)$ dizajna. Dokazano je da $2-(v, 3, 1)$ dizajn sa svojstvom rastavljivosti postoji za svaki broj točaka v oblika $v \equiv 3 \pmod{6}$, $v \geq 9$.*

Napomena 5.42 (Kolineacije afine ravnine). Ovdje nećemo podrobnije razmatrati grupu kolineacija afine ravnine, no služeći se načinom zaključivanja primijenjenim na projekтивne ravnine tipa $PG(2, F)$ i pomoću malo linearne algebre, lako možemo zaključiti kako $AG(2, F)$ posjeduje kolineacije oblika $(x, y) \mapsto (a_1x + b_1y + c_1, a_2x + b_2y + c_2)$ uz uvjet $a_1b_2 - a_2b_1 \neq 0$, dakle kompozicije djelovanja regularnim linearnim operatorom i translacije za vektor (c_1, c_2) . Nadalje, povezujući razmatranje kolineacija općenito s projekтивnom ravninom koja je iz afine dobivena proširivanjem pravcem L_∞ vidimo da su kolineacije afine ravnine inducirane upravo onim kolineacijama projekтивne ravnine koje pravac L_∞ drže fiksnim (u cjelini, ne nužno po svim točkama). Translacije u afinoj ravnini zapravo su elacije s osi L_∞ , a homologije s tom osi su homotetije u afinoj ravnini. Kako smo već spomenuli, ovim je objašnjen i pojam translacijskog pravca u projekтивnoj ravnini, a translacijska ravnina može se promatrati i kao projekтивna i kao afina ravnina.

Napomena 5.43 (Projektivni i afini prostori viših dimenzija). Analogno s $PG(2, F)$ i $AG(2, F)$ mogu se definirati projekтивne i afine geometrije dimenzija $m \geq 2$ nad bilo kojim poljem F . Tako je $PG(m, F)$ familija svih potprostora $(m+1)$ -dimenzionalnog vektorskog prostora V nad F , pri čemu osim točaka kao 1-dimenzionalnih potprostora imamo d -dimenzionalne potprostore za $2 \leq d \leq m$ u ulazi $(d-1)$ -dimenzionalnih “ravnina” (uočimo: algebarska dimenzija za 1 je veća od projekтивne dimenzije). Za konačne geometrije posebno je od interesa da unutar $PG(m, F)$ imamo dizajne koje čine potprostori bilo kojih dviju različitih dimenzija između 1 i $m-1$. Za izražavanje njihovih parametara praktično je upotrijebiti tzv. Gaussove koeficijente: $\begin{bmatrix} m \\ d \end{bmatrix}_q$ označava broj d -dimenzionalnih potprostora m -dimenzionalnog vektorskog prostora nad poljem $GF(q)$. Nije teško izračunati

$$\begin{bmatrix} m \\ d \end{bmatrix}_q = \frac{(q^m - 1)(q^m - q) \cdots (q^m - q^{d-1})}{(q^d - 1)(q^d - q) \cdots (q^d - q^{d-1})} = \frac{(q^m - 1)(q^{m-1} - 1) \cdots (q^{m-d+1} - 1)}{(q^d - 1)(q^{d-1} - 1) \cdots (q - 1)}.$$

Označimo s $PG_d(m, q)$ incidencijsku strukturu koju čine 1-dimenzionalni potprostori i $(d+1)$ -dimenzionalni potprostori $(m+1)$ -dimenzionalnog vektorskog prostora nad $GF(q)$ (projektivno geometrijski gledano, točke i d -ravnine u m -dimenzionalnom projekтивnom prostoru). Tada je $PG_d(m, q)$ dizajn s parametrima $v = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q = \frac{q^{m+1}-1}{q-1}$, $k = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q = \frac{q^{d+1}-1}{q-1}$, $\lambda = \begin{bmatrix} m-1 \\ d-1 \end{bmatrix}_q$. Slično, neka je $AG_d(m, q)$ incidencijska struktura koju čine vektori i d -dimenzionalne linearne mnogostrukosti u m -dimenzionalnom vektorskom prostoru nad $GF(q)$ (točke i d -ravnine u m -dimenzionalnom afinom prostoru). Tada je $AG_d(m, q)$ dizajn s parametrima $v = q^m$, $k = q^d$ i $\lambda = \begin{bmatrix} m-1 \\ d-1 \end{bmatrix}_q$. Primjerice, u “najmanjem” projekтивnom prostoru dimenzije 3, $PG_1(3, 2)$ je 2-(15, 3, 1) dizajn, a $PG_2(3, 2)$ je (simetrični) 2-(15, 7, 3) dizajn. U najmanjem afinom prostoru dimenzije 3, $AG_1(3, 2)$ je 2-(8, 2, 1) dizajn, a $AG_2(3, 2)$ je 2-(8, 4, 3) dizajn. Taj dizajn je rezidualni za $PG_2(3, 2)$.

5.6 Primjer nedesarguesovske ravnine reda 9

Već je spomenuto da postoje (do izomorfizma) točno četiri projekтивne ravnine reda 9, od kojih je jedna dezargovska $PG(2, 9)$, a tri su nedezargovske. Stoga postoje (do izomor-

fizma) i barem četiri³ afine ravnine reda 9. Nismo posebno isticali pojam dezargovske i nedezargovske afine ravnine, no uzimajući u obzir vezu afinih i projektivnih ravnina izloženu u prethodnom odjeljku o afnim ravninama, jasno je da ako Desarguesov teorem nije ispunjen u nekoj afinoj ravnini, onda to ne može biti ni u projektivnoj ravnini dobivenoj njezinim proširenjem. Stoga će nam model nedezargovske afine ravnine sam po sebi osigurati i model nedezargovske projektivne ravnine.

U ovom modelu modificirat će se ideja izgradnje ravnine $AG(2, 3)$ kako je izložena u primjeru 5.36. Neka je, dakle, F polje $\mathbb{Z}_3 = \{0, 1, 2\}$ s operacijama zbrajanja i množenja modulo 3. Neka je V vektorski prostor dimenzije 2 nad F . Prostor V se sastoji od 9 vektora. Za skup točaka incidencijske strukture uzet ćemo $V \times V$, tako da će postojati 81 točka, u skladu s brojem točaka afine ravnine reda 9. Pravci će biti skupovi točaka (x, y) , gdje su $x, y \in V$ koji zadovoljavaju određene jednadžbe, analogne prijašnjima.

Osim pravaca koji su skupovi parova s konstantnim $x = c$, ostali pravci bit će zadani jednadžbama oblika $y = Mx + b$, pri čemu ulogu “koeficijenta smjera” preuzima matrica M iz prikladno odabranog skupa $\mathcal{M}$ od 9 matrica reda 2 nad F , dok je $b \in V$. Pravaca opet ima $81 + 9 = 90$. No, treba ispitati kakva svojstva bi trebao imati skup $\mathcal{M}$ da bi izgrađena incidencijska struktura bila afina ravnina. Za aksiom (A1), jasno je da točke (c, y_1) i (c, y_2) imaju jedinstvenu spojnicu $x = c$, dok za (x_1, y_1) i (x_2, y_2) s različitim prvim koordinatama treba odrediti odgovarajuću matricu M i vektor b . Dobivamo: $y_2 - y_1 = M(x_2 - x_1)$. To znači da bi za zadane vektore $u, v \in V$, pri čemu je $u \neq 0$, trebala u skupu $\mathcal{M}$ postojati matrica M takva da je $Mu = v$. Jedan način da se to ostvari je sljedeći. Budući da V ima 9 elemenata, ako bi za bilo koje različite $M_1, M_2 \in \mathcal{M}$ vrijedilo $M_1u \neq M_2u$, onda bi se skup vektora Mu sastojao od 9 različitih elemenata, a među njima bi se nalazio i zadani v . (To je primjena poznate karakterizacije konačnih skupova da je svaka injekcija na takvom skupu ujedno i surjekcija). Dakle, za svake dvije od traženih matrica trebalo bi vrijediti $(M_1 - M_2)u \neq 0$ čim je $u \neq 0$, što znači da bi sve matrice $M_1 - M_2$ trebale biti regularne. Primijetimo da to ne znači da su pojedine matrice $M \in \mathcal{M}$ nužno regularne, ali se uvjet može postaviti tako da jedna od matrica bude 0 (nulmatrica), a ostalih osam da su regularne (zbog razlike s nulmatricom), uz dodatni uvjet da i njihove međusobne razlike budu regularne matrice. To se može ostvariti.

Nadalje, točkom izvan nekog pravca mora prolaziti točno jedan pravac koji nema zajedničkih točaka s tim pravcem (paralelni pravac). Lako se provjeri da su pravci s jednakim “koeficijentom smjera” (tj. matricom M) ili identični ili paralelni, dok pravci s različitim “koeficijentima” imaju jednu zajedničku točku. Naime, zajednička točka pravaca $y = M_1x + b_1$ i $y = M_2x + b_2$ dobiva se kao rješenje jednadžbe $(M_1 - M_2)x = b_2 - b_1$, a ono postoji zbog regularnosti matrice $M_1 - M_2$.

Napokon, tri nekolinearne točke su npr. $(0, 0)$, $(u, 0)$ i $(0, v)$ za bilo koje vektore $u, v \neq 0$.

Tako preostaje konstruirati odgovarajući skup od 9 matrica nad poljem reda 3, s prije navedenim svojstvima. Uz nulmatricu, to mogu biti: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$,

³Ukupan broj afinih ravnina je veći, jer uklanjanjem različitih pravaca projektivne ravnine možemo dobiti neizomorfne afine ravnine. Primjerice, afine ravnine dobivene uklanjanjem translacijskog pravca i netranslacijskog pravca iz iste projektivne ravnine nisu izomorfne. Pokazuje se da je ukupan broj afinih ravnina reda 9 jednak 7.

$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$ i $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$. Primijetimo da u prvom stupcu matrice imaju svih mogućih devet različitih oblika $\begin{bmatrix} a & \cdot \\ b & \cdot \end{bmatrix}$, s $a, b \in F$. Lako se provjeri da gornji skup matrica ima tražena svojstva tako da smo doista dobili afnu ravninu reda 9.

Jednadžbe pravaca možemo pisati i u obliku $(x_1, x_2) = \text{const.}$, odnosno $(y_1, y_2) = (\alpha_{11}x_1 + \alpha_{12}x_2 + \beta_1, \alpha_{21}x_1 + \alpha_{22}x_2 + \beta_2)$, pri čemu je $[\alpha_{ij}]$ neka od gore navedenih matrica, a $(x_1, x_2), (y_1, y_2) \in V \times V$.

Ova ravnina, nazovimo je $\mathcal{A}$, uobičajenim proširenjem daje projektivnu ravninu reda 9. Ta ravnina je translacijska, jer su preslikavanja oblika $(u, v) \mapsto (u + a, v + b)$ kolineacije ravnine $\mathcal{A}$, što se lako provjeri, kao i činjenica da takva preslikavanja (translacije) čine grupu, tranzitivnu na skupu svih točaka ravnine $\mathcal{A}$.

Preostaje pokazati da $\mathcal{A}$ nije dezargovska ravnina, dakle pronaći takav par trovrha koji imaju centar perspektiviteta, ali ne i os perspektiviteta (ili obrnuto). U afinoj ravnini možemo potražiti trovrhe kojima su vrhovi na tri paralelna pravca (centar je “neizmjerne daleka točka”), npr. na pravcima s jednadžbom $x = \text{const.}$ Uzmimo pravce $L_1: (x_1, x_2) = (0, 0)$, $L_2: (x_1, x_2) = (1, 0)$ i $L_3: (x_1, x_2) = (0, 1)$ te na njima redom točke $a = ((0, 0), (0, 0))$ i $a' = ((0, 0), (1, 0))$, $b = ((1, 0), (0, 0))$ i $b' = ((1, 0), (0, 1))$, $c = ((0, 1), (1, 2))$ i $c' = ((0, 1), (1, 0))$. Za strane trovrha dobivamo jednadžbe:

$$\begin{aligned} ab \dots (y_1, y_2) &= (0, 0), \\ a'b' \dots (y_1, y_2) &= (2x_2 + 1, x_1), \\ bc \dots (y_1, y_2) &= (2x_1 + 1, 2x_2), \\ b'c' \dots (y_1, y_2) &= (2x_1 + 2x_2 + 2, 2x_1 + x_2 + 2), \\ ca \dots (y_1, y_2) &= (x_1 + x_2, x_1 + 2x_2), \\ c'a' \dots (y_1, y_2) &= (1, 0). \end{aligned}$$

Pravci ab i $a'b'$ sijeku se u točki $((0, 1), (0, 0))$, pravci bc i $b'c'$ u točki $((1, 1), (0, 2))$, a pravci ca i $c'a'$ u točki $((2, 2), (1, 0))$. Spojnica prvih dvaju sjecišta je pravac $(y_1, y_2) = (x_2 + 2, 2x_1)$, ali taj pravac ne prolazi točkom $((2, 2), (1, 0))$ budući da za $x_1 = x_2 = 2$ vrijedi $(x_2 + 2, 2x_1) = (1, 1)$. Tako imamo primjer dva centralno perspektivna trovrha koji nisu osno perspektivni pa ravnina $\mathcal{A}$ nije dezargovska.

Zadaci

Zadatak 5.1. *Napišite cjelovite tablice zbrajanja i množenja u poljima $GF(2^2)$ i $GF(3^2)$ opisanim u primjeru 5.4.*

Zadatak 5.2. *Odredite primitivne elemente polja $GF(2^2)$ i $GF(3^2)$.*

Zadatak 5.3. *(a) Dizajn s parametrima $2-(7, 3, 1)$, tj. projektivnu ravninu reda 2 iz primjera 1.4 interpretirajte kao ravninu $PG(2, 2)$, dakle točkama koje su u to primjeru označene brojevima 1 do 7 pridružite odgovarajuće vektore nad poljem $GF(2)$.*

(b) Konstruirajte $PG(2, 3)$. Vodite pritom računa o tome da pojedini vektori različiti od nulvektora ne određuju uvijek različite 1-dimenzionalne potprostore (što ne dolazi do izražaja u $PG(2, 2)$ budući da u polju $GF(2)$ postoji samo jedan skalar osim 0).

(c) Pokušajte konstruirati neku projektivnu ravninu $PG(2, q)$ reda većeg od 3.

Zadatak 5.4. Koji su parametri projektivne ravnine $PG(2, 5)$ kao simetričnog blokovnog dizajna? Ako su $P = \langle (1, 0, 2) \rangle$ i $Q = \langle (0, 1, 3) \rangle$ dvije točke te ravnine, odredite koordinate svih točaka od $PG(2, 5)$ koje leže na spojnici PQ .

Zadatak 5.5. U projektivnoj ravnini $PG(2, 7)$ odredite sve točke na pravcu kroz $A = \langle (1, 5, 0) \rangle$ i $B = \langle (1, 1, 3) \rangle$. Točke zapišite s pomoću vektora predstavnika s vodećom nenul koordinatom 1, slično kao točke A i B . Koji su parametri od $PG(2, 7)$ kao simetričnog dizajna?

Zadatak 5.6. Odredite presjek pravaca $p = \langle (1, 2, 3), (1, 0, 2) \rangle$ i $q = \langle (1, 1, 1), (0, 1, 0) \rangle$ u projektivnoj ravnini $PG(2, 5)$.

Zadatak 5.7. Dokažite Desarguesov teorem za ravninu $PG(2, F)$ nad bilo kojim tijelom F . Uputa: tvrdnja se dokazuje sredstvima linearne algebre, budući da je takav i model ravnine $PG(2, F)$. Točke su 1-dimenzionalni potprostori pa uočimo da kolinearnost tri točke zapravo znači linearnu zavisnost vektora koji razapinju te potprostore. Označimo li, radi jednostavnosti, odgovarajuće vektore jednakim slovima kao same točke u definiciji 5.17, kolinearnost s, a, a' itd. znači da se s može izraziti kao linearna kombinacija a, a' , ali također i b, b' i c, c' . Odatle, eliminacijom s , možemo dobiti linearne kombinacije vektora a i b , odnosno b i c te c i a koje su međusobno linearno zavisne, dakle predstavljaju kolinearne točke, a redom su jednake nekim linearnim kombinacijama vektora a' i b' , odnosno b' i c' te c' i a' pa predstavljaju sjecišta pravaca ab i $a'b'$, bc i $b'c'$ odnosno ca i $c'a'$.

Zadatak 5.8. Dokažite da je svaka projektivna ravnina $PG(2, F)$ nad poljem F reda barem 3 Papposova. Uputa: Dokaz nije sasvim lagan jer zahtijeva malo vještine u linearnoalgebarskom modelu projektivne ravnine. Važno je da se bez smanjenja općenitosti za četiri od šest vrhova Papposovog šesterovrha mogu uzeti $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ i $(1, 1, 1)$ (to su vektori koji razapinju pripadne 1-dimenzionalne potprostore), a onda daljnje izračunavanje spojnica i sjecišta nije teško (pravci L i M uz ovaj izbor imaju jednadžbe $x_3 = 0$ odnosno $x_1 - x_2 = 0$). Štoviše, račun se može provoditi tako da se ne koristi komutativnost množenja pa da se tek za završni uvjet kolinearnosti vidi kako ovisi o tom svojstvu operacije množenja.

Zadatak 5.9. Dokažite propoziciju 5.37, obraćajući pozornost na važnost uvjeta simetričnosti dizajna $\mathcal{D}$.

Zadatak 5.10. Pokažite da se uklanjanjem jednog pravca i svih njegovih točaka iz bilo koje projektivne ravnine dobiva afina ravnina.

Zadatak 5.11. Dokažite da je za svaku afinu ravninu $\mathcal{A} = (\mathcal{T}, \mathcal{B}, I)$ proširena incidenzijska struktura $\mathcal{P} = (\mathcal{T}^+, \mathcal{B}^+, I^+)$ definirana na str. 50 projektivna ravnina. Uputa: kod provjeravanja ispunjenosti aksioma $(P1)$ – $(P3)$ treba razmotriti sve moguće slučajeve kako “afine točke” i “neizmjerno daleke točke” odnosno pravci ulaze u pretpostavke aksioma.

Zadatak 5.12. *Dokažite sve tvrdnje i formule iz napomene 5.43. Izračunajte i ostale parametre dizajna $PG_d(m, q)$ i $AG_d(m, q)$.*

Poglavlje 6

Diferencijski skupovi

U teoremu 3.16 vidjeli smo da od grupe koja djeluje t -homogeno na skup točaka lako dobivamo t -dizajne: za skup blokova možemo uzeti bilo koju orbitu k -članih podskupova. Međutim, za $t \geq 2$ takva djelovanja su rijetka. U ovom poglavlju naučit ćemo tehniku kojom od 1-homogenih grupa dobivamo 2-dizajne. Dizajn čine orbite k -članih podskupova koje zadovoljavaju neke dodatne uvjete. Ograničit ćemo se na simetrične dizajne i pretpostaviti jači uvjet od 1-homogenosti, tj. tranzitivnosti.

Definicija 6.1. *Neka grupa G djeluje na skup X . Kažemo da je djelovanje regularno ili strogo tranzitivno ako za svaka dva elementa $x, y \in X$ postoji jedinstveni $g \in G$ takav da je $y = gx$.*

Razlika u odnosu na tranzitivnost je što ovdje zahtijevamo jedinstvenost od g . Regularno djelovanje nam omogućuje identifikaciju elemenata skupa X s elementima grupe G . Izaberemo čvrsti $x_0 \in X$ i definiramo $\Phi : X \rightarrow G$ sa $\Phi(x) = g$, gdje je $g \in G$ jedinstveni element za koji je $gx_0 = x$. Lako se provjeri da je Φ bijekcija koja djelovanje od G na X prevodi u množenje elemenata iz G s lijeva: $\Phi(gx) = g \cdot \Phi(x)$, za sve $x \in X$, $g \in G$. Točke dizajna koje ćemo konstruirati bit će elementi grupe G , a blokovi će biti k -člani podskupovi od G sa svojstvom iz sljedeće definicije.

Definicija 6.2. *Neka je G grupa reda v s neutralnim elementom 1. Za k -člani podskup $D \subseteq G$ kažemo da je (v, k, λ) diferencijski skup ako se svaki element iz $G \setminus \{1\}$ prikazuje na točno λ načina u obliku $x^{-1}y$, za $x, y \in D$.*

Za komutativne grupe uobičajena je aditivna notacija umjesto multiplikativne. Tada neutralni element označavamo s 0, a uvjet iz definicije diferencijskog skupa kaže da se svaki element iz $G \setminus \{0\}$ prikazuje na točno λ načina kao razlika $x - y$, za $x, y \in D$.

Primjer 6.3. *Neka je $G = \mathbb{Z}_{21} = \{0, \dots, 20\}$ grupa s operacijom zbrajanja modulo 21. Promotrimo sve moguće razlike različitih elemenata iz skupa $D = \{0, 1, 4, 14, 16\}$:*

$0 - 1 = 20$	$1 - 0 = 1$	$4 - 0 = 4$	$14 - 0 = 14$	$16 - 0 = 16$
$0 - 4 = 17$	$1 - 4 = 18$	$4 - 1 = 3$	$14 - 1 = 13$	$16 - 1 = 15$
$0 - 14 = 7$	$1 - 14 = 8$	$4 - 14 = 11$	$14 - 4 = 10$	$16 - 4 = 12$
$0 - 16 = 5$	$1 - 16 = 6$	$4 - 16 = 9$	$14 - 16 = 19$	$16 - 14 = 2$

Vidimo da se svaki element iz $\mathbb{Z}_{21} \setminus \{0\}$ pojavio točno jednom kao razlika. Dakle, riječ je o $(21, 5, 1)$ diferencijskom skupu.

Primjer 6.4. Diferencijski skup s istim parametrima postoji i u nekomutativnoj grupi reda 21, $G = \langle a, b \mid a^3 = b^7 = 1, ba = ab^4 \rangle$. Slično kao u prethodnom primjeru može se provjeriti da “razlike” elemenata iz skupa $D = \{a, a^2, b, b^2, b^4\}$ pokrivaju $G \setminus \{1\}$ točno jednom.

Lijeva translacija, tj. množenje s lijeva nekim elementom grupe čuva svojstvo “biti diferencijski skup”.

Propozicija 6.5. Ako je $D(v, k, \lambda)$ diferencijski skup u grupi G , onda je to i $gD = \{gx \mid x \in D\}$.

Dokaz. Očito je $|gD| = |D|$. Nadalje, svaka dva $x', y' \in gD$ možemo na jedinstven način zapisati kao $x' = gx, y' = gy$, za $x, y \in D$. “Razlike” elemenata x', y' i x, y se podudaraju: $(x')^{-1}y' = (gx)^{-1}(gy) = x^{-1}g^{-1}gy = x^{-1}y$. Prema tome, gD je (v, k, λ) diferencijski skup ako i samo ako je to i D . $\square$

Nuždan uvjet za postojanje diferencijskih skupova podudara se s nužnim uvjetom za postojanje simetričnih dizajna (4.1).

Propozicija 6.6. Ako postoji (v, k, λ) diferencijski skup, onda vrijedi $k(k-1) = \lambda(v-1)$.

Dokaz. Od k -članog skupa možemo napraviti $k(k-1)$ razlika, a razlike pokrivaju svaki od $v-1$ elemenata iz $G \setminus \{1\}$ točno λ puta. $\square$

Sad ćemo vidjeti kako od diferencijskih skupova dobivamo simetrične dizajne.

Definicija 6.7. Neka je D podskup grupe G . Skup svih lijevih translata od D nazivamo razvoj skupa D i označavamo s $\text{dev } D = \{gD \mid g \in G\}$.

Primjer 6.8. Razvoj diferencijskog skupa $D = \{0, 1, 4, 14, 16\}$ iz primjera 6.3 je $\text{dev } D = \{\{0, 1, 4, 14, 16\}, \{1, 2, 5, 15, 17\}, \{2, 3, 6, 16, 18\}, \{3, 4, 7, 17, 19\}, \{4, 5, 8, 18, 20\}, \{0, 5, 6, 9, 19\}, \dots, \{0, 3, 13, 17, 20\}\}$. Po sljedećem teoremu riječ je o blokovima simetričnog $(21, 5, 1)$ dizajna, tj. projektivne ravnine reda 4. Ovu konstrukciju susreli smo u uvodu, u primjeru povezivanja telefona.

Teorem 6.9. Neka je $D(v, k, \lambda)$ diferencijski skup u grupi G . Onda je $\mathcal{D} = (G, \text{dev } D, \in)$ simetrični (v, k, λ) dizajn. Nadalje, G je grupa automorfizama od $\mathcal{D}$ koja djeluje regularno na skup točaka.

Dokaz. Ukupan broj točaka i blokova je $|G| = v$, a broj točaka u svakom bloku je $|gD| = k$. Treba dokazati da za svake dvije točke $x, y \in G$, $x \neq y$ vrijedi $\{x, y\} \subseteq gD$ točno za λ elemenata $g \in G$. Označimo $d = x^{-1}y \neq 1$. Po definiciji diferencijskog skupa, postoji točno λ parova $(x_i, y_i) \in D \times D$, $i = 1, \dots, \lambda$ takvih da je $x_i^{-1}y_i = d$. Definiramo $g_i = x \cdot x_i^{-1}$. Iz $x^{-1}y = x_i^{-1}y_i$ slijedi $x \cdot x_i^{-1} = y \cdot y_i^{-1}$, tj. $g_i = y \cdot y_i^{-1}$. Vidimo da je $\{x, y\} = \{g_i x_i, g_i y_i\} \subseteq g_i D$. Elementi $g_1, \dots, g_\lambda$ su međusobno različiti, pa smo dokazali da je $\{x, y\}$ sadržan barem u λ blokova razvoja $\text{dev } D$.

Obrnuto, pretpostavimo da je $\{x, y\} \subseteq g_i D$ za međusobno različite elemente $g_1, \dots, g_l \in G$. Tada postoje $(x_i, y_i) \in D \times D$ takvi da je $x = g_i x_i$, $y = g_i y_i$, za $i = 1, \dots, l$. Vrijedi $x_i^{-1} y_i = (g_i^{-1} x)^{-1} (g_i^{-1} y) = x^{-1} g_i g_i^{-1} y = x^{-1} y = d$ za $i = 1, \dots, l$. Element d prikazali smo l puta kao “razliku” elemenata iz diferencijskog skupa D , pa je $l \leq \lambda$. Time smo dokazali da je $\{x, y\}$ sadržan u točno λ blokova iz dev D , tj. $\mathcal{D}$ je simetrični (v, k, λ) dizajn.

Grupa G djeluje lijevim translacijama na samu sebe i na skup blokova dev D . Djelovanja su vjerna i čuvaju incidenciju: $x \in gD \iff hx \in hgD$, za svaki $h \in G$. Dakle, G je grupa automorfizama koja djeluje regularno na skup točaka dizajna $\mathcal{D}$ (djelovanje grupe G na samu sebe lijevim translacijama uvijek je regularno). $\square$

Idući cilj je pokazati da vrijedi obrat: svaki simetrični dizajn s grupom automorfizama koja djeluje regularno na točke može se dobiti od diferencijskog skupa.

Lema 6.10. *Ako grupa automorfizama djeluje regularno na točke simetričnog dizajna, onda djeluje regularno i na blokove tog dizajna.*

Dokaz. Zbog regularnog djelovanja, red grupe $|G|$ jednak je broju točaka v . Broj blokova je također v i G na njima djeluje tranzitivno, po korolaru 3.21. Regularnost slijedi iz jednakosti broja blokova s redom grupe. $\square$

Teorem 6.11. *Neka je G grupa automorfizama simetričnog (v, k, λ) dizajna $\mathcal{D}$ koja djeluje regularno na njegove točke. Tada postoji (v, k, λ) diferencijski skup u G takav da je njegov razvoj izomorfan s $\mathcal{D}$.*

Dokaz. Zbog regularnosti djelovanja možemo identificirati točke dizajna s elementima grupe G , blokove s k -članim podskupovima od G , a djelovanje s lijevim translacijama. Prema korolaru 3.21 djelovanje je tranzitivno na skupu blokova, tj. ako je D bilo koji blok, razvoj dev D podudara se sa skupom blokova dizajna. To znači da za svaki dvočlani podskup $\{x, y\} \subseteq G$ postoji točno λ elemenata $g_i \in G$ takvih da je $\{x, y\} \subseteq g_i D$, za $i = 1, \dots, \lambda$. Uzmimo bilo koji $d \in G \setminus \{1\}$ i neka su $g_1, \dots, g_\lambda \in G$ elementi za koje translati $g_i D$ pokrivaju dvočlani podskup $\{1, d\}$. Tada postoji točno λ parova $(x_i, y_i) \in D \times D$ takvih da je $1 = g_i x_i$, $d = g_i y_i$, tj. $d = x_i^{-1} y_i$. Tako vidimo da je D (v, k, λ) diferencijski skup u G . $\square$

Od diferencijskih skupova u grupama lako dobivamo dizajne, ali glavno pitanje je kako dobiti diferencijske skupove. Upoznat ćemo jednu konstrukciju diferencijskih skupova u aditivnim grupama konačnih polja. Prisjetimo se da polje reda q postoji ako i samo ako je q prim potencija. Ako postoji, jedinstveno je do na izomorfizam i označavamo ga s $GF(q)$. Aditivna grupa $(GF(q), +)$ je elementarno Abelova, tj. za $q = p^d$ oblika je $\mathbb{Z}_p \times \dots \times \mathbb{Z}_p$ (d faktora). Multiplikativna grupa $GF(q)^* = (GF(q) \setminus \{0\}, \cdot)$ je ciklička reda $q - 1$, a svaki element koji je generira nazivamo *primitivnim elementom* polja $GF(q)$.

Ako je q neparna prim potencija, pola elemenata multiplikativne grupe $GF(q)^*$ su kvadrati, a pola nisu kvadrati (propozicija 5.5 (1)). Skup nenul kvadrata označavamo $GF(q)^\square$, a skup nekvadrata $GF(q)^\square$. Kvadrati čine podgrupu multiplikativne grupe $GF(q)^*$ indeksa 2, a nekvadrati drugu susjednu klasu. Ako je ω primitivni element polja $GF(q)$, tj. $GF(q)^* = \langle \omega \rangle = \{\omega^i \mid i = 0, \dots, q-2\}$, onda je $GF(q)^\square = \{\omega^{2i} \mid i = 0, \dots, \frac{q-3}{2}\}$

skup parnih potencija od ω , a $GF(q)^{\square} = \{\omega^{2i+1} \mid i = 0, \dots, \frac{q-3}{2}\}$ je skup neparnih potencija od ω . Konačno, po propoziciji 5.5 (2), element -1 je kvadrat u $GF(q)$ ako i samo ako je $q \equiv 1 \pmod{4}$.

Teorem 6.12 (Paley). *Ako je $q \equiv 3 \pmod{4}$ prim potencija, onda je $GF(q)^{\square}$ diferencijski skup s parametrima $(q, \frac{q-1}{2}, \frac{q-3}{4})$ u aditivnoj grupi $(GF(q), +)$.*

Dokaz. Red aditivne grupe je $|GF(q)| = q$, a broj elemenata skupa je $|GF(q)^{\square}| = \frac{q-1}{2}$. Treba pokazati da se svaki nenul element prikazuje točno $\frac{q-3}{4}$ puta kao razlika dva kvadrata. Za $d \in GF(q)^*$ označimo s $\lambda_d = |\{(x, y) \in GF(q)^{\square} \times GF(q)^{\square} \mid d = x - y\}|$ broj načina na koji se d prikazuje kao razlika dva kvadrata. Zbog distributivnosti broj načina na koji d možemo prikazati kao razliku elemenata iz $GF(q)^{\square}$ odgovara broju načina na koji gd možemo prikazati kao razliku elemenata iz $gGF(q)^{\square}$, za proizvoljni $g \in GF(q)^*$. Ako je g kvadrat, vrijedi $gGF(q)^{\square} = GF(q)^{\square}$ i $gGF(q)^{\square} = GF(q)^{\square}$. Prema tome, postoje konstante $a, b \in \mathbb{N}$ takve da je $\lambda_d = a$ za sve $d \in GF(q)^{\square}$ i $\lambda_d = b$ za sve $d \in GF(q)^{\square}$. Još treba dokazati da je $a = b$. Očito je $\lambda_d = \lambda_{-d}$. S druge strane, zbog $q \equiv 3 \pmod{4}$ je $-1 \in GF(q)^{\square}$, pa je točno jedan od elemenata $d, -d$ kvadrat, a drugi je nekvadrat. Dakle, vrijedi $\lambda_d = a$, za svaki $d \in GF(q)^*$, tj. $GF(q)^{\square}$ je $(q, \frac{q-1}{2}, a)$ diferencijski skup. Relacija $a = \frac{q-3}{4}$ slijedi iz $k(k-1) = \lambda(v-1)$. $\square$

Diferencijske skupove iz teorema 6.12 zovemo *Paleyevim diferencijskim skupovima*. Od njih dobivamo simetrične dizajne s parametrima $(v, k, \lambda) = (q, \frac{q-1}{2}, \frac{q-3}{4})$ reda $n = \frac{q-1}{2} - \frac{q-3}{4} = \frac{q+1}{4}$. Vidimo da je $v = q = 4n - 1$, $k = \frac{q-1}{2} = 2n - 1$ i $\lambda = \frac{q-3}{4} = n - 1$, pa je riječ o Hadamardovim dizajnim. Po teoremu 4.12 oni su ekvivalentni s Hadamardovim matricama reda $q + 1$ i s $3\text{--}(q + 1, \frac{q+1}{2}, \frac{q-3}{4})$ dizajnim.

Primjer 6.13. *Primbroj $q = 11$ je kongruentan 3 modulo 4. Po teoremu 6.12 skup kvadrata $GF(11)^{\square} = \{1, 4, 9, 5, 3\}$ je $(11, 5, 2)$ diferencijski skup u $GF(11)$. Iz teorema 6.9 dobivamo simetrični $(11, 5, 2)$ dizajn, koji je po teoremu 4.12 ekvivalentan Hadamardovoj matrici reda 12 i $3\text{--}(12, 6, 2)$ dizajnu.*

Prema Dirichletovom teoremu o prostim brojevima u aritmetičkom nizu, postoji beskonačno mnogo prostih brojeva $p \equiv 3 \pmod{4}$. Zato iz teorema 6.12 dobivamo beskonačnu seriju Hadamardovih matrica i dizajna. Klasične projektivne ravnine $PG(2, q)$ također je moguće konstruirati pomoću diferencijskih skupova.

Teorem 6.14 (Singer). *Za svaku prim potenciju q postoji $(q^2 + q + 1, q + 1, 1)$ diferencijski skup u cikličkoj grupi reda $q^2 + q + 1$.*

Dokaz. Sjetimo se konstrukcije konačne projektivne ravnine reda q kao trodimenzionalnog vektorskog prostora V nad poljem $GF(q)$. Točke su jednodimenzionalni potprostori od V , pravci su dvodimenzionalni potprostori, a incidencija je inkluzija. Uzmimo sada za V polje $GF(q^3)$, koje možemo tumačiti kao trodimenzionalni vektorski prostor nad potpoljem $GF(q)$. Neka je ω primitivni element polja $GF(q^3)$, tj. $GF(q^3)^* = \{\omega^i \mid i = 0, \dots, q^3 - 2\}$. Potencije od ω kojima je eksponent djeljiv s $\frac{q^3-1}{q-1} = q^2 + q + 1$ čine nenul elemente potpolja: $GF(q)^* = \{\omega^{i(q^2+q+1)} \mid i = 0, \dots, q - 2\}$.

Definiramo preslikavanje $f : GF(q^3) \rightarrow GF(q^3)$, $f(x) = \omega x$. Riječ je o linearnom operatoru: za sve $\alpha, \beta \in GF(q)$ i $x, y \in GF(q^3)$ vrijedi $f(\alpha x + \beta y) = \omega(\alpha x + \beta y) =$

$\alpha\omega x + \beta\omega y = \alpha f(x) + \beta f(y)$. Množenje s $\frac{1}{\omega}$ (tj. funkcija $g : GF(q^3) \rightarrow GF(q^3)$, $g(x) = \frac{1}{\omega}x$) je inverzna funkcija od f , pa je f regularni linearni operator vektorskog prostora $V = GF(q^3)$. Zato preslikava potprostore od V u potprostore i pritom čuva njihovu dimenziju i inkluziju. Na taj način inducira automorfizam $\bar{f}$ projektivne ravnine. Tvrdimo da je red tog automorfizma $q^2 + q + 1$.

Tražimo najmanji prirodni broj k za koji f^k preslikava sve jednodimenzionalne potprostore od $V = GF(q^3)$ u same sebe. Jednodimenzionalni potprostori su oblika $\{\alpha x \mid \alpha \in GF(q)\}$, za $x \in GF(q^3)^*$. Množenje s ω^k ih preslikava u same sebe ako vrijedi $\omega^k \alpha x = \beta x$, za $\alpha, \beta \in GF(q)$. To je ekvivalentno s $\omega^k = \frac{\beta}{\alpha} \in GF(q)$, a tada k mora biti djeljiv s $q^2 + q + 1$. Zaključujemo da automorfizam generira cikličku grupu $\langle \bar{f} \rangle$ reda $q^2 + q + 1$ koja djeluje regularno na točke projektivne ravnine. Prema teoremu 6.11, projektivna ravnina se može dobiti od diferencijskog skupa u grupi $\langle \bar{f} \rangle$. $\square$

Primjer 6.15. *Fanovu ravninu $PG(2, 2)$ možemo konstruirati pomoću polja $GF(8)$ shvaćenog kao trodimenzionalni vektorski prostor nad $GF(2)$. Elementi polja $GF(8)$ su polinomi stupnja najviše 2 s koeficijentima iz $GF(2) = \{0, 1\}$, a množe se modulo ireducibilnog polinoma $g(x) = x^3 + x^2 + 1$. Pokazuje se da je $\omega = x$ primitivni element, tj. svi nenul elementi polja su njegove potencije: $\omega^0 = 1$, $\omega^1 = x$, $\omega^2 = x^2$, $\omega^3 = x^3 \equiv x^2 + 1$, $\omega^4 = x^3 + x \equiv x^2 + x + 1$, $\omega^5 = x^3 + x^2 + x \equiv x + 1$, $\omega^6 = x^2 + x$. Točke ravnine su jednodimenzionalni potprostori i sastoje se od nulvektora i jednog od 7 nenul vektora. Pravac razapet dvjema točkama sastoji se od odgovarajućih nenul vektora, njihovog zbroja i nulvektora. Naprimjer, pravac kroz ω^0 i ω^1 osim ta dva vektora sadrži i $\omega^0 + \omega^1 = 1 + x = \omega^5$. To znači da je $\{\omega^0, \omega^1, \omega^5\}$ diferencijski $(7, 3, 1)$ skup u multiplikativnoj grupi $\{\omega^i \mid i = 0, \dots, 6\}$. Množenje potencija od ω odgovara zbrajanju eksponenata modulo 7. Preko tog izomorfizma dolazimo do diferencijskog skupa $\{0, 1, 5\}$ u grupi $\mathbb{Z}_7$.*

Pri konstrukcijama simetričnih dizajna pomoću diferencijskih skupova, važno je odabrati prikladnu grupu te, dakako, pronaći u toj grupi odgovarajući diferencijski skup, ako postoji. Od velike pomoći pritom može biti tzv. multiplikator, a to je automorfizam grupe koji na jednostavan način djeluje na diferencijski skup, tako što ga preslikava u neki njegov translat ili ga, što je naročito povoljno, ostavlja invarijantnim. Detaljna razmatranja multiplikatora u punoj općenitosti algebarski su vrlo zahtjevna pa ćemo ovdje izložiti samo neke jednostavnije posebne slučajeve, uglavnom bez dokaza, ali u obliku koji će nam omogućiti djelotvornu primjenu u konstrukcijama diferencijskih skupova i dizajna. Ograničit ćemo se na Abelove grupe pa ćemo se, kako je to uobičajeno, sada služiti aditivnom notacijom: grupa $(G, +)$ s neutralnim elementom 0. Za element $a \in G$ i za prirodni broj m označit ćemo $a + a + \dots + a = ma$ (suma s m pribrojnika).

Propozicija 6.16. *Neka je $(G, +)$ Abelova grupa reda $|G| = v$ i neka je $k \in \mathbb{N}$. Tada je preslikavanje $a \mapsto ka$ homomorfizam grupe G u samu sebe. Posebno, ako je k relativno prost s v , onda je taj homomorfizam injektivan, a time i bijektivan, dakle automorfizam.*

Dokaz. Za $a, b \in G$ očito vrijedi $k(a + b) = ka + kb$ pa je “množenje” s k homomorfizam. Nadalje, neka je $\text{NZM}(k, v) = 1$. Element $a \in G$ pripada jezgri tog homomorfizma ako i samo ako je $ka = 0$, no to znači da a generira podgrupu reda k . (Njezini elementi su $a, 2a, \dots, (k - 1)a, 0$). Kako po Lagrangeovom teoremu red podgrupe dijeli red grupe,

ovdje mora biti $k = 1$. Stoga se u jezgri nalazi samo 0 pa je homomorfizam injektivan, a kako je grupa konačna, on je i bijektivan, to jest automorfizam grupe G . $\square$

Napomenimo da za cikličku grupu svi automorfizmi imaju upravo oblik naveden u prethodnoj propoziciji.

Definicija 6.17. *Neka je $D(v, k, \lambda)$ diferencijski skup u grupi G i neka je φ automorfizam te grupe. Kažemo da je φ multiplikator skupa D ako postoji $a \in G$ takav da je $\varphi(D) = D + a$. ($S \varphi(D)$ označen je skup slika svih elemenata skupa D pod djelovanjem automorfizma φ).*

Uzimajući u obzir propoziciju 6.16, za očekivati je da ćemo tražiti multiplikatore zadane “množenjem” elemenata grupe nekim prirodnim brojem koji je relativno prost s redom grupe. Odatle i naziv multiplikator (množitelj). Uočimo da je kompozicija multiplikatora također multiplikator. Štoviše, multiplikatori istog diferencijskog skupa i sami čine podgrupu grupe $\text{Aut } G$.

Osnovna ideja za određivanje diferencijskog skupa sastojat će se u tome da ćemo tražiti podskup grupe koji je invarijantan pod djelovanjem multiplikatora. Za tu svrhu važna su sljedeća dva rezultata.

Propozicija 6.18. *Neka je $D(v, k, \lambda)$ diferencijski skup u Abelovoj grupi G , pri čemu je $\text{NZM}(v, k) = 1$. Tada postoji $b \in G$ takav da je skup $D + b$ invarijantan pod djelovanjem svakog multiplikatora skupa D .*

Dokaz. Neka je $D = \{d_1, \dots, d_k\}$ i φ bilo koji multiplikator skupa D . Budući da je “množenje” s k automorfizam grupe G , zbog surjektivnosti postoji točno jedan $b \in G$ takav da vrijedi $kb = -(d_1 + \dots + d_k)$. Po svojstvu multiplikatora imamo $\varphi(D) = D + a$ za neki $a \in G$ pa stoga $\varphi(D + b) = D + a + \varphi(b)$. Stavimo $c = a + \varphi(b)$ pa treba pokazati da je $c = b$. Iz $0 = kb + (d_1 + \dots + d_k)$ djelovanjem s φ dobivamo $0 = k\varphi(b) + d_1 + \dots + d_k + ka = k\varphi(b) - kb + ka = kc - kb = k(c - b)$. Zbog injektivnosti “množenja” s k slijedi $c - b = 0$, dakle $\varphi(D + b) = D + b$. $\square$

U sljedećem teoremu nije nužna pretpostavka o komutativnosti grupe G .

Teorem 6.19 (Mann). *Neka je $D(v, k, \lambda)$ diferencijski skup u grupi G , neka je $k > \lambda$ i φ multiplikator skupa D . Tada postoji translat $D + a$ skupa D koji je invarijantan pod djelovanjem φ .*

Dokaz. Kao automorfizam grupe G , funkcija φ fiksira element 0. No, 0 je ujedno i točka dizajna dev D , a φ djeluje i kao automorfizam dizajna dev D , budući da po samoj definiciji multiplikatora preslikava blokove tog dizajna u blokove. Po lemi 3.19 znamo da automorfizam simetričnog dizajna ima jednako mnogo fiksnih točaka i fiksnih blokova, dakle φ fiksira barem jedan blok, a to je neki translat skupa D . $\square$

Napomena 6.20. *Ako je “množenje” nekim prirodnim brojem m automorfizam grupe G i multiplikator diferencijskog skupa $D \subseteq G$, često se jednostavno kaže da je sam taj m multiplikator.*

Primjer 6.21. U primjeru 6.3 uočavamo multiplikator $m = 4$, a u primjeru 6.13 svaki od brojeva 3, 4, 5 i 9 je multiplikator skupa kojeg čine svi kvadrati različiti od 0 u polju $GF(11)$. Općenito, za Paleyev diferencijski skup iz teorema 6.12 svaki kvadrat u polju, različit od 0, jest multiplikator koji očito ostavlja diferencijski skup invarijantnim. Za pronalaženje diferencijskog skupa poput onog u primjeru 6.3 zapravo možemo pokušati primijeniti automorfizam množenja s 2 (pa onda i s 4) kao mogući multiplikator. Množenje s 2 djeluje na grupu $G = \mathbb{Z}_{21}$ kao permutacija sa sljedećim orbitama – ciklusima: $(0)(1, 2, 4, 8, 16, 11)(3, 6, 12)(5, 10, 20, 19, 17, 13)(7, 14)(9, 18, 15)$. Ako je 2 multiplikator, onda po teoremu 6.19 postoji $(21, 5, 1)$ diferencijski skup invarijantan pod množenjem s 2, a to znači da se takav diferencijski skup mora sastojati od cijelih orbita pod djelovanjem na grupu. Očito su ciklusi duljine 6 preveliki, a ukupno 5 elemenata možemo dobiti samo kombiniranjem dvočlanog ciklusa s nekim od tročlanih ciklusa. Lako se provjeri da $\{7, 14\}$ daje diferencijski skup unijom s $\{3, 6, 12\}$, kao i unijom s $\{9, 18, 15\}$. Pokušamo li s multiplikatorom 4, diferencijski skup iz primjera 6.3 dobit ćemo kao uniju tri ciklusa: $(0)(1, 4, 16)(14)$.

Idući teorem daje dovoljne uvjete za postojanje multiplikatora diferencijskog skupa u Abelovoj grupi. Primijetimo da su uvjeti isključivo aritmetički (na parametre), a ne na strukturu diferencijskog skupa D i grupe G .

Teorem 6.22 (o multiplikatoru). *Neka je $D(v, k, \lambda)$ diferencijski skup u Abelovoj grupi G i neka primbroj p dijeli red $n = k - \lambda$, a ne dijeli v . Ako je $p > \lambda$, onda je p multiplikator skupa D .*

Za dokaz su potrebne neke algebarske tehnike kojima se ovdje nećemo baviti (tzv. grupni prsten), a dan je npr. u knjizi [16]. Teorem je iznimno koristan za traženje diferencijskog skupa sa zadanim parametrima ili dokazivanje da takav diferencijski skup ne postoji. Primjenjuje se obično u kombinaciji s teoremom 6.19, na način kako je skicirano u primjeru 6.21. Sljedeći specijalni slučaj odnosi se na diferencijske skupove s $\lambda = 1$, iz kojih dobivamo projektivne ravnine.

Korolar 6.23. *Neka je $D(v, k, 1)$ diferencijski skup u Abelovoj grupi G . Tada je svaki prim djeliteľ p od $n = k - 1$ multiplikator skupa D .*

Dokaz. Tvrdnja slijedi direktno iz teorema 6.22 ako uočimo da je svaki djeliteľ od n nužno relativno prost s $v = n(n + 1) + 1$. $\square$

Na kraju navodimo nekoliko primjera kako se s pomoću diferencijskih skupova i multiplikatora konstruiraju projektivne ravnine i drugi simetrični dizajni. Katkad je potrebno manje, katkad više truda da se od orbita pod djelovanjem multiplikatora na grupu sastavi diferencijski skup. Primijetimo da nam teorem 6.14 (Singer) osigurava postojanje diferencijskog skupa u cikličkoj grupi reda $q^2 + q + 1$ za svaku projektivnu ravninu reda q nad poljem $GF(q)$ i da je za dokaz zapravo korišten stanoviti multiplikator, samo što konstrukciju nije tako lako provesti.

Primjer 6.24. *Projektivna ravnina reda 8, tj. $(73, 9, 1)$ dizajn. Po korolaru 6.23, ako postoji odgovarajući diferencijski skup u grupi $\mathbb{Z}_{73}$, onda je $p = 2$ njegov multiplikator. Već nam ciklus $(1, 2, 4, 8, 16, 32, 64, 55, 37)$ daje $(73, 9, 1)$ diferencijski skup, što lako provjerimo.*

Primjer 6.25. Projektivna ravnina reda 9, tj. $(91, 10, 1)$ dizajn. Pokušavamo s grupom $\mathbb{Z}_{91}$ i, dakako, multiplikatorom $p = 3$. Sada nećemo imati prikladan ciklus duljine 10, a element 1 generira ciklus $(1, 3, 9, 27, 81, 61)$. Ciklus duljine 6 dobit ćemo također ako uzimamo elemente relativno proste s 91, dakle sve one koji nemaju ni 7 ni 13 kao djelitelje. Dva takva ciklusa zajedno sadrže previše točaka. Ciklus $(13, 39, 26, \dots)$ ne dolazi u obzir jer je $39 - 26 = 26 - 13 = 13$, što znači barem dva prikaza istog elementa, suprotno definiciji diferencijskog skupa s $\lambda = 1$. Nadalje, imamo cikluse $(7, 21, 63)(14, 42, 35)(28, 84, 70)(49, 56, 77)$. Vidimo da se 10 elemenata skupa D može dobiti samo u jednom od oblika $10 = 1 + 6 + 3 = 1 + 3 + 3 + 3$. Druga varijanta otpada, jer bi u njoj svi elementi skupa D bili djeljivi sa 7, a time i sve njihove razlike, čime onda ne možemo prikazati sve elemente od G . Uz malo eksperimentiranja, dolazimo napokon do diferencijskog skupa kao unije ciklusa (0) , $(1, 3, 9, 27, 81, 61)$ i $(49, 56, 77)$. Naglasimo, a to se vidi i iz ovog primjera, kako podudaranje zbroja duljina nekih ciklusa s brojem k elemenata traženog (v, k, λ) diferencijskog skupa nipošto ne znači, samo po sebi, da je unija dotičnih ciklusa doista diferencijski skup. Riječ je o nužnom, a ne dovoljnom uvjetu.

Primjer 6.26. Simetrični $(37, 9, 2)$ dizajn možemo pokušati konstruirati pomoći multiplikatora $p = 7$. Lako se dobiva ciklus $(1, 7, 12, 10, 33, 9, 26, 34, 16)$ koji je doista $(37, 9, 2)$ diferencijski skup u cikličkoj grupi $\mathbb{Z}_{37}$. Tako dobivamo još jedan primjer tzv. dvoravnine, simetričnog dizajna s $\lambda = 2$.

Primjer 6.27. Evo i jednog “negativnog” primjera. Iako simetrični $(31, 10, 3)$ dizajn postoji, ne može se dobiti kao razvoj dev D nekog diferencijskog skupa D . Naime, svaka grupa reda 31 je ciklička, a po teoremu 6.22 $p = 7$ bio bi multiplikator diferencijskog skupa, ako bi taj postojao. Neki diferencijski skup morao bi biti invarijantan pod množenjem sa 7, ali svaki element grupe $\mathbb{Z}_{31}$ različit od 0 generira predugačak ciklus za vrijednost $k = 10$ (provjerite!).

U ovom poglavlju upoznali smo diferencijske skupove. Oni predstavljaju metodu konstrukcije simetričnih dizajna s grupama automorfizama koje djeluju regularno na točke dizajna. Metoda se može generalizirati na nesimetrične dizajne s regularnim grupama automorfizama – to su takozvane *diferencijske familije*. Daljnju generalizaciju predstavljaju metode za konstrukciju dizajna s grupama automorfizama koje ne moraju djelovati regularno niti tranzitivno. Jedna od njih je Kramer-Mesnerova metoda [14], a druga takozvana *metoda taktičkih dekompozicija*. Za njezin razvoj zaslužan je i hrvatski matematičar Zvonimir Janko, poznat po otkriću sporadičnih jednostavnih grupa J_1 , J_2 , J_3 i J_4 .

Zadaci

Zadatak 6.1. Pomoću diferencijskih skupova i multiplikatora konstruirajte projektivne ravnine reda 5 i 7 te Hadamardov dizajn s parametrima $(15, 7, 3)$.

Zadatak 6.2. Dokažite da je komplement (v, k, λ) diferencijskog skupa također diferencijski skup i odredite mu parametre.

Poglavlje 7

Teorem Brucka, Rysera i Chowle

Uz opće nužne aritmetičke uvjete za postojanje dizajna s određenim parametrima (2. poglavlje), što za simetrične dizajne ukratko znači da vrijedi $\lambda(v-1) = k(k-1)$, za simetrične dizajne može se izvesti i jedan dodatni, nešto složenije izraženi uvjet. Polazište su nam relacije za incidencijske matrice iz teorema 2.10. Odsad, dakle, u ovom poglavlju uzimamo da je $\mathcal{D}$ simetrični (v, k, λ) dizajn, a A njegova incidencijska matrica. Dakako, A je kvadratna matrica reda v . Razlikovat ćemo slučajeve kada je broj točaka v paran, odnosno neparan.

Teorem 7.1 (Schützenberger, 1949.). *Ako je broj točaka v simetričnog dizajna paran, red tog dizajna $n = k - \lambda$ je kvadrat cijelog broja.*

Dokaz. Iz leme 2.11 izravno slijedi da za matricu A vrijedi

$$\begin{aligned}\det(AA^T) &= n^{v-1}[k + \lambda(v-1)] \\ &= n^{v-1}[k + k(k-1)] \\ &= n^{v-1}k^2.\end{aligned}$$

Primjenom Binet-Cauchyjeva teorema na lijevoj strani dobivamo:

$$(\det A)^2 = n^{v-1}k^2.$$

Kako je $\det A$ cijeli broj, imamo i na desnoj strani kvadrat cijelog broja pa mora i n^{v-1} biti kvadrat. No, $v-1$ je neparan broj pa stoga n mora biti kvadrat cijelog broja. (Za ove zaključke potrebna je samo elementarna teorija brojeva pa ne ulazimo u pojedinosti). $\square$

Primjer 7.2. *Parametri $(22, 7, 2)$ zadovoljavaju opće nužne uvjete postojanja dizajna, jer je $v = b = 22$, $2(22-1) = 7 \cdot 6$, ali dizajn bi bio simetričan, s parnim brojem točaka, dok bi red dizajna bio $n = 5$, što nije moguće po upravo dokazanom teoremu.*

Prelazimo na slučaj neparnog broja točaka. Glavni teorem ovog poglavlja najprije su dokazali Bruck i Ryser (1949.), samo za konačne projektivne ravnine, to jest simetrične dizajne s $\lambda = 1$, a $v = n^2 + n + 1$ u tom slučaju uvijek je neparan. Ubrzo je uslijedilo i poopćenje, za sve simetrične dizajne s neparnim v , u radu Rysera i Chowle (1950.). Mi ćemo ovdje formulirati tu općenitu verziju, a kasnije se posebno osvrnuti na slučaj projektivne ravnine.

Teorem 7.3 (Bruck, Ryser i Chowla). *Neka je $\mathcal{D}$ simetrični (v, k, λ) dizajn s neparnim brojem točaka v . Tada jednadžba*

$$nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2 = z^2 \quad (7.1)$$

ima netrivialno cjelobrojno rješenje (x, y, z) , to jest postoje cijeli brojevi x, y, z koji zadovoljavaju jednadžbu (7.1) i nisu sva tri jednaka 0.

Jednadžba (7.1) pripada posebnom tipu diofantske jednadžbe, koja se naziva Legendrovom jednadžbom, budući da je A.M. Legendre u potpunosti istražio njezinu rješivost u cijelim brojevima (1785.).

Najprije navodimo neke dobro poznate, ali netrivialne rezultate iz teorije brojeva koje ćemo primijeniti u dokazu teorema Brucka, Rysera i Chowle. Riječ je o mogućnosti prikazivanja prirodnih brojeva kao zbroja nekoliko kvadrata cijelih brojeva. Takvim problemima bavili su se i veliki matematičari poput P. Fermata i J.L. Lagrangea, a ovdje navodimo samo glavne rezultate (pojednostaki dokazi mogu se naći npr. u [8]) i jedan dio računa koji ćemo također izravno primijeniti u dokazu. Sljedeći teorem zapravo će nam biti potreban za jedan oblik formulacije Bruck-Ryserova teorema.

Teorem 7.4 (Fermat). *Prirodni broj n može se izraziti kao zbroj kvadrata dvaju cijelih brojeva ako i samo ako u rastavu broja n na prim faktore primbrojevi oblika $p \equiv 3 \pmod{4}$ dolaze isključivo s parnim eksponentima.*

Ilustrirajmo ovu tvrdnju primjerima. Ako se primbrojevi 3, 7, 11, 19... uopće ne pojavljuju kao faktori nekog broja, taj se sigurno može izraziti kao zbroj dva kvadrata, npr. $85 = 5 \cdot 17$, $85 = 6^2 + 7^2$. “Ne smeta” ni ako se npr. 3 pojavi u rastavu s parnim eksponentom: $85 \cdot 9 = 765 = 27^2 + 6^2$. No, $85 \cdot 3 = 255$ ne može se prikazati kao zbroj dva kvadrata. Uočimo da je 6 najmanji prirodni broj koji nije primbroj, a ne može se napisati kao zbroj dva kvadrata; to će biti povezano s činjenicom da ne postoji projektivna ravnina reda 6.

Trebat će nam i sljedeći

Korolar 7.5. *Ako se prirodni broj može izraziti kao zbroj kvadrata dvaju racionalnih brojeva, onda se može izraziti i kao zbroj kvadrata dvaju cijelih brojeva.*

Dokaz. Naglasimo najprije kako ova tvrdnja ne znači da su racionalni brojevi u pretpostavljenom prikazu nužno cijeli, jer npr. $1 = 1^2 + 0^2 = (3/5)^2 + (4/5)^2$. Neka je, dakle, $n = (s/t)^2 + (u/w)^2$, pri čemu su s, t, u i w nenegativni cijeli brojevi, t i w različiti od 0. Pomnožimo jednakost s $t^2 w^2$ pa dobivamo

$$n \cdot (tw)^2 = (sw)^2 + (ut)^2.$$

Desna strana je sada zbroj dva cjelobrojna kvadrata pa i broj na lijevoj strani ima to svojstvo. Po teoremu 7.4 primbrojevi oblika $p \equiv 3 \pmod{4}$ dolaze u rastavu broja na lijevoj strani samo s parnim eksponentima, a kako je $(tw)^2$ sam po sebi kvadrat, to se i u rastavu n na prim faktore spomenuti primbrojevi moraju javljati samo s parnim eksponentima. Time n ispunjava nuždan i dovoljan uvjet za prikazivost pomoću dva cjelobrojna kvadrata. $\square$

Primijetimo, nadalje, kako je svojstvo prikazivosti pomoću dva cjelobrojna kvadrata multiplikativno, to jest, ako vrijedi za neka dva prirodna broja n i m , onda vrijedi i za njihov umnožak. Naime, ako je $n = a^2 + b^2$ i $m = c^2 + d^2$, vrijedi

$$n \cdot m = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Budući da je 2 očito zbroj dva kvadrata, iz prethodnog možemo lako zaključiti kako je mogućnost prikaza pomoću dva cjelobrojna kvadrata potrebno ispitati samo za neparne primbrojeve. Gornji identitet je jednostavan, no korisno je uočiti da ga možemo interpretirati pomoću poznatog svojstva modula kompleksnog broja. Definiramo li, naime, $z_1 = a + bi$ i $z_2 = c + di$, vrijedi $|z_1 z_2| = |z_1| |z_2|$ odakle kvadriranjem dobivamo upravo $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. To ističemo zato što se slična ideja primjenjuje i kod zbroja četiri kvadrata.

Teorem 7.6 (Lagrange). *Svaki prirodni broj može se izraziti kao zbroj četiri kvadrata cijelih brojeva.*

Inače, postoji i kriterij za prikazivost pomoću tri cjelobrojna kvadrata, ali to nam ovdje nije potrebno. Prikazivost pomoću četiri kvadrata također je multiplikativno svojstvo, no u ovom slučaju rastav umnoška dva zbroja po četiri kvadrata u obliku zbroja četiri kvadrata nije tako lako “pogoditi” kao kod zbroja dva kvadrata. Možemo se, međutim, poslužiti poopćenjem kompleksnih brojeva – kvaternionima, a to su brojevi oblika $q = a + bi + cj + dk$ pri čemu su a, b, c, d realni brojevi (nama će biti dostatne cjelobrojne vrijednosti), dok su i, j, k tri “imaginarne jedinice”: $i^2 = j^2 = k^2 = -1$, s pravilima međusobnog množenja: $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$. Uz “obično” zbrajanje i množenje pomoću navedenih pravila, kvaternioni imaju algebarsku strukturu nekomutativnog tijela. Uvedemo li normu kvaterniona po uzoru na kompleksne brojeve: $|q| = |a + bi + cj + dk| = \sqrt{a^2 + b^2 + c^2 + d^2}$, možemo izravnim računom provjeriti kako vrijedi jednakost $|q_1 q_2|^2 = |q_1|^2 |q_2|^2$ za svaka dva kvaterniona. Time zapravo dobivamo tzv. Lagrangeov identitet, kao eksplicitnu formulu za pretvaranje umnoška dva zbroja od po četiri kvadrata u jedan zbroj četiri kvadrata. Naravno, za dokaz teorema 7.6 to znači reduciranje tvrdnje samo na primbrojeve.

Mi ćemo samo navesti identitet i to uz oznake koje će nam kasnije biti prikladne, budući da će se raditi o stanovitoj transformaciji koordinata. Uzmimo $n = a^2 + b^2 + c^2 + d^2$ i varijable $x_i, y_i, i = 1, 2, 3, 4$. Vrijedi:

$$n \cdot (x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

pri čemu je

$$\begin{aligned} y_1 &= ax_1 - bx_2 - cx_3 - dx_4, \\ y_2 &= bx_1 + ax_2 - dx_3 + cx_4, \\ y_3 &= cx_1 + dx_2 + ax_3 - bx_4, \\ y_4 &= dx_1 - cx_2 + bx_3 + ax_4. \end{aligned} \tag{7.2}$$

Ove relacije možemo zapisati i matricno:

$$\begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}. \tag{7.3}$$

Označimo gornju matricu reda 4 s M i (7.3) sažeto zapišimo kao $M \cdot X = Y$. Očito su retci i stupci matrice M međusobno ortogonalni (umnožak svaka dva različita jednak je 0) te vrijedi $M \cdot M^\tau = (a^2 + b^2 + c^2 + d^2)I_4 = nI_4$. Čim je n različit od 0, M je regularna matrica s cjelobrojnim koeficijentima, a njezina inverzna matrica je $M^{-1} = \frac{1}{n}M^\tau$. Vrijedi:

$$X = \frac{1}{n}M^\tau Y. \quad (7.4)$$

Dakle, inverzna matrica svakako ima racionalne koeficijente i to će nam kasnije biti važno: varijable x_1, x_2, x_3, x_4 moći ćemo zamijeniti racionalnim linearnim kombinacijama varijabli y_1, y_2, y_3, y_4 u skladu s (7.4).

Nakon ovih priprema, prelazimo na dokaz teorema 7.3.

Dokaz. Neka je, dakle, $\mathcal{D}$ simetrični (v, k, λ) dizajn s neparnim brojem točaka v . Za $n = k - \lambda$ primijenit ćemo teorem 7.6, to jest prikaz $n = a^2 + b^2 + c^2 + d^2$ pri čemu su a, b, c, d cijeli brojevi. Za incidencijsku matricu A tog dizajna vrijedi, po teoremu 2.10, jednakost

$$A \cdot A^\tau = nI + \lambda J. \quad (7.5)$$

Sve su matrice ovdje kvadratne reda v , a J je, podsjetimo, matrica čiji su svi koeficijenti jednaki 1. Uočimo da su i na lijevoj i na desnoj strani simetrične matrice (I, J i $A \cdot A^\tau$ su simetrične) pa možemo na uobičajeni način simetričnoj matrici pridružiti kvadratnu formu – homogeni polinom stupnja 2 u varijablama $x_1, x_2, \dots, x_v$. Neka je $X = \begin{bmatrix} x_1 & x_2 & \cdots & x_v \end{bmatrix}$ pa pomnožimo (7.5) s lijeve strane s X , a s desne strane s X^τ :

$$XA \cdot A^\tau X^\tau = nXX^\tau + \lambda XJX^\tau,$$

odakle imamo

$$XA \cdot (XA)^\tau = nXX^\tau + \lambda XJX^\tau.$$

Sada je $XX^\tau = x_1^2 + x_2^2 + \dots + x_v^2$ i $XJX^\tau = (x_1 + x_2 + \dots + x_v)^2$ pa na desnoj strani imamo jednostavne polinome stupnja 2. Na lijevoj strani, XA je jednoretdčana matrica koja se sastoji od cjelobrojnih kombinacija varijabli $x_1, x_2, \dots, x_v$ s koeficijentima 1 i 0, dakle od linearnih polinoma koje ćemo ukratko označiti s $L_i(x_1, x_2, \dots, x_v) = L_i$ pa konačno lijevu stranu možemo pisati kao $L_1^2 + L_2^2 + \dots + L_v^2$. Dobivamo, dakle, jednakost kvadratnih formi:

$$\sum_{i=1}^v L_i^2 = n \sum_{i=1}^v x_i^2 + \lambda \left(\sum_{i=1}^v x_i \right)^2. \quad (7.6)$$

Važno je uočiti da je (7.6) ekvivalentno s (7.5) u smislu da je (7.5) ispunjeno ako i samo ako je (7.6) zadovoljeno za svaki izbor vrijednosti $x_1, x_2, \dots, x_v$, pri čemu je nama dostatno uzimati vrijednosti iz polja $\mathbb{Q}$. Upravo će određeni izbor vrijednosti tih varijabli svesti (7.6) na jednadžbu iz iskaza teorema.

Na ovom mjestu treba razlikovati kakav ostatak daje v pri dijeljenju s 4. Uzmimo najprije $v \equiv 3 \pmod{4}$. Radi transformacije varijabli, trebat će nam da broj tih varijabli bude djeljiv s 4 pa stoga uvodimo i varijablu x_{v+1} te na obje strane (7.6) pribrojimo član nx_{v+1}^2 :

$$\sum_{i=1}^v L_i^2 + nx_{v+1}^2 = n \sum_{i=1}^v x_i^2 + nx_{v+1}^2 + \lambda \left(\sum_{i=1}^v x_i \right)^2. \quad (7.7)$$

Sada ćemo, služeći se relacijama (7.2), prijeći na varijable $y_1, y_2, \dots, y_v, y_{v+1}$. Dakako, (7.2) primjenjujemo redom na skupine “četiri po četiri” varijabli x_i pa se na kraju n više neće pojavljivati na desnoj strani, dok će se $\sum_{i=1}^{v+1} x_i$ transformirati u neku racionalnu linearnu kombinaciju varijabli y_i . Nama će biti važno samo to da je $(\sum_{i=1}^v x_i)^2$ kvadrat nekog racionalnog broja i označit ćemo taj izraz ukratko s t^2 . Na lijevoj strani, cjelobrojne linearne kombinacije varijabli x_i označene s L_i , $i = 1, 2, \dots, v$, pretvaraju se u racionalne linearne kombinacije varijabli y_i , $i = 1, 2, \dots, v+1$. Naš je cilj izabrati vrijednosti y_i tako da se izrazi L_i^2 redom ukinu s y_i^2 . Neka je $L_1 = c_1 y_1 + c_2 y_2 + \dots + c_v y_v + c_{v+1} y_{v+1}$. Ako je $c_1 = 1$, postavimo uvjet $-y_1 = y_1 + c_2 y_2 + \dots + c_v y_v + c_{v+1} y_{v+1}$, odakle je $y_1 = -\frac{1}{2}(c_2 y_2 + \dots + c_{v+1} y_{v+1})$. Ovom supstitucijom za y_1 postizemo $L_1^2 = y_1^2$. Ako je pak $c_1 \neq 1$, stavimo $y_1 = c_1 y_1 + c_2 y_2 + \dots + c_v y_v + c_{v+1} y_{v+1}$ pa će nam trebati supstitucija $y_1 = (c_2 y_2 + \dots + c_{v+1} y_{v+1})/(1 - c_1)$ za istu svrhu. Nakon ukidanja L_1^2 s y_1^2 ostaju nam izrazi u varijablama $y_2, \dots, y_{v+1}$ koje na analogni način reduciramo korak po korak. Na kraju dolazimo do jednakosti

$$nx_{v+1}^2 = y_{v+1}^2 + \lambda t^2$$

odnosno

$$nx_{v+1}^2 - \lambda t^2 = y_{v+1}^2. \quad (7.8)$$

S obzirom da je u ovom slučaju $\frac{v-1}{2}$ neparan, prepoznavamo oblik jednadžbe (7.1), s tim da ovdje imamo netrivialno rješenje u racionalnim brojevima (kako za y_{v+1} još uvijek imamo slobodan izbor, $(0, 0, 0)$ nije jedino rješenje). No, množenjem jednadžbe zajedničkim nazivnikom racionalnih brojeva dobivamo cjelobrojno rješenje.

Preostaje razmotriti $v \equiv 1 \pmod{4}$. Sad imamo jednu varijablu “viška” kod grupiranja po četiri radi primjene relacija (7.2). Stoga se (7.6) analognim postupkom kao gore transformira u oblik

$$\sum_{i=1}^v L_i^2 = \sum_{i=1}^{v-1} y_i^2 + nx_v^2 + \lambda t^2. \quad (7.9)$$

Zatim se, izborom $y_1, \dots, y_{v-1}$ kao prije, međusobno ukidaju odgovarajući L_i^2 s y_i^2 te se jednakost svodi na

$$L_v^2 = nx_v^2 + \lambda t^2,$$

odnosno

$$nx_v^2 + \lambda t^2 = L_v^2 \quad (7.10)$$

što prepoznavamo kao oblik (7.1) kada je $\frac{v-1}{2}$ paran te kao prije vidimo da postoji netrivialno cjelobrojno rješenje jednadžbe $nx^2 + \lambda y^2 = z^2$. Time je teorem dokazan. $\square$

Pogledajmo sada posebni slučaj projektivne ravnine, tj. $\lambda = 1$. Imamo $v = n(n+1)+1$ pa je $v \equiv 1 \pmod{4}$ ako i samo ako je $n \equiv 0$ ili $3 \pmod{4}$. Jednadžba (7.1) poprima oblik $nx^2 + y^2 = z^2$ ili $nx^2 = z^2 - y^2$, no rješivost ove jednadžbe ne postavlja zapravo nikakvu restrikciju na vrijednost n , budući da se za $x = 1$ svodi na prikazivost n kao razlike cjelobrojnih kvadrata. Naime, za svaki prirodni broj djeljiv sa 4 možemo pisati $4m = (m+1)^2 - (m-1)^2$, a za svaki neparni broj $2m+1 = (m+1)^2 - m^2$ što obuhvaća oba razmatrana slučaja za n . Od interesa je stoga uzeti samo $n \equiv 1$ ili $2 \pmod{4}$. Tada je $v \equiv 3 \pmod{4}$ pa (7.1) dobiva oblik $nx^2 - y^2 = z^2$ odnosno $nx^2 = y^2 + z^2$. U netrivialnom rješenju mora biti $x \neq 0$ pa možemo pisati $n = \left(\frac{y}{x}\right)^2 + \left(\frac{z}{x}\right)^2$, dakle teorem 7.3 povlači

da se red projektivne ravnine u ovom slučaju može prikazati kao zbroj dva kvadrata racionalnih brojeva. No, po korolaru 7.5 postoji onda i prikaz n kao zbroja dva kvadrata cijelih brojeva. Time dobivamo tvrdnju teorema koji je prethodio teoremu 7.3:

Teorem 7.7 (Bruck-Ryser). *Neka je n red konačne projektivne ravnine, pri čemu je $n \equiv 1$ ili $2 \pmod{4}$. Tada se n može prikazati kao zbroj dva kvadrata cijelih brojeva.*

U izvornoj formulaciji ovog teorema zapravo se uzima karakterizacija iz teorema 7.4 no ovaj iskaz čini se nešto jednostavniji. Napomenimo još da se u izvornom dokazu Brucka i Rysera koristila teorija Hasse-Minkowskog o jednakosti kvadratnih formi, no primjenom dosjetke o prikazu n kao zbroja četiri kvadrata dokaz ostaje u granicama elementarne matematike.

Primjer 7.8. *Ne postoji simetrični 2 -($29, 8, 2$) dizajn. Postojanje takvog dizajna povlačilo bi postojanje netrivialnog cjelobrojnog rješenja jednadžbe $6x^2 + 2y^2 = z^2$, a ovo se može opovrgnuti elementarnim razmatranjem svojstava djeljivosti. Naime, pretpostavimo da cijeli brojevi x, y, z čine takvo rješenje, a očito je onda da su sva tri različita od 0. Pretpostavimo da x, y i z nemaju zajedničkih djelitelja većih od 1, tj. skratimo jednadžbu koliko je moguće. Očito z mora biti paran pa uvrstimo $z = 2z_1$. Nakon skraćivanja s 2 dobivamo $3x^2 + y^2 = 2z_1^2$. Oдавde mora $2z_1^2 - y^2$ biti djeljiv s 3, a stoga i $z_1^2 + y^2$ djeljiv s 3. No, kako kvadrat cijelog broja može pri dijeljenju s 3 dati ostatak samo 0 ili 1, vidimo da bi z_1 i y oba morala biti djeljiva s 3. Tada bi i x bio djeljiv s 3, suprotno pretpostavci da je najveća zajednička mjera brojeva x, y i z jednaka 1.*

Primjer 7.9.

- (a) *Ne postoji projektivna ravnina reda 6. Ovo slijedi izravno iz teorema 7.7.*
- (b) *Ako je $n \equiv 6 \pmod{8}$ tada ne postoji projektivna ravnina reda n . Oдавde vidimo da Teorem Brucka i Rysera isključuje mogućnost postojanja projektivne ravnine za beskonačno mnogo vrijednosti n , npr. za niz 6, 14, 22, 30 itd. Sve su to brojevi na koje je teorem primjenjiv jer vrijedi $n \equiv 2 \pmod{4}$, ali zbog $n = 8m + 6 = 2(4m + 3)$ vidimo kako se neki prim djelitelj p od n , oblika $p \equiv 3 \pmod{4}$ mora pojaviti s neparnim eksponentom u faktorizaciji n pa za n nije ispunjen nužni uvjet iz teorema 7.7.*

Primjer 7.10. *Nužni uvjet za red projektivne ravnine iz teorema 7.7 nije dovoljan. Naime, $n = 10 = 1^2 + 3^2$, ali pokazano je da ne postoji projektivna ravnina reda 10 (C.W.H. Lam, L.H. Thiel i S. Swiercz, 1989.). Broj 10 jedina je zasad poznata iznimka u tom smislu. Primijetimo da na vrijednosti $n = 12, 15, 20 \dots$ teorem 7.7 nije ni primjenjiv. Nadalje, sve dosad poznate konačne projektivne ravnine imaju red oblika potencije primbroja pa je još uvijek aktualna slutnja da ravnina drukčijeg reda niti nema.*

Primjer 7.11. *Ako je n kvadrat cijelog broja, parametri (v, k, λ) ispunjavaju uvjet teorema 7.3 za svaki (neparni) v . Naime, jednadžba (7.1) ima tada rješenje $x = 1, y = 0, z = \sqrt{n}$. Vidimo stoga da ako je n kvadrat cijelog broja, za sve vrijednosti od v , parne (teorem 7.1) ili neparne, dakako uz ispunjavanje osnovne relacije $\lambda(v - 1) = k(k - 1)$, u dosad poznatim rezultatima nema zapreke za postojanje odgovarajućeg simetričnog dizajna. Doista, još uopće nije poznat primjer “dobrih” parametara s kvadratnim redom n za koje simetrični dizajn ne postoji.*

Primjer 7.12. *Za parametre koji odgovaraju Hadamardovom dizajnu, dakle $v = 4\lambda + 3$, $k = 2\lambda + 1$, uvjet iz teorema 7.3 uvijek je ispunjen. Sada je $n = \lambda + 1$ pa (7.1) glasi: $(\lambda + 1)x^2 - \lambda y^2 = z^2$, s očitim rješenjem $x = y = z = 1$. Kao i za kvadratne vrijednosti n , Hadamardovi dizajni ne samo što parametrima “glatko” prolaze nužni uvjet iz teorema 7.3 nego su doista izrazito “skloni postojanju”. (Kako je navedeno pri kraju 4. poglavlja, broj 668 je zasad (2011.) najmanji višekratnik od 4 za koji nije poznato postoji li Hadamardova matrica tog reda, što znači Hadamardov dizajn sa 667 točaka.) Ipak, valja upamtiti da Teorem Brucka, Rysera i Chowle općenito daje samo nužne, ne i dovoljne uvjete za postojanje simetričnog dizajna.*

Poglavlje 8

Latinski kvadrati

Inicirano glasovitim Eulerovim “Problemom 36 oficira” (1782.), proučavanje takozvanih latinskih kvadrata, odnosno grčko-latinskih kvadrata, čini značajan dio područja konačnih geometrija i to ne samo u povijesnom smislu. Osnovna činjenica ovdje je ekvivalentnost postojanja projektivne ravnine reda n i maksimalnog sustava međusobno ortogonalnih latinskih kvadrata reda n . Vidjet ćemo da se takav maksimalni sustav sastoji od $n - 1$ kvadratne matrice, u parovima “ortogonalne”, od kojih svaka “kodira” po jednu klasu paralelnih pravaca affine ravnine. Naime, iako tih klasa ukupno ima $n + 1$, dvije od njih mogu se formirati “po volji” i svode se na početnu numeraciju n^2 točaka ravnine, dok su onih preostalih $n - 1$ stvarno važne za konstrukciju. Sustavi ortogonalnih latinskih kvadrata imaju ključnu ulogu i u nekim drugim konstrukcijama u teoriji dizajna, npr. u Wilsonovom dokazu da su jednostavni aritmetički nužni uvjeti za postojanje dizajna također i dovoljni u asimptotičkom smislu, tj. za dostatno veliki broj točaka.

Definicija 8.1. *Kvadratna matrica L reda n naziva se latinski kvadrat reda n ako koeficijenti matrice poprimaju vrijednosti u skupu od n različitih simbola tako da se svaki od tih simbola pojavljuje točno jedanput u svakom retku i svakom stupcu matrice L .*

Napomena 8.2. *Kao što je to uobičajeno u kombinatorici, za simbole u latinskom kvadratu nije bitno kakve konkretne vrijednosti poprimaju nego samo koliko ih ima. Zato možemo uzeti da su to jednostavno cijeli brojevi $1, 2, \dots, n$ ili, po potrebi, simboli $a_1, a_2, \dots, a_n$.*

Primjeri

Matrice

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \quad \text{i} \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

očito su latinski kvadrati reda 2 koji se ne razlikuju bitno, nego samo međusobnom zamjenom simbola 1 i 2. Matrica

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

je latinski kvadrat reda 3 po čijem se uzorku lako može konstruirati latinski kvadrat bilo kojeg reda n , cikličkim pomacima koeficijenata prvog retka ili stupca matrice. Stoga za

svaki n postoji latinski kvadrat tog reda. Osnovna teškoća i nije u konstrukciji pojedinih latinskih kvadrata, nego takvih koji će biti međusobno ortogonalni. Matrica

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

također je latinski kvadrat, koji se, međutim, od onog prvog očito razlikuje i samom “strukturom” matrice, premda se iz one prve dobiva međusobnom zamjenom drugog i trećeg retka, jer ne postoji permutacija simbola 1, 2, 3 koja bi jednu matricu prevela u drugu. To će doći do izražaja i za $n \geq 4$. Prije nego što to ustanovimo, uočimo vezu između latinskih kvadrata i Cayleyevih tablica za stanovite algebarske strukture – kvazigrupe.

Definicija 8.3. *Grupoid $(G, \cdot)$ naziva se kvazigrupa ako su u njemu jednoznačno rješive jednadžbe oblika $ax = b$ i $ya = b$ za zadane $a, b \in G$.*

Grupoid je grupa ako i samo ako je kvazigrupa sa svojstvom asocijativnosti. Za konačnu kvazigrupu, njezina definicijska svojstva na Cayleyevu tablicu operacije odražavaju se upravo kao pojava svakog elementa u svakom retku i svakom stupcu tablice (uvjerite se u to, interpretirajući npr. rješivost jednadžbe $ax = b$ kao uvjet da se element b mora naći u retku Cayleyeve tablice koji odgovara elementu a). To znači da je pojam latinskog kvadrata ekvivalentan pojmu kvazigrupe. Iz gornjih primjera latinskih kvadrata reda 3 vidljivo je da postoji kvazigrupa s 3 elementa koja nije ujedno i grupa. Nadalje, već iz činjenice da za beskonačno mnogo vrijednosti n postoje neizomorfne grupe reda n može se naslutiti da će postojati i “bitno različiti” latinski kvadrati odgovarajućeg reda. Npr. za $n = 4$ postoje ciklička grupa i tzv. Kleinova grupa tog reda (u kojoj su, osim jedinice, sva tri elementa involutorna i produkt bilo koja dva od njih jednak je trećem). Pripadne Cayleyeve tablice, a time i latinski kvadrati, mogu se napisati ovako:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix} \quad \text{i} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}.$$

Pogledajmo ponovno navedene latinske kvadrate reda 3:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad \text{i} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}.$$

Ako formiramo uređene parove od koeficijenata matrica koji se nalaze na jednakim pozicijama, dobit ćemo svih 9 mogućih različitih parova koji čine skup $\{1, 2, 3\} \times \{1, 2, 3\}$. Upravo to znači ortogonalnost tih latinskih kvadrata. Ako izaberemo zapis u kojem se umjesto 1, 2, 3 u prvoj matrici pojavljuju grčka slova α, β, γ , a u drugoj latinska slova a, b, c , možemo obje matrice zapisati zajedno, tako da do izražaja dođe ortogonalnost:

$$\begin{bmatrix} \alpha a & \beta b & \gamma c \\ \beta c & \gamma a & \alpha b \\ \gamma b & \alpha c & \beta a \end{bmatrix}.$$

To je grčko-latinski kvadrat.

Definicija 8.4. *Neka su $L = [\lambda_{ij}]$ i $M = [\mu_{ij}]$ dva latinska kvadrata reda n . Kažemo da su L i M ortogonalni ako su svi uređeni parovi (λ_{ij}, μ_{ij}) , $i, j = 1, 2, \dots, n$ međusobno različiti.*

Primijetimo da u definiciji nije bitno kojim su simbolima popunjeni pojedini kvadrati. Za skup od k latinskih kvadrata reda n kaže se da je *sustav međusobno ortogonalnih latinskih kvadrata* ako su svaka dva kvadrata iz tog skupa međusobno ortogonalna. Važna je sljedeća ocjena najvećeg mogućeg broja međusobno ortogonalnih latinskih kvadrata:

Propozicija 8.5. *Za sustav od k međusobno ortogonalnih latinskih kvadrata reda n vrijedi $k \leq n - 1$.*

Dokaz. Primijetimo da se relacija ortogonalnosti dva latinska kvadrata neće narušiti ako se u nekom od njih na bilo koji način permutiraju simboli kojima je popunjen. Stoga možemo pretpostaviti da imamo međusobno ortogonalne $L_1, L_2, \dots, L_k$ takve da se prvi redak svakog od njih sastoji od koeficijenata $1, 2, \dots, n$ u prirodnom poretku. Uočimo sada poziciju $(2, 1)$ u svakoj od k matrica. Niti u jednoj matrici ne može se na tom mjestu nalaziti koeficijent 1, jer se već nalazi na poziciji $(1, 1)$. Na raspolaganju preostaje $n - 1$ simbola, a niti jedan od njih ne može se naći više od jedanput na poziciji $(2, 1)$ u promatranim matricama, jer bi se ponavljanjem nekog simbola a dvaput pojavio par oblika (a, a) , suprotno ortogonalnosti svaka dva kvadrata našeg skupa. Zato k ne može biti veći od $n - 1$. $\square$

Napomena 8.6 (Eulerov problem 36 oficira). *Leonhard Euler postavio je problem 36 oficira u sljedećem obliku: Može li se 36 oficira, od kojih svaki pripada jednoj od šest regimenti i svaki posjeduje jedan od šest činova, svrstati u kvadratnu formaciju 6×6 tako da u svakom retku i svakom stupcu tog kvadrata bude zastupljena svaka regimenta i svaki čin? Euler je takvu formaciju nazvao “novom vrstom magičnog kvadrata”, a njegova tvrdnja, navedena bez dokaza, glasila je da takav kvadratni raspored ne postoji. Očito je da se Eulerov problem svodi na postojanje grčko-latinskog kvadrata reda 6, tj. dva ortogonalna latinska kvadrata reda 6. Valjanost njegove slutnje potvrdio je Tarry, tek početkom 20. stoljeća, pri čemu se postupak sastojao u “inspekciji”, tj. nalaženju svih latinskih kvadrata reda 6 i provjeri da nikoja dva nisu ortogonalna. Naravno, kasnije su se pojavile i znatno elegantnije metode dokaza. No, Euler je postavio i općenitu slutnju kako ne postoji “magični kvadrat” reda $n = 4k + 2$ ni za koji prirodni broj k . Ta se pak pokazala pogrešnom, jer je slučaj $n = 6$ zapravo iznimka; za svaki $k \geq 2$ postoje barem dva ortogonalna latinska kvadrata reda $n = 4k + 2$.*

Teorem 8.7. *Projektivna ravnina reda n postoji ako i samo ako postoji maksimalni sustav od $n - 1$ ortogonalnih latinskih kvadrata reda n .*

Prije dokaza, evo komentara o nekim posljedicama teorema. Iz negativnog odgovora na Eulerov problem za $n = 6$, jasno je sada da ne postoji projektivna ravnina reda 6 i da je, štoviše, takva ravnina “daleko” od postojanja, budući da ne postoje čak ni dva od nužnih pet ortogonalnih latinskih kvadrata reda 6. S druge strane, budući da projektivna ravnina reda n postoji za po volji velike vrijednosti n ako su oblika potencije prim-broja,

vidimo da time postoje i maksimalni sustavi ortogonalnih po volji “ogromnih” latinskih kvadrata. Spomenimo i uobičajenu oznaku $MOLS(n)$ za skup međusobno ortogonalnih latinskih kvadrata reda n . Prijeđimo na dokaz teorema, koji je konstruktivne prirode.

Dokaz. Najprije pretpostavimo da postoji projektivna ravnina $\mathcal{P}$ reda n . Izgradit ćemo sustav od $n - 1$ međusobno ortogonalnih latinskih kvadrata. Izaberimo bilo koji pravac ravnine i označimo ga s ℓ_∞ , pridajući mu ulogu “neizmjereno dalekog pravca” te bilo koje dvije točke na njemu označimo s R i S (za “retke” i “stupce” budućih latinskih kvadrata). Pravce kroz R i S , različite od ℓ_∞ , označimo s r_i , odnosno s_i , $i = 1, 2, \dots, n$. Sada svaka od n^2 točaka ravnine izvan ℓ_∞ ima jedinstveni prikaz kao sjecište nekih r_i i s_j . Označimo takvo sjecište s P_{ij} , shvaćajući točku ujedno kao poziciju (i, j) u kvadratnoj matrici L reda n . Sad prijeđimo na pravce kroz daljnje točke $P_1, P_2, \dots, P_{n-1}$ na ℓ_∞ . Skup od n pravaca kroz pojedinu P_i definirat će po jedan latinski kvadrat (u jeziku afine ravnine, svaka od tih paralelnih klasa definirat će latinski kvadrat). Uzmimo npr. P_1 i označimo pravce kroz tu točku, različite od ℓ_∞ , s $a_1, a_2, \dots, a_n$. Sada je npr. a_1 incidentan s n točaka P_{ij} i svake dvije od njih “nalaze se” u različitim retcima i različitim stupcima matrice L , budući da bi inače neke dvije od tih točaka bile spojene i pravcem r_i (ili s_j) i pravcem a_1 . Formiramo matricu L_1 tako da upišemo a_1 na svako mjesto gdje se nalazi točka incidentna s a_1 i analogno postupimo za $a_2, \dots, a_n$. Očito dobivamo latinski kvadrat L_1 , popunjen simbolima $a_1, a_2, \dots, a_n$. Treba se još uvjeriti da su bilo koja dva tako dobivena kvadrata ortogonalna. (Za $n = 2$ očito dobivamo jedan jedini latinski kvadrat, a za $n = 3$ dva kvadrata - za vježbu konstruirajte te kvadrate polazeći od po volji odabranog modela ravnine reda 3). Radi jednostavnijih oznaka, uzmimo latinske kvadrate L_1 i L_2 , popunjene simbolima $a_1, a_2, \dots, a_n$, odnosno $b_1, b_2, \dots, b_n$. Ako bi se npr. par (a_p, b_q) pojavio dvaput prilikom formiranja parova od simbola na odgovarajućim mjestima u L_1 i L_2 , recimo na mjestima (i, j) i (k, l) , to bi značilo da su točke P_{ij} i P_{kl} spojene različitim pravcima a_p i b_q , nemoguće. Dakle, polazeći od projektivne ravnine reda n doista možemo konstruirati maksimalni sustav latinskih kvadrata reda n .

Obrnuti smjer tvrdnje sada je gotovo očigledan. Uvedemo oznake za točke projektivne ravnine (odnosno, zasad, samo incidencijske strukture) po volji, pri čemu se možemo poslužiti oznakama iz prethodne konstrukcije (razlikovanje točaka na jednom odabranom pravcu ℓ_∞ i n^2 točaka P_{ij} izvan njega). Daljnje pravce, osim “očitih” koji imaju ulogu redaka i stupaca matrice $[P_{ij}]$, očitavamo iz raspoloživih latinskih kvadrata, tako da na pojedinu pravac, uz jednu točku s ℓ_∞ , svrstamo sve one točke iz pojedinog latinskog kvadrata na čijim pozicijama je upisan jedan te isti simbol (poput onih $a_i, b_j, \dots$ u prethodnoj konstrukciji). Inače, svaki skup od n pozicija latinskog kvadrata na kojima se nalazi isti simbol (i stoga se nalaze u različitim retcima i različitim stupcima) naziva se *transverzala* latinskog kvadrata.

Treba provjeriti da će tako dobivena incidencijska struktura doista biti projektivna ravnina reda n . Provjera (P1) netrivialna je samo za točke P_{ij} i P_{kl} s različitim i, k , odnosno j, l , a zapravo znači da postoji točno jedna transverzala (dakle, u točno jednom od latinskih kvadrata) koja prolazi pozicijama (i, j) i (k, l) . Zbog relacije ortogonalnosti jasno je da postoji najviše jedna takva transverzala, ali postojanje barem jedne nije izravno očigledno. To ćemo utvrditi “prebrojavanjem”, uočivši da je po konstrukciji svaka točka incidentna s $n + 1$ pravcem, a svaki pravac s $n + 1$ točkom. Zato se na pravcima kroz

bilo koju točku T nalazi svih ostalih $n(n+1) = n^2 + n$ točaka, a kako je spajanje točaka najviše jednostruko, T je spojena točno jednim pravcem s bilo kojom drugom točkom. Za (P2) moraju svaka dva pravca imati sjecište. To se opet lako vidi prebrojavanjem, ali i po konstrukciji, jer za latinske kvadrate znači da svake dvije transverzale različitih kvadrata imaju (bar jednu, a onda točno jednu) zajedničku poziciju u matrici. To je doista ispunjeno stoga što je svaka točka P_{ij} spojena sa svakom točkom na ℓ_∞ . $\square$

Primjer 8.8. *Konstruiramo maksimalni MOLS(4) (skup od tri međusobno ortogonalna latinska kvadrata reda 4). Polazimo od projektivne ravnine reda 4 i to cikličkog modela, u kojem je skup točaka $\mathbb{Z}_{21} = \{0, 1, 2, \dots, 20\}$, osnovni pravac je $l_0 = \{0, 1, 4, 14, 16\}$, a daljnji pravci su $l_i = \{x + i : x \in l_0\}$ (vidi primjer 6.8). Pravac l_0 će ujedno imati ulogu pravca ℓ_∞ , za točke R i S možemo uzeti npr. 0 i 1, dok će tri latinska kvadrata odgovarati pravcima kroz točke 4, 14 i 16. Najprije treba rasporediti 16 točaka na pravcima kroz R i S u kvadratnu matricu reda 4. Za to, kao i za daljnju konstrukciju, može biti praktično (iako nije neophodno) ispisati sve pravce ravnine. Retci i stupci mogu se popuniti npr. ovako, vodeći računa o kolinearnosti točaka na pravcima kroz točke $R = 0$ (retci) i $S = 1$ (stupci):*

$$\begin{bmatrix} 2 & 7 & 8 & 11 \\ 5 & 6 & 9 & 19 \\ 15 & 20 & 3 & 13 \\ 17 & 10 & 12 & 18 \end{bmatrix}.$$

Sada konstruiramo L_1 , upisujući redom a_1, a_2, a_3 i a_4 na mjesta u matrici koja odgovara točkama na pravcima kroz točku 4:

$$\begin{bmatrix} a_1 & a_3 & a_2 & a_4 \\ a_2 & a_4 & a_1 & a_3 \\ a_4 & a_2 & a_3 & a_1 \\ a_3 & a_1 & a_4 & a_2 \end{bmatrix}.$$

Analogno dobivamo preostala dva latinska kvadrata, pomoću pravaca kroz točke 14 i 16:

$$\begin{bmatrix} b_1 & b_4 & b_3 & b_2 \\ b_2 & b_3 & b_4 & b_1 \\ b_4 & b_1 & b_2 & b_3 \\ b_3 & b_2 & b_1 & b_4 \end{bmatrix}, \quad \begin{bmatrix} c_1 & c_2 & c_3 & c_4 \\ c_2 & c_1 & c_4 & c_3 \\ c_3 & c_4 & c_1 & c_2 \\ c_4 & c_3 & c_2 & c_1 \end{bmatrix}.$$

Lako se vidi da su svaka dva međusobno ortogonalna.

Primjer 8.9. *MOLS(4) iz prethodnog primjera možemo iskoristiti npr. za izvedbu sljedećeg eksperimenta. Treba testirati četiri automobila (a_1, a_2, a_3, a_4) i četiri vrste benzina (b_1, b_2, b_3, b_4) tako da bude testiran svaki par (a_i, b_j) . Na raspolaganju su četiri vozača (c_1, c_2, c_3, c_4), četiri vremenska termina (npr. od 9–10 h, 10–11 h itd.) i četiri rute. U istom terminu na pojedinoj ruti može se naći samo jedan automobil. Ako npr. stupcima matrica reda 4 pridružimo vremenske termine, a retcima pojedine rute, MOLS(4) može nam poslužiti kao plan testiranja u kojem su u svakom terminu aktivni svi vozači i u pogonu su svi automobili, a ispitane su sve kombinacije automobila i vrste benzina. Pritom, svaki vozač vozio je svaki automobil točno jedanput i na različitim rutama, dakako u različitim*

vremenskim terminima. Time su ostvareni ravnopravni uvjeti (premda, naravno, nije svaki vozač testirao svaku kombinaciju automobila i benzina na svakoj ruti, što bi bilo preskupo).

Primjer 8.10. Konstrukcija maksimalnog $MOLS(q)$ pomoću konačnog polja $GF(q)$. Neka je q potencija primbroja i $F = GF(q)$ polje od q elemenata (vidi poglavlje 5). Za svaki $a \in F$, $a \neq 0$, definiramo na F binarnu operaciju $x \cdot_a y = ax + y$ (sa zbrajanjem i množenjem iz F). Lako se provjeri da je $(F, \cdot_a)$ kvazigrupa pa je njezina Cayleyeva tablica latinski kvadrat. Imamo, dakle, $q - 1$ latinskih kvadrata popunjenih elementima polja F . Pokažimo da su kvadrati pridruženi operacijama za različite $a, b \in F$ međusobno ortogonalni. Kad ne bi bilo tako, za neke parove (x_1, y_1) i (x_2, y_2) s $x_1 \neq x_2$, $y_1 \neq y_2$, vrijedilo bi $ax_1 + y_1 = ax_2 + y_2$ i $bx_1 + y_1 = bx_2 + y_2$. Odatle slijedi $a = b = (y_2 - y_1)(x_1 - x_2)^{-1}$, proturječenje.

U ovoj konstrukciji očito nam svaki latinski kvadrat predstavlja jednu klasu paralelnih pravaca (s koeficijentom smjera a) afine ravnine $AG(2, q)$ nad poljem $GF(q)$. Iz teorema 8.7 (odnosno njegove varijante s afinom ravninom) imamo konstrukciju maksimalnog $MOLS(n)$ za bilo koju projektivnu (afinu) ravninu reda n , no ova za slučaj nad poljem je algebarski jednostavnija.

Poglavlje 9

Teorija kodiranja

9.1 Kodovi za ispravljanje pogrešaka

Teorija kodiranja bavi se problemom prijenosa informacija putem kanala sa šumom. Za razliku od kriptografije, u kojoj je cilj sakriti informacije od neovlaštenih primatelja, u teoriji kodiranja informacije se kodiraju na način koji omogućuje otkrivanje i ispravljanje pogrešaka nastalih pri prijenosu.

Primjer 9.1. *Svakoj knjizi dodjeljuje se takozvani ISBN kod (“International Standard Book Number”). Naprimjer, knjiga [11] ima kod 0-19-853803-0. Prva znamenka označava jezik (0 - engleski), druga grupa znamenaka označava izdavača (19 - Oxford University Press), iduća grupa je broj knjige kojeg dodjeljuje izdavač (853803 za knjigu [11]), a na kraju je kontrolna znamenka koja nam je ovdje najzanimljivija. Ako su $x_1, x_2, \dots, x_{10}$ znamenke ISBN koda, kontrolna znamenka x_{10} računa se¹ kao ostatak pri dijeljenju izraza $\sum_{i=1}^9 i x_i$ s 11. Ako je ostatak 10, za kontrolnu znamenku stavlja se X. Za knjigu [11] izraz je jednak 187. Rezultat je djeljiv s 11 pa je kontrolna znamenka 0.*

Kontrolna znamenka jednoznačno je određena s prethodnih 9 znamenaka i predstavlja redundanciju. To nam omogućuje otkrivanje pogrešaka koje nastaju promjenom jedne znamenke ili zamjenom dviju znamenaka ISBN koda. Ako se znamenka x_i promijeni u $x_i + a$, izraz će se promijeniti za $i \cdot a \not\equiv 0 \pmod{11}$. Slično, zamjena znamenaka x_i i x_j mijenja izraz za $(j - i) \cdot (x_i - x_j)$, što je djeljivo s 11 samo ako je $x_i = x_j$ (u tom slučaju zamjena nije promijenila ISBN kod).

Kontrolnu znamenku imaju i serijski brojevi novčanica, “poziv na broj” pri plaćanju računa i jedinstveni matični broj građanina (JMBG). Kontrolna znamenka omogućuje otkrivanje pogrešaka, ali ne omogućuje automatsko ispravljanje. Ako knjižničar u bazu podataka unese pogrešan ISBN kod, aplikacija ga može na to upozoriti. Knjižničar mora ponovo pogledati knjigu i “ručno” ispraviti pogrešku. U nekim situacijama to nije dovoljno, nego ispravljanje pogrešaka treba biti automatizirano.

Primjer 9.2. *Glazba se zapisuje na CD u obliku spirale. Laser očitava mikroskopske udubine i izbočine u CD-u koje odgovaraju nulama i jedinicama u digitaliziranoj snimci.*

¹Od 2007. godine umjesto 10-znamenkastog koristi se 13-znamenkasti ISBN kod. U njemu se kontrolna znamenka računa drugačije nego što je opisano u primjeru.

Zapis je iznimno gust, duljina spirale iznosi oko 5 kilometara. Najmanje ogrebotine na površini CD-a uzrokovale bi pogreške koje bi se čule pri reprodukciji glazbe. Zato se podaci kodiraju s takozvanim CIRC kodom ("Cross-interleaved Reed-Solomon Code"), koji može ispraviti do 4000 uzastopnih pogrešnih bitova. To odgovara ogrebotini od oko 2 milimetra u smjeru kružnice koncentrične s diskom. Ogrebotine u drugim smjerovima uništavaju podatke koji nisu uzastopni i na njih je sustav manje osjetljiv.

Sad ćemo formalno definirati kod za ispravljanje pogrešaka. Neka je Q konačan skup od q elemenata. Elemente zovemo *simbolima*, a skup Q *abecedom*. Uređene n -torke elemenata iz Q zovemo *vektorima*, iako je Q^n vektorski prostor samo u slučaju da je $Q = GF(q)$ konačno polje. Često se promatra upravo taj slučaj, ali jedina struktura nužna za ispravljanje pogrešaka je metrika na Q^n . *Hammingova*² *udaljenost* vektora $x = (x_1, \dots, x_n)$ i $y = (y_1, \dots, y_n)$ definira se kao broj koordinata na kojima se ti vektori razlikuju:

$$d(x, y) = |\{i \mid x_i \neq y_i\}|.$$

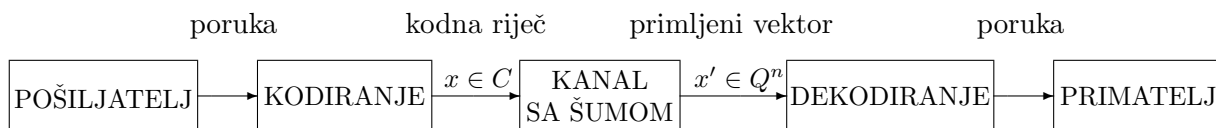
Naprimjer, za $Q = \{0, 1\}$ i $n = 4$, udaljenost vektora $x = 0110$ i $y = 1100$ je $d(x, y) = 2$.

Propozicija 9.3. *Hammingova udaljenost je metrika na skupu Q^n .*

Dokaz. Očito je $d(x, y) \geq 0$ i jednakost vrijedi ako i samo ako je $x = y$. Simetričnost $d(x, y) = d(y, x)$ je također očita. Treba provjeriti nejednakost trokuta $d(x, z) \leq d(x, y) + d(y, z)$. Udaljenosti vektora x i z doprinosi svaka koordinata i za koju je $x_i \neq z_i$. U tom slučaju sigurno je $x_i \neq y_i$ ili $y_i \neq z_i$, pa imamo doprinos i na desnoj strani (ako je $x_i \neq y_i$ i $y_i \neq z_i$, doprinos je 2). Prema tome, lijeva strana ne može biti veća od desne. $\square$

Definicija 9.4. Kod s parametrima (n, M, d, q) je podskup $C \subseteq Q^n$. Pritom je n duljina koda, $M = |C|$ je broj kodnih riječi, $d = \min\{d(x, y) \mid x, y \in C, x \neq y\}$ je minimalna udaljenost koda, a $q = |Q|$ je broj simbola.

Kodove nad abecedom veličine q zovemo q -arnim kodovima. U primjenama su najčešći *binarni kodovi*, nad abecedom $Q = \{0, 1\}$. Elementi koda (kodne riječi) predstavljaju moguće poruke. Pošiljatelj bira jednu od M poruka i šalje odgovarajuću kodnu riječ $x \in C$ putem kanala sa šumom. Zbog pogrešaka pri prijenosu primljeni vektor $x' \in Q^n$ može se razlikovati od poslana kodne riječi. Primateelj ga dekodira kao kodnu riječ $y \in C$ koja je najbliža primljenom vektoru x' u Hammingovoj metrici. Ako je $x = y$, kod je uspio ispraviti pogreške.



Propozicija 9.5. Kod C s parametrima (n, M, d, q) može otkriti bilo kojih $d - 1$ ili manje pogrešaka i ispraviti bilo kojih $e = \lfloor \frac{d-1}{2} \rfloor$ ili manje pogrešaka.

²Richard W. Hamming (1915.-1998.), američki matematičar.

Točnije, moguće je ustanoviti da je došlo do pogreške ako se poslana kodna riječ $x \in C$ i primljeni vektor $x' \in Q^n$ razlikuju na najviše $d - 1$ koordinata, a jednoznačno rekonstruirati x ako se razlikuju na najviše e koordinata.

Dokaz. Hammingova udaljenost poslane kodne riječi $x \in C$ i primljenog vektora $x' \in Q^n$ je manja od d , a udaljenost od x do bilo koje druge kodne riječi ne može biti manja od d . Prema tome, primljeni vektor x' je različit od svih kodnih riječi pa prepoznamo da je došlo do pogreške.

Sad pretpostavimo da je $d(x, x') \leq e$. Za bilo koju drugu kodnu riječ $y \in C$, $y \neq x$ vrijedi $d(x', y) > e$. U suprotnom bismo imali $d(x, y) \leq d(x, x') + d(x', y) \leq 2e \leq d - 1$, što je kontradikcija s pretpostavkom da je d minimalna udaljenost kodnih riječi. Dakle, x je najbliža kodna riječ primljenom vektoru x' pa je možemo jednoznačno dekodirati. $\square$

Primjer 9.6. Binarni kod $C = \{00 \dots 0, 11 \dots 1\}$ sastoji se od dvije kodne riječi duljine n . Minimalna udaljenost je $d = n$, a parametar $e = \lfloor \frac{n-1}{2} \rfloor$. To je takozvani kod ponavljanja u kojem otkrivanje i ispravljanje pogrešaka počiva na ponavljanju poruke (u ovom slučaju samo su dvije poruke, 0 i 1). Naprimjer, za $n = 5$ kod može otkriti bilo koje četiri pogreške i ispraviti bilo koje dvije pogreške.

U praksi se koriste sofisticiraniji kodovi od ovog. Dobar (n, M, d, q) kod treba imati:

- što manju duljinu vektora n (da komunikacija bude brža),
- što veći broj kodnih riječi M (da možemo prenijeti više poruka),
- što veću minimalnu udaljenost d (da možemo otkriti i ispraviti više pogrešaka).

Zahtjevi su međusobno kontradiktorni, o čemu preciznije govore sljedeće nejednakosti. Nazivamo ih *ocjenama* na parametre koda.

Propozicija 9.7 (Singletonova³ ocjena). *Ako postoji (n, M, d, q) kod C , onda vrijedi*

$$M \leq q^{n-d+1}.$$

Dokaz. Definiramo funkciju $f : C \rightarrow Q^{n-d+1}$, $f(x_1, \dots, x_n) = (x_1, \dots, x_{n-d+1})$ (uklanjanje zadnjih $d - 1$ koordinata). Kodne riječi se razlikuju na bar d koordinata, pa je f injekcija. Prema tome, broj elemenata domene $M = |C|$ je manji ili jednak od broja elemenata kodomene $|Q^{n-d+1}| = q^{n-d+1}$. $\square$

Kodove koji dostižu Singletonovu ocjenu zovemo *MDS kodovima*, prema engleskom nazivu “maximum distance separable”. Vidjet ćemo da su povezani s ortogonalnim latin-skim kvadratima.

Propozicija 9.8 (Ocjena pakiranja kugli⁴). *Ako postoji (n, M, d, q) kod C i ako je $e = \lfloor \frac{d-1}{2} \rfloor$, onda vrijedi*

$$M \leq \frac{q^n}{\sum_{i=0}^e \binom{n}{i} (q-1)^i}.$$

³Richard C. Singleton (1928.-2007.), američki matematičar i statističar.

⁴Eng. *sphere packing bound*.

Dokaz. Promotrimo zatvorene kugle polumjera e u metričkom prostoru Q^n s Hammingovom metrikom: $K(x, e) = \{y \in Q^n \mid d(x, y) \leq e\}$. Broj vektora udaljenih od x za i je $\binom{n}{i}(q-1)^i$, pa svaka kugla sadrži $\sum_{i=0}^e \binom{n}{i}(q-1)^i$ vektora. Kugle sa središtima u kodnim riječima $x \in C$ su međusobno disjunktne (u suprotnom bi kodne riječi bile udaljene manje od d). Zato broj kodnih riječi pomnožen s brojem vektora u kugli ne može biti veći od ukupnog broja vektora, $M \cdot \sum_{i=0}^e \binom{n}{i}(q-1)^i \leq q^n$. $\square$

Kodove koji dostižu ocjenu pakiranja kugli nazivamo *savršenim kodovima*. U njima je cijeli prostor Q^n pokriven kuglama polumjera e sa središtima u kodnim riječima, tj. bilo koji primljeni vektor jednoznačno određuje kodnu riječ udaljenu najviše za e . Vidjet ćemo da su savršeni kodovi povezani s dizajnima. Zadnja ocjena koju spominjemo odnosi se na binarne kodove s velikom minimalnom udaljenosti.

Propozicija 9.9 (Plotkinova ocjena). *Ako postoji binarni $(n, M, d, 2)$ kod C s $d > \frac{n}{2}$, onda vrijedi*

$$M \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor.$$

Dokaz. Neka je $C = \{x_1, \dots, x_M\}$ i neka je A matrica dimenzija $M \times n$ kojoj su reci kodne riječi $x_1, \dots, x_M$. Označimo sa $S = \sum_{i=1}^M \sum_{j=1}^M d(x_i, x_j)$ sumu svih udaljenosti kodnih riječi. Za $i \neq j$ članovi sume su veći ili jednaki od d , pa je $S \geq M(M-1)d$. Neka je t_k broj jedinica i $M - t_k$ broj nula u k -tom stupcu matrice A . Svaki par jedinice i nule doprinosi 2 u sumi S , jer udaljenosti računamo u oba redoslijeda. Stoga je $S = \sum_{k=1}^n 2t_k(M - t_k)$. Dobili smo nejednakost $M(M-1)d \leq \sum_{k=1}^n 2t_k(M - t_k)$. Ocijenit ćemo njezinu desnu stranu posebno za parni i za neparni M .

Funkcija $t \mapsto t(M-t)$ postiže maksimum $\frac{M^2}{4}$ za $t = \frac{M}{2}$. Zato je suma na desnoj strani manja ili jednaka od $2n \cdot \frac{M^2}{4} = \frac{nM^2}{2}$. Sređivanjem dobivamo $(2d-n)M \leq 2d$. Zbog $d > \frac{n}{2}$ smijemo dijeliti s $2(2d-n) > 0$ i tako dobivamo $\frac{M}{2} \leq \frac{d}{2d-n}$. Za parni M je $\frac{M}{2} = \lfloor \frac{M}{2} \rfloor \leq \lfloor \frac{d}{2d-n} \rfloor$ i time je dokazana Plotkinova ocjena.

Za neparni M funkcija $t \mapsto t(M-t)$, $t \in \mathbb{N}$ postiže maksimum za $t = \frac{M-1}{2}$ i $t = \frac{M+1}{2}$. Maksimum iznosi $\frac{M-1}{2} \cdot \frac{M+1}{2} = \frac{M^2-1}{4}$, pa slično kao ranije dobivamo $M(M-1)d \leq \frac{n(M^2-1)}{2}$. Sređivanjem slijedi $(2d-n)M \leq n$, tj. $M \leq \lfloor \frac{n}{2d-n} \rfloor \leq \lfloor \frac{2d}{2d-n} \rfloor - 1$ (zadnja nejednakost slijedi iz $n < 2d$). Budući da za svaki $\varepsilon > 0$ vrijedi $\lfloor 2\varepsilon \rfloor \leq 2\lfloor \varepsilon \rfloor + 1$, ponovo smo dobili Plotkinovu ocjenu $M \leq 2 \lfloor \frac{d}{2d-n} \rfloor$. $\square$

Kodovi koji dostižu Plotkinovu ocjenu povezani su s Hadamardovim matricama, što ćemo vidjeti u cjelini 9.3.

9.2 Linearni kodovi

Ako je q prim potencija, skup simbola Q možemo snabdjeti strukturom konačnog polja $GF(q)$. Tada je Q^n vektorski prostor nad $GF(q)$. Ranije smo kod definirali kao bilo koji podskup $C \subseteq Q^n$. Sad ćemo se ograničiti na potprostore vektorskog prostora. To je važan specijalni slučaj u kojem imamo jednostavne algoritme za kodiranje i dekodiranje.

Definicija 9.10. Linearni kod s parametrima $[n, m, d, q]$ je m -dimenzionalni potprostor $C \leq Q^n$ n -dimenzionalnog vektorskog prostora nad poljem $Q = GF(q)$. Pritom je $d = \min\{d(x, y) \mid x, y \in C, x \neq y\}$ minimalna udaljenost koda.

Za općenite kodove drugi parametar označava broj kodnih riječi $M = |C|$, a za linearne kodove dimenziju m potprostora C . Veza je $M = q^m$. Da naglasimo razliku, parametre linearnih kodova pišemo u uglatim zagradama. Ako je kod linearan, umjesto minimalne udaljenosti možemo gledati minimalnu težinu vektora.

Definicija 9.11. Težina vektora $x = (x_1, \dots, x_n) \in Q^n$ je broj koordinata različitih od nule: $w(x) = |\{i \mid x_i \neq 0\}|$. Minimalna težina koda $C \subseteq Q^n$ je broj $\min\{w(x) \mid x \in C, x \neq 0\}$.

Propozicija 9.12. Za linearne kodove minimalna težina jednaka je minimalnoj udaljenosti koda.

Dokaz. Označimo minimalnu težinu koda C s $w(C)$, a minimalnu udaljenost s $d(C)$. Za proizvoljne vektore $x, y \in Q^n$ očito vrijedi $d(x, y) = w(x - y)$. Ako je C linearan, onda iz $x, y \in C$ slijedi $x - y \in C$. Vidimo da se udaljenost kodnih riječi x i y postiže kao težina kodne riječi $x - y$, pa je $w(C) \leq d(C)$. Obrnuto, zbog linearnosti je $0 \in C$, pa se težina kodne riječi $x \in C$ postiže kao udaljenost $d(x, 0) = w(x)$ i vrijedi $w(C) \geq d(C)$. Dakle, vrijedi jednakost $w(C) = d(C)$. $\square$

Da bismo po definiciji izračunali minimalnu udaljenost koda s M vektora, $\binom{M}{2}$ puta računamo udaljenost vektora. Za linearne kodove računamo samo $M - 1$ težina vektora različitih od nulvektora. Još jedna prednost linearnih kodova je efikasnije zadavanje. Opći kod zadajemo navođenjem svih M kodnih riječi, a linearni kod navođenjem baze koja se sastoji od $m = \log_q M$ vektora.

Definicija 9.13. Generirajuća matrica linearnog $[n, m, d, q]$ koda C je $m \times n$ matrica G kojoj reci čine bazu za C . Kažemo da je G u standardnom obliku ako je oblika $G = [I_m \mid A]$, gdje je I_m jedinična matrica, a A neka $m \times (n - m)$ matrica nad $GF(q)$.

Linearni $[n, m, d, q]$ kod omogućuje kodiranje $M = q^m$ poruka, koje možemo identificirati s vektorima iz Q^m . Kodiranje je tada injektivna funkcija $Q^m \rightarrow Q^n$ kojoj je slika kod C . Ako je kod zadan generirajućom matricom G , ta funkcija je jednostavno množenje vektora $u \in Q^m$ s matricom G zdesna: $u \mapsto u \cdot G$. Riječ je o injektivnom linearnom operatoru (monomorfizmu vektorskih prostora) kojem je slika potprostor $C \leq Q^n$.

Kodiranje je posebno jednostavno ako je generirajuća matrica $G = [I_m \mid A]$ u standardnom obliku. Tada su reci sigurno linearno nezavisni, bez obzira što uzmemo za matricu $A = [\alpha_{ij}]$. Poruka $u = (u_1, \dots, u_m) \in Q^m$ kodira se kao $u \cdot G = x = (x_1, \dots, x_n)$, pri čemu je $x_i = u_i$ za $i = 1, \dots, m$ i $x_{m+j} = \sum_{i=1}^m \alpha_{ij} u_i$ za $j = 1, \dots, n - m$. Dakle, prvih m koordinata podudara se s porukom, a zadnjih $n - m$ koordinata su “kontrolne znamenke” koje omogućuju otkrivanje i ispravljanje pogrešaka.

Primjer 9.14. Promotrimo binarni linearni kod duljine $n = 7$ i dimenzije $m = 4$ zadan generirajućom matricom u standardnom obliku:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Poruke su $M = 2^4 = 16$ binarnih vektora duljine četiri; možemo ih identificirati s heksadecimalnim znamenkama. Odgovarajuće kodne riječi dobivamo množenjem poruka s G :

$0 \rightarrow 0000\ 000$	$4 \rightarrow 0100\ 101$	$8 \rightarrow 1000\ 110$	$C \rightarrow 1100\ 011$
$1 \rightarrow 0001\ 111$	$5 \rightarrow 0101\ 010$	$9 \rightarrow 1001\ 001$	$D \rightarrow 1101\ 100$
$2 \rightarrow 0010\ 011$	$6 \rightarrow 0110\ 110$	$A \rightarrow 1010\ 101$	$E \rightarrow 1110\ 000$
$3 \rightarrow 0011\ 100$	$7 \rightarrow 0111\ 001$	$B \rightarrow 1011\ 010$	$F \rightarrow 1111\ 111$

Prve četiri koordinate odgovaraju binarnom prikazu heksadecimalnih brojeva (to su vektori koje smo množili s G), a zadnje tri koordinate su kontrolne znamenke. Ako nije došlo do pogreške pri prijenosu, dekodiranje se svodi na odbacivanje zadnjeg dijela. Minimalna težina nenul kodnih riječi je 3, što znači da kod može otkriti dvije i ispraviti jednu pogrešku.

Postavlja se pitanje možemo li svaki linearni kod zadati generirajućom matricom u standardnom obliku. To nas dovodi do pojma ekvivalencije kodova. Svi m -dimenzionalni potprostori n -dimenzionalnog vektorskog prostora međusobno su izomorfni kao vektorski prostori. Međutim, nisu svi ekvivalentni sa stanovišta teorije kodiranja jer nemaju istu minimalnu težinu, odnosno minimalnu udaljenost. Ekvivalencija općih (ne nužno linearnih) kodova definira se na sljedeći način.

Definicija 9.15. Za kodove $C_1, C_2 \subseteq Q^n$ kažemo da su ekvivalentni ako se kodne riječi od C_2 mogu dobiti iz kodnih riječi od C_1 permutiranjem koordinata i permutiranjem simbola na pojedinim koordinatama (operacije primjenjujemo istovremeno na svim kodnim riječima od C_1).

Ako kodne riječi od C_1 zapišemo u $M \times n$ matricu, prva operacija odgovara permutiranju stupaca te matrice, a druga operacija permutiranju simbola u pojedinim stupcima. Redoslijed u kojem su napisani reci smatramo nevažnim jer kodove shvaćamo kao skupove vektora. Operacije očito ne mijenjaju udaljenost među vektorima (primjenjujemo ih na oba vektora čiju udaljenost računamo), pa za ekvivalentne kodove vrijedi $d(C_1) = d(C_2)$. Relacija iz definicije 9.15 očito je relacija ekvivalencije na skupu svih kodova.

Linearni kod može biti ekvivalentan kodu koji nije linearan. Permutiranje koordinata ne kvari linearnost, ali permutiranje simbola na nekoj od koordinata može pokvariti linearnost (npr. možemo izbaciti nulvektor iz koda). Želimo finiju relaciju ekvivalencije koja ne kvari linearnost.

Definicija 9.16. Za linearne kodove $C_1, C_2 \leq Q^n$ kažemo da su ekvivalentni ako se kodne riječi od C_2 mogu dobiti iz kodnih riječi od C_1 permutiranjem koordinata i množenjem elemenata na pojedinim koordinatama skalarima $\alpha \in GF(q)$, $\alpha \neq 0$.

Množenje skalarom $\alpha \neq 0$ je specijalni slučaj permutiranja simbola koji ne kvari linearnost. Sljedeća propozicija govori kako ekvivalentne linearne kodove prepoznamo preko njihovih generirajućih matrica.

Propozicija 9.17. *Dvije $m \times n$ matrice nad $GF(q)$ generiraju ekvivalentne linearne kodove ako i samo ako se jedna može dobiti od druge*

1. *permutiranjem stupaca,*
2. *množenjem stupaca skalarima $\alpha \neq 0$,*
3. *elementarnim transformacijama nad recima.*

Dokaz. Elementarne transformacije nad recima matrice ne mijenjaju potprostor razapet recima. Operacije 1. i 2. odgovaraju permutiranju koordinata i množenju koordinata skalarima, kao u definiciji 9.16. $\square$

Sada možemo odgovoriti na pitanje o zadavanju kodova generirajućim matricama u standardnom obliku.

Korolar 9.18. *Svaki linearni kod ekvivalentan je linearnom kodu zadanom generirajućom matricom u standardnom obliku.*

Dokaz. Operacijama 1., 2. i 3. iz prethodne propozicije bilo koju $m \times n$ matricu ranga m možemo svesti na oblik $[I_m \mid A]$. $\square$

Nad recima generirajuće matrice smijemo raditi sve tri vrste elementarnih transformacija, a nad stupcima samo dvije (permutiranje i množenje skalarom različitim od nule). Kad bismo dozvolili još i zbrajanje stupaca, svaku matricu mogli bismo svesti na oblik $[I_m \mid 0]$, kao kod računanja ranga matrice. Tada bismo dobili relaciju ekvivalencije koja odgovara izomorfizmu vektorskih prostora.

Sad ćemo se baviti problemom otkrivanja i ispravljanja pogrešaka s pomoću linearnih kodova. Treba nam operacija množenja vektora iz Q^n .

Definicija 9.19. *Neka je $Q = GF(q)$. Produkt vektora $x = (x_1, \dots, x_n)$ i $y = (y_1, \dots, y_n)$ iz Q^n je skalar $x \cdot y = \sum_{i=1}^n x_i y_i$. Kažemo da su x i y ortogonalni ako je $x \cdot y = 0$.*

Produkt ima slična svojstva kao skalarni produkt na realnom vektorskom prostoru: simetričnost $x \cdot y = y \cdot x$, $\forall x, y \in Q^n$ i bilinearnost $(\alpha x + \beta y) \cdot z = \alpha(x \cdot z) + \beta(y \cdot z)$, $\forall x, y, z \in Q^n$, $\alpha, \beta \in Q$. Svojstvo pozitivnosti nema smisla jer u konačnom polju nemamo uređaj. Osim toga produkt vektora sa samim sobom može biti nula i za vektore različite od nulvektora. Naprimjer, za $x = (1, 1) \in GF(2)^2$ je $x \cdot x = 0$.

Definicija 9.20. *Dualni kod od $C \leq Q^n$ je kod $C^\perp = \{x \in Q^n \mid x \cdot y = 0, \forall y \in C\}$.*

Propozicija 9.21. *Ako je $\dim C = m$, onda je $C^\perp$ linearni kod dimenzije $n - m$.*

Dokaz. Neka su $g_1, \dots, g_m$ reci generirajuće matrice, tj. neka čine bazu koda C . Za vektor $x \in Q^n$ vrijedi $x \in C^\perp$ ako i samo ako je $x \cdot g_i = 0$, za $i = 1, \dots, m$. Nužnost je očita jer vektori $g_1, \dots, g_m$ pripadaju kodu C . Za dovoljnost primijetimo da se svaki vektor $y \in C$ može napisati kao linearna kombinacija $y = \sum_{i=1}^m \alpha_i g_i$. Ako je $x \in Q^n$ ortogonalan na $g_1, \dots, g_m$, onda vrijedi $x \cdot y = x \cdot (\sum_{i=1}^m \alpha_i g_i) = \sum_{i=1}^m \alpha_i (x \cdot g_i) = 0$, pa je ortogonalan i na y . Prema tome, $C^\perp$ je skup rješenja sustava homogenih linearnih jednadžbi $x \cdot g_i = 0$, $i = 1, \dots, m$. Riječ je o potprostoru dimenzije $n - m$ jer su vektori $g_1, \dots, g_m$ linearno nezavisni. $\square$

Usprkos tome što je $\dim C + \dim C^\perp = n$, dualni kod ne mora biti ortogonalni komplement od C . Presjek $C \cap C^\perp$ nije uvijek trivijalan, a suma $C + C^\perp$ može biti pravi potprostor od Q^n .

Propozicija 9.22. *Za svaki linearni kod $C \leq Q^n$ vrijedi $(C^\perp)^\perp = C$.*

Dokaz. Inkluzija $C \subseteq (C^\perp)^\perp$ slijedi direktno iz definicije 9.20. Po propoziciji 9.21 to su potprostori iste dimenzije m , pa vrijedi jednakost. $\square$

Definicija 9.23. Matrica provjere parnosti⁵ koda $C \leq Q^n$ je generirajuća matrica dualnog koda $C^\perp$.

Ako je C kod duljine n i dimenzije m , njegova generirajuća matrica G je tipa $m \times n$. Dualni kod je duljine n i dimenzije $n - m$, pa je matrica provjere parnosti P tipa $(n - m) \times n$. Uz pomoć matrice P možemo provjeriti pripada li primljeni vektor kodu, tj. jesu li pri prijenosu nastale pogreške.

Propozicija 9.24. *Neka je P matrica provjere parnosti koda C . Vektor $x \in Q^n$ pripada kodu C ako i samo ako je $x \cdot P^\tau = 0$.*

Dokaz. Relacija $x \cdot P^\tau = 0$ znači da je vektor x ortogonalan na retke matrice P . To je ekvivalentno s ortogonalnošću od x na sve vektore iz potprostora razapetog recima, tj. na sve vektore dualnog koda $C^\perp$. Po definiciji 9.20 vektor x pripada dualu duala $(C^\perp)^\perp$, a on je po propoziciji 9.22 jednak C . $\square$

Ako je kod zadan generirajućom matricom u standardnom obliku, lako je napisati njegovu matricu provjere parnosti.

Propozicija 9.25. *Neka je $G = [I_m \mid A]$ generirajuća matrica koda C . Tada je $P = [-A^\tau \mid I_{n-m}]$ matrica provjere parnosti tog koda.*

Dokaz. Vrijedi

$$G \cdot P^\tau = \begin{bmatrix} I_m & A \end{bmatrix} \cdot \begin{bmatrix} -A \\ I_{n-m} \end{bmatrix} = -A + A = 0.$$

To znači da su reci matrice P ortogonalni na retke od G , pa razapinju potprostor od $C^\perp$. Po propoziciji 9.21 je $\dim C^\perp = n - m$, a reci od P očito razapinju $n - m$ dimenzionalni potprostor. Zato razapinju cijeli $C^\perp$ i P je matrica provjere parnosti od C . $\square$

⁵Eng. *parity check matrix*.

Primjer 9.26. Matrica provjere parnosti $[7, 4, 3, 2]$ koda iz primjera 9.14 je

$$P = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Primijetimo da u polju $GF(2)$ vrijedi $-1 = 1$, pa je $-A^\tau = A^\tau$.

Osim za otkrivanje pogrešaka, matrica provjere parnosti služi i za ispravljanje pogrešaka nastalih pri prijenosu kodnih riječi. Vektorski prostor Q^n prikazuje se kao disjunktna unija linearnih mnogostrukosti “paralelnih” s potprostorom C . Linearne mnogostrukosti su oblika $a + C$, svaka sadrži q^m vektora i ima ih q^{n-m} . Priljeni vektor $x' \in Q^n$ pripada točno jednoj od linearnih mnogostrukosti; možemo je identificirati s pomoću takozvanog sindroma.

Definicija 9.27. Neka je $C \leq Q^n$ linearni kod s matricom provjere parnosti P . Sindrom vektora $x \in Q^n$ je vektor $S(x) = x \cdot P^\tau \in Q^{n-m}$.

Po propoziciji 9.24, vektor x pripada kodu C ako i samo ako je njegov sindrom nul-vektor.

Propozicija 9.28. Vektori $x, y \in Q^n$ pripadaju istoj linearnoj mnogostrukosti ako i samo ako je $S(x) = S(y)$.

Dokaz. Vrijedi $x + C = y + C \iff x - y \in C \iff (x - y)P^\tau = 0 \iff xP^\tau = yP^\tau \iff S(x) = S(y)$. $\square$

Neka je $s = q^{n-m}$ i neka su $a_1, \dots, a_s$ predstavnici minimalnih težina iz linearnih mnogostrukosti paralelnih s potprostorom C . To znači da je $Q^n = (a_1 + C) \cup \dots \cup (a_s + C)$ (disjunktna unija) i da je a_i vektor minimalne težine iz skupa $a_i + C$. Neka priljeni vektor $x' \in Q^n$ pripada mnogostrukosti $a_i + C$. Tvrdimo da je tada $y = x' - a_i \in C$ kodna riječ najmanje udaljena od x' . To slijedi iz $d(x', y) = w(x' - y) = w(a_i)$ i iz činjenice da je a_i izabran kao predstavnik minimalne težine. Prema tome, x' dekodiramo kao $y = x' - a_i$. Algoritam za dekodiranje izračunava sindrom priljenog vektora $S(x')$, traži vektor iz $\{a_1, \dots, a_s\}$ za koji je $S(a_i) = S(x')$ i dekodira x' kao $x' - a_i$.

Vidimo da su vektori pogrešaka koje kod C ispravlja upravo predstavnici minimalnih težina iz linearnih mnogostrukosti paralelnih s C . Budući da kod ispravlja bilo kojih $e = \lfloor \frac{d-1}{2} \rfloor$ pogrešaka, zaključujemo da se među predstavnicima nalaze svi vektori težine manje ili jednake od e .

Iduća propozicija povezuje minimalnu težinu koda s matricom provjere parnosti P .

Propozicija 9.29. Neka je C linearni kod s matricom provjere parnosti P . Minimalna težina od C jednaka je minimalnom broju linearno zavisnih stupaca od P . Točnije, vrijedi $w(C) = d$ ako i samo ako u P postoji d linearno zavisnih stupaca, a bilo kojih $d - 1$ ili manje stupaca su linearno nezavisni.

Dokaz. Neka su $P_1, \dots, P_n$ stupci matrice P i $x = (x_1, \dots, x_n) \in Q^n$. Znamo da je $x \in C$ ako i samo ako je $x \cdot P^\tau = 0$, što možemo zapisati kao $x_1 P_1 + \dots + x_n P_n = 0$. Ako je $x \in C$

kodna riječ minimalne težine $d = w(x)$, onda imamo d linearno zavisnih stupaca od P (koji odgovaraju nenul komponentama od x). Zato je minimalni broj linearno zavisnih stupaca manji ili jednak od minimalne težine $w(C)$.

Obrnuto, neka je d minimalni broj linearno zavisnih stupaca od P . Tada postoje indeksi $i_1, \dots, i_d$ i skalari $x_{i_1}, \dots, x_{i_d} \in Q$ takvi da je $x_{i_1}P_{i_1} + \dots + x_{i_d}P_{i_d} = 0$. Vektor $x = (0, \dots, 0, x_{i_1}, 0, \dots, 0, x_{i_d}, 0, \dots, 0)$ je težine d i zadovoljava $x \cdot P^T = 0$, pa pripada kodu C . Dakle, minimalna težina koda manja je ili jednaka od minimalnog broja linearno zavisnih stupaca od P . Time je dokazana jednakost. $\square$

Ova propozicija daje nam ideju kako s pomoću matrice provjere parnosti definirati klasu linearnih kodova minimalne težine 3. Kao stupce od P uzimamo po jedan vektor iz svakog jednodimenzionalnog potprostora vektorskog prostora Q^r nad poljem $Q = GF(q) = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$ (prvo smo napisali elemente $\alpha_0 = 0$ i $\alpha_1 = 1$). Možemo uzeti “normalizirane” vektore, tj. vektore kojima je vodeća nenul koordinata jednaka 1. Svaka dva takva vektora su linearno nezavisna, pa je minimalni broj linearno zavisnih stupaca u sljedećoj matrici jednak tri:

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 1 & 1 & \cdots & 1 & \cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ 1 & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} & \cdots & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} \end{bmatrix}. \quad (9.1)$$

Prvi stupac ima vodeću jedinicu na zadnjoj (r -toj) koordinati, idućih q stupaca na koordinati $r - 1$ (predzadnjoj), idućih q^2 stupaca na koordinati $r - 2$ i tako dalje. Zadnjih q^{r-1} stupaca imaju vodeću jedinicu na prvoj koordinati. Matrica P ima r redaka i $1 + q + q^2 + q^{r-1} = \frac{q^r - 1}{q - 1}$ stupaca.

Definicija 9.30. *Linearni kod definiran matricom provjere parnosti (9.1) zovemo q -arnim Hammingovim kodom s parametrom r i označavamo $\text{Ham}(r, q)$.*

Propozicija 9.31. *Parametri Hammingova koda $\text{Ham}(r, q)$ su $\left[\frac{q^r - 1}{q - 1}, \frac{q^r - 1}{q - 1} - r, 3, q\right]$.*

Dokaz. Duljina koda $n = \frac{q^r - 1}{q - 1}$ odgovara broju stupaca matrice P . Recimo matrice P su linearno nezavisni, pa je dualni kod $\text{Ham}(r, q)^\perp$ dimenzije r . Po propoziciji 9.21 dimenzija od $\text{Ham}(r, q)$ je $m = n - r = \frac{q^r - 1}{q - 1} - r$. Matricu P smo definirali tako da svaka dva stupca budu linearno nezavisna, pa je po propoziciji 9.29 minimalna težina Hammingova koda 3. Konačno, zadnji parametar je q jer je $\text{Ham}(r, q)$ definiran nad poljem $GF(q)$. $\square$

Kod $\text{Ham}(3, 2)$ ima parametre $[7, 4, 3, 2]$ i ekvivalentan je kodu iz primjera 9.14. Općenito, svi Hammingovi kodovi imaju minimalnu težinu 3, otkrivaju dvije pogreške i ispravljaju jednu pogrešku. Hammingovi kodovi su savršeni.

Propozicija 9.32. *$\text{Ham}(r, q)$ je savršen kod, tj. postiže jednakost u ocjeni pakiranja kugli (propoziciji 9.8).*

Dokaz. Treba vidjeti da vrijedi $M \cdot \sum_{i=0}^e \binom{n}{i} (q - 1)^i = q^n$. Parametri Hammingova koda su $M = q^m$, $m = n - r$, $n = \frac{q^r - 1}{q - 1}$, $e = 1$ pa je jednakost ekvivalentna s $1 + \binom{n}{1} (q - 1) = q^{n-m} \iff 1 + \frac{q^r - 1}{q - 1} (q - 1) = q^r$. Zadnja jednakost očito vrijedi. $\square$

9.3 Veze kodova i drugih konačnih struktura

Najavili smo da su savršeni kodovi povezani s dizajnima. Blokove dizajna dobivamo kao nosače kodnih riječi minimalne težine. Nosač vektora $x = (x_1, \dots, x_n) \in Q^n$ je skup $\text{supp } x = \{i \mid x_i \neq 0\}$. Težina $w(x)$ jednaka je kardinalnom broj nosača $\text{supp } x$.

Teorem 9.33. *Neka je C linearni $[n, m, d, q]$ kod i $d = 2e + 1$. Ako je C savršen, onda nosači kodnih riječi minimalne težine čine $(e + 1)$ -($n, d, (q - 1)^e$) dizajn.*

Dokaz. Točke dizajna su brojevi $\{1, \dots, n\}$ kojima su indeksirane koordinate koda. Blokovi su nosači kodnih riječi minimalne težine i svi su veličine d . Uzmimo proizvoljni $(e + 1)$ -člani skup točaka i neka je $x \in Q^n$ bilo koji vektor kojemu je taj skup nosač. Takvih vektora ima $(q - 1)^{e+1}$. Budući da je kod savršen, postoji jedinstvena kodna riječ $y \in C$ takva da je $d(x, y) \leq e$. Udaljenost nulvektora od x je $d(x, 0) = e + 1$, pa je $y \neq 0$ i $w(y) \geq d = 2e + 1$. Vektor x ima samo $e + 1$ koordinata različitih od nule, a y barem $2e + 1$; zato je $d(x, y) = e$ i $w(y) = d$. Dakle, y je kodna riječ minimalne težine koja se podudara s x na svim nenul koordinatama, iz čega slijedi $\text{supp } x \subseteq \text{supp } y$. Pokazali smo da za bilo koji $(e + 1)$ -člani skup indeksa postoji $(q - 1)^{e+1}$ kodnih riječi minimalne težine čiji nosači sadrže taj skup. Množenje s nenul skalarom ne mijenja nosač vektora, pa različitih nosača ima $q - 1$ puta manje. Time smo dokazali da nosači čine $(e + 1)$ -dizajn s parametrom $\lambda = (q - 1)^e$. $\square$

Ovaj teorem dokazali su Assmus i Mattson [1]. Kasnije su dokazali općenitiji dovoljan uvjet da bi nosači vektora fiksne težine k činili dizajn, koji vrijedi i za nesavršene kodove [2]. Iz teorema slijedi da nosači vektora težine 3 u binarnom Hammingovom kodu $\text{Ham}(r, 2)$ čine dizajn s parametrima 2 -($2^r - 1, 3, 1$) (Steinerov sustav trojki).

Primjer 9.34. *U primjeru 9.14 navedene su kodne riječi $[7, 4, 3, 2]$ koda ekvivalentnog s Hammingovim kodom $\text{Ham}(3, 2)$. Riječi minimalne težine odgovaraju porukama 2, 3, 4, 5, 8, 9, E i njihovi su nosači redom $\{3, 6, 7\}$, $\{3, 4, 5\}$, $\{2, 5, 7\}$, $\{2, 4, 6\}$, $\{1, 5, 6\}$, $\{1, 4, 7\}$, $\{1, 2, 3\}$. To su blokovi 2 -($7, 3, 1$) dizajna, tj. Fanove ravnine.*

Postavlja se pitanje postoje li drugi savršeni kodovi osim Hammingovih? Trivijalni primjeri su jednočlani skup $C = \{00 \dots 0\}$ (kugla oko jedine kodne riječi polumjera n pokriva Q^n) i cijeli prostor $C = Q^n$ (kugle polumjera 0 pokrivaju Q^n). Binarni kod n -terostrukog ponavljanja $C = \{00 \dots 0, 11 \dots 1\}$ s neparnim n također je savršen. Za njega je $d = n = 2e + 1$ i kugle polumjera e sadrže $\sum_{i=0}^e \binom{n}{i} = 2^{n-1}$ vektora. Kugle oko dvije kodne riječi su disjunktne i pokrivaju svih 2^n vektora.

U članku [10] od samo jedne stranice, M. Golay⁶ dao je generirajuće matrice savršenog binarnog koda G_{23} s parametrima $[23, 12, 7, 2]$ i savršenog ternarnog koda G_{11} s parametrima $[11, 6, 5, 3]$. U istom radu generalizirao je binarne Hammingove kodove na q -arne i postavio hipotezu da su to jedini netrivialni savršeni kodovi.

Golayevi kodovi povezani su s Wittovim dizajnima. Binarni Golayev kod ispravlja $e = 3$ pogrešaka. Prema teoremu 9.33, nosači vektora težine 7 u G_{23} čine 4 -($23, 7, 1$) dizajn. To je derivirani dizajn velikog Wittovog 5 -($24, 8, 1$) dizajna iz zadatka 3.5. Alternativno, možemo proširiti G_{23} sa znamenkom $x_{24} = \sum_{i=1}^{23} x_i \pmod{2}$ i dobiti kod G_{24}

⁶Marcel J.E. Golay (1902.-1989.), švicarski matematičar i fizičar.

s parametrima $[24, 12, 8, 2]^7$. Nosači vektora težine 8 u tom kodu čine 5-(24, 8, 1) dizajn. Ternarni Golayev kod G_{11} ispravlja $e = 2$ pogrešaka i nosači vektora težine 5 čine 3-(11, 5, 4) dizajn. Pokazuje se da je to zapravo 4-(11, 5, 1) dizajn, derivirani dizajn malog Wittovog 5-(12, 6, 1) dizajna iz primjera 3.17. Godine 1973. J.H. van Lint i A. Tietäväinen dokazali su sljedeći teorem.

Teorem 9.35. *Ako je q prim potencija, svaki netrivialni savršeni q -arni kod ima parametre kao jedan od Hammingovih ili Golayevih kodova.*

Ako q nije prim potencija, pitanje postojanja drugih savršenih kodova i dalje je otvoreno. Sad ćemo upoznati dvije konstrukcije MDS kodova, koji dostižu Singletonovu ocjenu (propoziciju 9.7). Kodovi u idućem teoremu ne moraju biti linearni i q ne mora biti potencija prostog broja.

Teorem 9.36. *Ako postoji skup od k međusobno ortogonalnih latinskih kvadrata reda q , onda postoji MDS kod s parametrima $(k + 2, q^2, k + 1, q)$.*

Dokaz. Neka su $L_1, \dots, L_k$ međusobno ortogonalni latinski kvadrati s unosima iz skupa $\{1, \dots, q\}$. Element na mjestu (i, j) kvadrata L_a označavamo s $L_a(i, j)$. Definiramo kod $C = \{(i, j, L_1(i, j), \dots, L_k(i, j)) \mid i, j = 1, \dots, q\}$. Očito je C q -arni kod duljine $k + 2$ koji se sastoji od q^2 kodnih riječi. Tvrdimo da je minimalna udaljenost tog koda $k + 1$, tj. da se dvije kodne riječi mogu podudarati najviše u jednoj koordinati. Pretpostavimo da se $x = (i_1, j_1, L_1(i_1, j_1), \dots, L_k(i_1, j_1))$ i $y = (i_2, j_2, L_1(i_2, j_2), \dots, L_k(i_2, j_2))$ podudaraju u dvije koordinate. Ako je $i_1 = i_2$ i $j_1 = j_2$, sve ostale koordinate također se podudaraju i vrijedi $x = y$. Ako je $i_1 = i_2 = i$ i $L_a(i, j_1) = L_a(i, j_2) = s$, vrijedi $j_1 = j_2$ jer se simbol s javlja samo na jednom mjestu u i -tom retku matrice L_a . Tada je također $x = y$. Analogno zaključujemo ako je $j_1 = j_2 = j$ i $L_a(i_1, j) = L_a(i_2, j) = s$ (koristimo svojstvo da se s javlja točno jednom u j -tom stupcu od L_a). Konačno, pretpostavimo da je $L_a(i_1, j_1) = L_a(i_2, j_2) = s_1$ i $L_b(i_1, j_1) = L_b(i_2, j_2) = s_2$. Zbog ortogonalnosti kvadrata L_a i L_b par simbola (s_1, s_2) javlja se točno jednom među parovima $(L_a(i, j), L_b(i, j))$, $i, j = 1, \dots, q$. Zato je ponovo $i_1 = i_2, j_1 = j_2$ i vrijedi $x = y$. Time smo dokazali da kod C ima parametre $n = k + 2, M = q^2, d = k + 1$. Uvrštavanjem vidimo da parametri zadovoljavaju $M = q^{n-d+1}$, pa je riječ o MDS kodu. $\square$

Broj kodnih riječi u linearnom $[n, m, d, q]$ kodu je $M = q^m$. Singletonova ocjena tada glasi $q^m \leq q^{n-d+1}$, odnosno $m \leq n - d + 1$. Prema tome, linearni MDS kodovi zadovoljavaju $m = n - d + 1$.

Propozicija 9.37. *Ako linearni kod C dostiže Singletonovu ocjenu, onda i njemu dualni kod $C^\perp$ dostiže Singletonovu ocjenu.*

Dokaz. Neka C ima parametre $[n, m, n - m + 1, q]$. Dualni kod $C^\perp$ ima parametre $[n, n - m, d, q]$ i pritom vrijedi $n - m \leq n - d + 1$, tj. $d \leq m + 1$. Treba vidjeti da se ta nejednakost dostiže. Neka je P matrica provjere parnosti za C , tj. generirajuća matrica za $C^\perp$. To je $(n - m) \times n$ matrica u kojoj su po propoziciji 9.29 bilo kojih $n - m$ stupaca

⁷Prošireni Golayev kod G_{24} korišten je oko 1980. u svemirskim letjelicama Voyager I i II za slanje slika Jupitera i Saturna na Zemlju.

linearno nezavisni. Prema tome, svaka $(n - m) \times (n - m)$ podmatrica od P je regularna i netrivialnim linearnim kombinacijama njezinih redaka ne može se dobiti nulvektor. Zato svaka netrivialna linearna kombinacija redaka od P ima barem $n - (n - m - 1) = m + 1$ nenul koordinata. Drugim riječima, minimalna težina koda $C^\perp$ je $d \geq m + 1$. Time smo dokazali jednakost $d = m + 1$ pa je $C^\perp$ MDS kod. $\square$

Iz dokaza prethodne propozicije slijedi karakterizacija linearnih MDS kodova.

Korolar 9.38. *Neka je C linearni $[n, m, d, q]$ kod s generirajućom matricom G i matricom provjere parnosti P . Ekvivalentno je:*

- (a) C je MDS kod, tj. vrijedi $m = n - d + 1$,
- (b) bilo kojih $n - m$ stupaca matrice P su linearno nezavisni,
- (c) bilo kojih m stupaca matrice G su linearno nezavisni.

Idući teorem daje direktnu konstrukciju linearnog MDS koda iz konačnog polja $GF(q)$.

Teorem 9.39. *Neka je q prim potencija i $m \in \{2, \dots, q\}$. Tada postoji linearni MDS kod s parametrima $[q, m, q - m + 1, q]$.*

Dokaz. Elemente polja $GF(q)$ označimo s $\alpha_0, \alpha_1, \dots, \alpha_{q-1}$, pri čemu je $\alpha_0 = 0$ i $\alpha_1 = 1$. Kod C zadajemo matricom provjere parnosti P , slično kao i Hammingove kodove. Neka je $r = q - m$ i P sljedeća $r \times q$ matrica:

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ 0 & 1 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha_2^{r-1} & \alpha_3^{r-1} & \cdots & \alpha_{q-1}^{r-1} \end{bmatrix}.$$

Parametri koda lako slijede ako uočimo da su bilo kojih r stupaca ove matrice linearno nezavisni. Naime, $r \times r$ podmatrica sastavljena od stupaca koji odgovaraju elementima polja $\alpha_{s_1}, \dots, \alpha_{s_r}$ je Vandermondeova matrica. Determinanta joj je

$$\prod_{1 \leq i < j \leq r} (\alpha_{s_i} - \alpha_{s_j}) \neq 0,$$

pa je svaka takva podmatrica regularna. Dakle, rang matrice P je r , pa su joj i reci linearno nezavisni. To znači da je dualni kod $C^\perp$ dimenzije r , a kod C je dimenzije $q - r = m$. Nadalje, po propoziciji 9.29 minimalna težina koda C je $d = r + 1 = q - m + 1$. Time smo dokazali da kod C ima parametre $[q, m, q - m + 1, q]$, koji očito dostižu Singletonovu ocjenu. $\square$

Kodovi iz prethodnog teorema nazivaju se *Reed-Solomonovim* kodovima. Za $q = 256$ i $m = 224$ dobivamo $[256, 224, 33, 256]$ kod, kojeg možemo “skratiti” do $[255, 223, 33, 256]$ koda.

Lema 9.40 (Skraćivanje koda). *Ako postoji (n, M, d, q) kod C , onda postoji $(n-1, M', d, q)$ kod C' s $M' \geq \frac{M}{q}$.*

Dokaz. Gledamo kodne riječi iz C s fiksnim simbolom a na prvoj koordinati: $C_a = \{x \in C \mid x_1 = a\}$. Po Dirichletovom principu, postoji $a \in Q$ takav da je $M' = |C_a| \geq \frac{M}{q}$. Izbacivanjem prve koordinate dobivamo kod C' duljine $n-1$ s M' kodnih riječi. Minimalna udaljenost d je ostala ista jer se riječi iz C_a podudaraju na izbačenoj koordinati. $\square$

U linearnim kodovima simboli se javljaju jednako mnogo puta na svakoj koordinati, pa vrijedi $M' = \frac{M}{q}$. CIRC kodovi koji se koriste za zapisivanje glazbe na CD, spomenut u primjeru 9.2, napravljeni su najčešće od dva isprepletena skraćena Reed-Solomonova [255, 223, 33, 256] koda. Ispreplitanjem se postiže da uzastopne pogreške budu raspršene, što omogućuje ispravljanje duljih nizova pogrešaka. Abeceda je polje reda 256, a pojedini simboli realiziraju se kao bajtovi (nizovi od 8 bitova).

Na kraju pogledajmo kako od Hadamardovih matrica dobivamo kodove koji dostižu Plotkinovu ocjenu (propoziciju 9.9).

Teorem 9.41. *Ako postoji Hadamardova matrica reda $n \geq 4$, onda postoje binarni kodovi s parametrima $(n-1, n, \frac{n}{2}, 2)$ i $(n-2, \frac{n}{2}, \frac{n}{2}, 2)$ koji dostižu Plotkinovu ocjenu.*

Dokaz. Prisjetimo se da je Hadamardova matrica kvadratna matrica nad $\{1, -1\}$ s ortogonalnim recima. Kad računamo skalarni produkt redaka, dobivamo 1 ako množimo jednake unose (dvije jedinice ili dvije minus jedinice), a -1 ako množimo različite unose. Skalarni produkt je 0, pa je broj jednakih unosa isti kao broj različitih unosa. To znači da je Hammingova udaljenost bilo koja dva retka $\frac{n}{2}$, tj. reci Hadamardove matrice čine $(n, n, \frac{n}{2}, 2)$ kod nad abecedom $\{1, -1\}$. Taj kod je ekvidistantan (svake dvije kodne riječi su na minimalnoj udaljenosti $d = \frac{n}{2}$), ali na njega ne možemo primijeniti Plotkinovu ocjenu jer ne zadovoljava uvjet $d > \frac{n}{2}$. Kod s parametrima $(n-1, n, \frac{n}{2}, 2)$ dobivamo tako da uzmemo Hadamardovu matricu H u standardnom obliku (s jedinicama u prvom stupcu), obrišemo prvi stupac i retke proglasimo kodnim riječima. U ostalim stupcima matrice H ima jednako mnogo jedinica i minus jedinica, pa skraćivanjem tog koda dobivamo $(n-2, \frac{n}{2}, \frac{n}{2}, 2)$ kod. Ova dva koda zadovoljavaju uvjet $d > \frac{n}{2}$ i dostižu Plotkinovu ocjenu. $\square$

Primjer 9.42. *Od Hadamardove matrice reda 8 iz primjera 4.14 dobivamo kod $C_1 = \{1111111, 0101010, 1001100, 0011001, 1110000, 0100101, 1000011, 0010110\}$ s parametrima $(7, 8, 4, 2)$ i kod $C_2 = \{111111, 001100, 110000, 000011\}$ s parametrima $(6, 4, 4, 2)$. Ovdje smo unose -1 zamijenili s 0.*

Sljedeći teorem je generalizacija ove konstrukcije. Dobivamo kodove koji dostižu Plotkinovu ocjenu za bilo koje parne n i d , ako je istinita hipoteza o postojanju Hadamardovih matrica svih redova djeljivih s 4.

Teorem 9.43 (Levenshtein). *Neka su n i d parni prirodni brojevi takvi da je $2d > n$ i neka je $k = \lfloor \frac{d}{2d-n} \rfloor$. Ako postoje Hadamardove matrice reda $4k$ i $4k+4$, onda postoji $(n, 2k, d, 2)$ kod koji dostiže Plotkinovu ocjenu.*

Dokaz se nalazi u knjizi [16] na str. 241.

Zadaci

Zadatak 9.1. Jedinstveni matični broj građanina (JMBG) sastoji se od 13 znamenaka. Zadnja znamenka je kontrolna i računa se na sljedeći način. Prvih 12 znamenaka množe se redom s 4, 5, 6, 7, 8, 9, 4, 5, 6, 7, 8, 9 i umnošci se zbroje. Kontrolna znamenka je ostatak pri dijeljenju dobivenog zbroja s 11 (ako je ostatak 10 stavlja se 0). Provjerite slaže li se to sa zadnjom znamenkom vašeg JMBG-a. Uvjerite se da kontrolna znamenka omogućuje otkrivanje pogrešaka koje nastaju promjenom jedne znamenke ili zamjenom susjednih znamenaka JMBG-a.

Zadatak 9.2. Primljena je sljedeća poruka, kodirana s pomoću $[7, 4, 3, 2]$ koda iz primjera 9.14: 1011010 0001000 1100010 0010101. Dekodirajte poruku, tj. otkrijte koje su heksadecimalne znamenke poslane, ako je poznato da je pri prijenosu nastala najviše jedna pogreška po kodnoj riječi.

Zadatak 9.3. Konstruirajte nelinearni kod ekvivalentan kodu iz primjera 9.14.

Zadatak 9.4. Dokažite da je Hammingov kod $\text{Ham}(2, 2)$ jednak binarnom kodu trostrukog ponavljanja $C = \{000, 111\}$.

Zadatak 9.5. Dokažite da je Hammingov kod $\text{Ham}(3, 2)$ ekvivalentan s binarnim kodom iz primjera 9.14.

Zadatak 9.6. Dokažite obrat teorema 9.33: ako nosači kodnih riječi minimalne težine u linearnom $[n, m, d, q]$ kodu s $d = 2e + 1$ čine $(e + 1)$ -($n, d, (q - 1)^e$) dizajn, onda je taj kod savršen.

Zadatak 9.7. Dokažite obrat teorema 9.36: ako postoji MDS kod s parametrima $(k + 2, q^2, k + 1, q)$, onda postoji skup od k međusobno ortogonalnih latinskih kvadrata reda q .

Zadatak 9.8. Dokažite obrat teorema 9.41: ako postoji ekvidistantni kod s parametrima $(n - 1, n, \frac{n}{2}, 2)$, onda postoji Hadamardova matrica reda n .

Poglavlje 10

Jedna primjena dizajna: algoritam za grupno testiranje

Pretpostavimo da je u nekoj skupini uzoraka potrebno identificirati one uzorke koji se ističu određenim svojstvom. Tipični je primjer određivanje “pozitivnih” uzoraka krvi kao uzoraka zaraženih nekim virusom. Ako je pojedinačni test previše skup, korisno je najprije grupirati uzorke i testirati smjesu uzoraka čitave grupe. Dakako, pozitivan rezultat značit će da je barem jedan uzorak zaražen, a negativan rezultat da nijedan uzorak iz te grupe nije zaražen, uz pretpostavku da je test pouzdan. Potrebno je, dakle, definirati grupe uzoraka na takav način da se iz rezultata testiranja cijelih grupa može jednoznačno identificirati pozitivne individualne uzorke, a da pritom broj grupa bude manji od broja pojedinačnih uzoraka. To će biti moguće ako pozitivnih uzoraka nema “previše”.

Izložiti ćemo u osnovnim crtama jedan postupak za grupno testiranje, tipa NAGTA (eng. *non-adaptive group testing algorithm*), pri čemu “neadaptivan” znači da je plan testiranja čvrsto određen unaprijed i ne prilagođava se djelomičnim ishodima tokom postupka (primjerice, da se uzorci koji su sačinjavali “negativnu” grupu ne obuhvaćaju daljnjim testovima). To ima svojih prednosti, među ostalima zbog lakše pripreme i mogućnosti usporednog odvijanja više testova.

Za incidencijsku strukturu koju ćemo ovdje razmatrati uvest ćemo nešto drukčije oznake od dosad uobičajenih. Neka je X skup od m elemenata, koje ćemo zvati *uzorcima*, a $\mathcal{A}$ familija nekih n podskupova od X koje ćemo nazivati *testovima*. Ne postavlja se uvjet balansiranosti ili uniformnosti na strukturu $(X, \mathcal{A})$, no kako želimo minimizirati broj testova, pretpostavljamo da je $n < m$ (u protivnom možemo jednočlanim testovima trivijalno identificirati “pozitivne” uzorke). Zbog tog uvjeta bit će nam potrebna dualna struktura dizajna, u skladu s Fisherovom nejednakosti. U daljnjem ćemo uređeni par $(X, \mathcal{A})$ s navedenim svojstvima nazivati (m, n) -NAGTA.

Označimo nadalje s U podskup “pozitivnih” uzoraka, kratko *pozitivan podskup*. Cilj postupka je određivanje U , a rezultate testiranja pojedinih podskupova od X izrazit ćemo s pomoću test funkcije $f : 2^X \rightarrow \{0, 1\}$ koja podskupu $Y \subseteq X$ pridružuje 1 ili 0 već prema tome je li $Y \cap U$ neprazan ili prazan, to jest sadrži li Y barem jedan pozitivan uzorak ili ne. Jasno je da funkcija f ovisi o podskupu U . Za određeni (m, n) -NAGTA i pozitivni podskup U , binarna uređena n -torka $R(U)$ vrijednosti $f(A)$, za sve $A \in \mathcal{A}$, predstavlja rezultat svih n testova. Kažemo da $(X, \mathcal{A})$ *identificira pozitivni podskup* U ako je U

jednoznačno određen kao funkcija vektora $R(U)$, odnosno ako za različite podskupove $U, V \subseteq X$ nužno vrijedi $R(U) \neq R(V)$. U praksi je prihvatljiva pretpostavka da broj pozitivnih uzoraka ne prelazi neki fiksirani pozitivni cijeli broj s . Kaže se da je $(X, \mathcal{A})$ (m, n) -NAGTA s *pragom* s ako za svaka dva podskupa $U, V \subseteq X$, takva da niti jedan od njih nema više od s elemenata, vrijedi $R(U) \neq R(V)$.

Primjer 10.1. *Uzmimo $(8, 6)$ -NAGTA tako da je $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ i $\mathcal{A} = \{\{1, 2, 3, 4\}, \{1, 2, 5, 6\}, \{3, 5, 7, 8\}, \{1, 4, 5, 8\}, \{2, 3, 6, 7\}, \{4, 6, 7, 8\}\}$. Lako se provjeri da se za sve jednočlane podskupove $U \subseteq X$ dobivaju međusobno različiti vektori $R(U)$, tako da je prag barem 1. No, postoje već dvočlani podskupovi, npr. $V_1 = \{1, 6\}$ i $V_2 = \{2, 4\}$, takvi da se rezultati podudaraju: $R(V_1) = R(V_2) = (1, 1, 0, 1, 1, 1)$. Stoga je to $(8, 6)$ -NAGTA s pragom točno 1.*

Neka je sada $(Y, \mathcal{B})$ $2-(v, k, 1)$ dizajn. Njegovu dualnu strukturu označimo s $(X, \mathcal{A})$, jer to će biti odabrani (b, v) -NAGTA. Uzimajući u obzir poznata svojstva dizajna i njegove dualne strukture, vidimo da se svaki od b uzoraka pojavljuje u točno k testova, svaki od ukupno v testova sadrži r uzoraka i svaki se par različitih uzoraka pojavljuje zajedno u najviše jednom testu. Pokažimo da ovaj NAGTA ima prag $s = k - 1$. Opisat ćemo algoritam koji identificira pozitivan podskup U , ako taj sadrži najviše $k - 1$ elemenata.

Primijetimo najprije da za bilo koji NAGTA i za bilo koji podskup $U \subseteq X$ očito vrijedi da je U sadržan u skupu $X \setminus \bigcup A$, pri čemu se unija uzima po svim “negativnim” testovima, dakle svim podskupovima $A \in \mathcal{A}$ takvima da je $f(A) = 0$. No, za NAGTA dobiven dualiziranjem $2-(v, k, 1)$ dizajna vrijedit će ne samo inkluzija nego jednakost, uz pretpostavku da podskup U ima najviše $k - 1$ elemenata. Stoga će se pozitivni podskup jednostavno određivati kao komplement unije svih negativnih testova. Pretpostavimo suprotno, da za podskup U koji ima najviše $k - 1$ elemenata vrijedi stroga inkluzija, to jest da postoji x koji ne pripada podskupu U i koji se ne nalazi ni u jednom negativnom testu (negativni uzorak koji je sadržan samo u pozitivnim testovima). Uzorak x pojavljuje se onda u točno k testova i svi su pozitivni, što znači da svaki mora sadržavati bar jedan pozitivni uzorak. Svi ti pozitivni uzorci međusobno su različiti, jer se x s bilo kojim drugim uzorkom nalazi u istom testu najviše jedanput, odakle slijedi da postoji barem k različitih pozitivnih uzoraka. To je proturječenje s pretpostavkom pa je naša tvrdnja dokazana. Možemo formulirati sljedeći

Teorem 10.2. *Ako postoji $2-(v, k, 1)$ dizajn, onda postoji (b, v) -NAGTA s pragom $k - 1$.*

Uočimo još jednu korisnu činjenicu. Ako pozitivnih uzoraka ima barem k , nećemo moći pouzdano identificirati pozitivni podskup U , no iz inkluzije U u komplementu unije svih negativnih testova vidimo da će tada i taj komplement imati barem k elemenata. To znači da ako postoji barem k uzoraka koji se ne pojavljuju ni u jednom negativnom testu, onda je sigurno da pozitivnih uzoraka ima barem k .

Evo na kraju i jednog primjera NAGTA na temelju dokazanog teorema.

Primjer 10.3. *Kao pogodan nesimetrični dizajn može poslužiti afina ravnina reda 3, dakle $2-(9, 3, 1)$ dizajn, čija će dualna struktura predstavljati $(12, 9)$ -NAGTA s pragom jednakim 2.*

Neka su točke afine ravnine označene s $1, 2, \dots, 9$, a pravci neka su $\{1, 2, 3\}$, $\{4, 5, 6\}$, $\{7, 8, 9\}$, $\{1, 4, 7\}$, $\{2, 5, 8\}$, $\{3, 6, 9\}$, $\{1, 5, 9\}$, $\{2, 6, 7\}$, $\{3, 4, 8\}$, $\{1, 6, 8\}$, $\{2, 4, 9\}$ i $\{3, 5, 7\}$. Uzmemo li da su pravci numerirani redom $B_1, \dots, B_{12}$, dualiziranjem dobivamo sljedeći skup testova (pri čemu radi jednostavnosti izostavljamo oznaku B i pišemo samo brojeve koji odgovaraju indeksima): $A_1 = \{1, 4, 7, 10\}$, $A_2 = \{1, 5, 8, 11\}$, $A_3 = \{1, 6, 9, 12\}$, $A_4 = \{2, 4, 9, 11\}$, $A_5 = \{2, 5, 7, 12\}$, $A_6 = \{2, 6, 8, 10\}$, $A_7 = \{3, 4, 8, 12\}$, $A_8 = \{3, 5, 9, 10\}$, $A_9 = \{3, 6, 7, 11\}$.

Uzmimo da je testiranjem dobiven vektor $R(U) = (1, 0, 0, 1, 0, 1, 1, 1, 0)$. Negativni testovi su A_2 , A_3 , A_5 i A_9 , a njihova unija glasi $\{1, 2, 3, 5, 6, 7, 8, 11, 12\}$. Izostali su uzorci 4 i 10 pa je $U = \{4, 10\}$ pozitivan podskup.

Uočimo još što bi se moglo dogoditi kad bi broj pozitivnih uzoraka prelazio prag. Ako je npr. $U = \{5, 6, 12\}$, lako vidimo da ovaj postupak daje samo dva negativna testa, A_1 i A_4 , pa bi negativni uzorci 3 i 8 bili pogrešno uvršteni među pozitivne. No, ipak bi bilo jasno da pozitivnih uzoraka ima barem 3 i da se oni nalaze u skupu $\{3, 5, 6, 8, 12\}$.

Poglavlje 11

Rješenja nekih zadataka

Zadatak 3.2. Lako se provjeri da za sve $n_1, n_2 \in N$ vrijedi $n_1 n_2^{-1} \in N$, pa je N podgrupa od G . Za normalnost treba provjeriti $gN = Ng$, tj. $gNg^{-1} = N$, za zvaki $g \in G$. Neka su $g \in G$ i $n \in N$ proizvoljni. Tvrdimo da je $gng^{-1} \in N$:

$$(gng^{-1})x = g(n(g^{-1}x)) = g(g^{-1}x) = (gg^{-1})x = 1x = x, \quad \forall x \in X.$$

Dakle, $gNg^{-1} \subseteq N$, a obrnuta inkluzija slijedi iz jednakobrojnosti ta dva skupa.

Zadatak 4.5. Postoje takvi dizajni s parametrima $(25, 9, 3)$ (vidi [7]). Pitanje postojanja projektivnih ravnina koje su samodualne, ali nisu samopolarne je otvoreno.

Zadatak 6.2. Neka je D diferencijski skup s parametrima (v, k, λ) u grupi G . Tvrdimo da je komplement D^c diferencijski skup s parametrima $(v, v - k, v - 2k + \lambda)$. Treba pokazati da se svaki element $d \in G \setminus \{1\}$ može prikazati na točno $\lambda^c = v - 2k + \lambda$ načina kao “diferencija” elemenata iz D^c , tj. u obliku $d = x^{-1}y$ za $x, y \in D^c$. Očito vrijedi

$$|\{(x, y) \in D \times D \mid x^{-1}y = d\}| = \lambda,$$

$$|\{(x, y) \in G \times G \mid x^{-1}y = d\}| = v,$$

$$|\{(x, y) \in D \times G \mid x^{-1}y = d\}| = k,$$

$$|\{(x, y) \in G \times D \mid x^{-1}y = d\}| = k.$$

Označimo sa

$$m = |\{(x, y) \in D \times D^c \mid x^{-1}y = d\}|,$$

$$n = |\{(x, y) \in D^c \times D \mid x^{-1}y = d\}|.$$

Zbog $D \times G = (D \times D) \dot{\cup} (D \times D^c)$ i $G \times D = (D \times D) \dot{\cup} (D^c \times D)$ (disjunktna unija) vrijedi $k = \lambda + m = \lambda + n$, odnosno $m = n = k - \lambda$. Dakle, brojevi $m, n \in \mathbb{N}$ ne ovise o izboru elementa $d \in G \setminus \{1\}$. Sada zbog $G \times G = (D \times D) \dot{\cup} (D \times D^c) \dot{\cup} (D^c \times D) \dot{\cup} (D^c \times D^c)$ imamo $v = \lambda + m + n + \lambda^c$, pa vidimo da ni $\lambda^c = v - m - n - \lambda = v - 2k + \lambda$ ne ovisi o izboru $d \in G \setminus \{1\}$.

Bibliografija

- [1] E.F. Assmus, H.F. Mattson, *On tactical configurations and error-correcting codes*, J. Combinatorial Theory **2** (1967), 243-257.
- [2] E.F. Assmus, H.F. Mattson, *New 5-designs*, J. Combinatorial Theory **6** (1969), 122-151.
- [3] T. Beth, D. Jungnickel, H. Lenz, *Design theory*, Cambridge University Press, 1993.
- [4] P.J. Cameron, *Combinatorics: topics, techniques, algorithms*, Cambridge University Press, 1994.
- [5] C.J. Colbourn, J.H. Dinitz (eds.), *The handbook of combinatorial designs, Second edition*, CRC Press, 2007.
- [6] P. Dembowski, *Finite Geometries*, Springer, 1968.
- [7] R.H.F. Denniston, *Enumeration of symmetric designs* (25, 9, 3), Algebraic and geometric combinatorics, 111-127, North-Holland Math. Stud. **65**, North-Holland, Amsterdam, 1982.
- [8] A. Dujella, *Uvod u teoriju brojeva*, skripta, PMF-Matematički odsjek, 2009. Dostupno na <http://web.math.hr/~duje/utb/utblink.pdf>
- [9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008. Dostupno na <http://www.gap-system.org>
- [10] M.J.E. Golay, *Notes on digital coding*, Proc. IRE, **37** (1949), 657.
- [11] R. Hill, *A first course in coding theory*, Oxford University Press, 1996.
- [12] D.R. Hughes, F.C. Piper, *Projective Planes*, Springer, 1973.
- [13] H. Kharaghani, B. Tayfeh-Rezaie, *A Hadamard matrix of order 428*, J. Combin. Des. **13** (2005), 435-440.
- [14] E.S. Kramer, D.M. Mesner, *t-designs on hypergraphs*, Discrete Math. **15** (1976), 263–296.
- [15] D. Palman, *Projektivna geometrija*, Školska knjiga, Zagreb, 1984.
- [16] D.R. Stinson, *Combinatorial designs. Constructions and analysis*, Springer, 2004.