Rastavljivi dizajni

Marković, Ilija

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Ilija Marković

Rastavljivi dizajni

Diplomski rad

Voditelj rada:
prof.dr.sc. Vedran Krčadinac

Zagreb, studeni 2015.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____ , predsjednik
2. _____ , član
3. _____ , član

Povjerenstvo je rad ocijenilo ocjenom _____ .

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

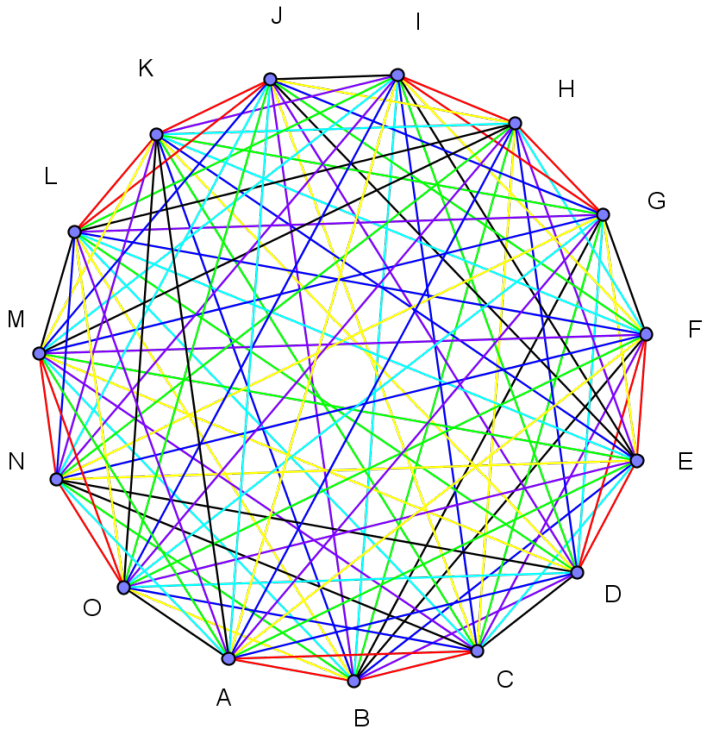
Sadržaj

1 Uvod

Poznato nam je da rješavanje matematičkih problema dovodi do nastanka novih matematičkih disciplina. Sjetimo se Fermatovog problema u teoriji brojeva, kojeg su brojni matematičari rješavali dugi niz godina. Jedan matematički problem, objavljen 1850. kao nagradno pitanje u engleskom časopisu *The Lady's and Gentleman's Diary*, glasi: petnaest učenica šeta svaki dan, u pet redova po tri učenice. Mogu li se učenice svrstati tako da se u sedam dana svake dvije učenice nađu zajedno u istom redu točno jedanput? Problem je objavio velečasni Thomas Penyngton Kirkman, pa govorimo o *Kirkmanovu problemu 15 učenica*. Taj problem postao je karakteristični primjer rastavljivog dizajna. Rastavljivi dizajn je matematička struktura kojom ćemo se baviti u ovom diplomskom radu. No, kako bismo riješili postavljeni problem ako ne znamo ništa o dizajnima. Neka nam slova A,B,C,...,M,N,O predstavljaju učenice. Prikažimo rješenje problema pomoću tablice.

ponedjeljak	ABC	DEF	GHI	JKL	MNO
utorak	ADH	BEK	CIO	FLN	GJM
srijeda	AEM	BHN	CGK	DIL	FJO
četvrtak	AFI	BLO	CHJ	DKM	EGN
petak	AGL	BDJ	CFM	EHO	IKN
subota	AJN	BIM	CEL	DOG	FHK
nedjelja	AKO	BFG	CDN	EIJ	HLM

Iz tablice vidimo da se učenice mogu svrstati na traženi način. Ispisivanje šetnji koje zadovoljavaju tražene uvjete je dosta komplicirano. Svaka dva slova smiju biti zajedno samo jedanput, svako slovo mora biti u trojkama sa svima preostalim slovima i u svakom retku tablice moramo imati zastupljena sva slova. Postoji li jednostavniji način prikazivanja rješenja? Rješenje problema možemo prikazati i grafički. Neka je $ABC...MNO$ petnaesterokut. Ako nacrtamo dijagonale tada su nam svake dvije točke međusobno spojene. Svake tri točke su vrhovi trokuta. Znamo da iz svakog vrha izlazi 12 dijagonala, pa je ukupan broj dijagonala 90 (svaku dijagonalu smo brojali 2 puta). Kako imamo 15 stranica petnaesterokuta, to je ukupno 105 spojnica dviju točaka. Kako vidimo na grafu sa slike 1 vrhovi nam predstavljaju učenice, boje dane i trokuti redove šetnje. Trokuti iste boje sadrže svaki vrh točno jednom. Particionirali smo cijeli skup od 105 bridova grafa na 7 takvih skupova od 5 disjunktnih trokuta (obojanih istom bojom).



Slika 1: Vizualizacija Kirkmanova problema

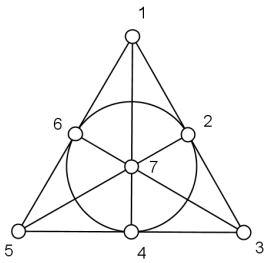
Pokazat ćemo još jednu interpretaciju Kirkmanova problema kada se upoznamo s rastavljivim dizajnima.

2 Dizajni

Proučavati ćemo konačne pravilne matematičke strukture. Za početak neka su nam dani konačni skupovi $\mathcal{T}$ i $\mathcal{B}$. Elemente skupa $\mathcal{T}$ nazivamo *točkama*, a elemente skupa $\mathcal{B}$ *blokovima*. Relaciju $I \subseteq \mathcal{T} \times \mathcal{B}$ nazivamo relacijom *incidencije*. Uređena trojka $(\mathcal{T}, \mathcal{B}, I)$ je *konačna incidencijska struktura*. Ako za $x \in \mathcal{T}$ i $B \in \mathcal{B}$ vrijedi $(x, B) \in I$ zapisujemo xIB i kažemo da točka x leži na bloku B ili blok B prolazi točkom x.

Definicija 2.1. 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.*

Primjer 2.2. *Neka je* $\mathcal{T} = \{1, 2, 3, 4, 5, 6, 7\}$*, a* $\mathcal{B} = \{\{1, 2, 3\}, \{3, 4, 5\}, \{1, 5, 6\}, \{1, 4, 7\}, \{2, 5, 7\}, \{3, 6, 7\}, \{2, 4, 6\}\}$*. Ukupan broj točaka je* 7*, na svakom bloku leže* 3 *točke i kroz svake dvije točke prolazi jedan blok. Prema tome imamo dizajn s parametrima* $(7, 3, 1)$ *koji nazivamo* Fanovom ravninom*.*



Slika 2: Fanova ravnina

Propozicija 2.3. *Kroz svaku točku* (v, k, λ) *dizajna prolazi točno* $r = \lambda \cdot \dfrac{v-1}{k-1}$ *blokova.*

Dokaz. Neka je x_0 točka, označimo broj blokova kroz x_0 s r. Promotrimo sljedeći skup

$$\{(x, B) | x \in \mathcal{T}, B \in \mathcal{B}, x \neq x_0, x, x_0 I B\}.$$

Elemente skupa možemo prebrojiti na dva načina. Točku x možemo odabrati na $v-1$ načina i kroz točke x i x_0 prolazi λ blokova, pa imamo $(v-1)\cdot\lambda$ parova. Blok B kroz točku x_0 možemo izabrati na r načina, a na svakom bloku leži

$k-1$ točaka x različitih od x_0. U ovom slučaju broj parova je $r \cdot (k-1)$. Kada izjednačimo broj parova u oba slučaja dobivamo $r = \lambda \cdot \dfrac{v-1}{k-1}$. □

Propozicija 2.4. *Ukupan broj blokova (v, k, λ) dizajna je $b = \lambda \cdot \dfrac{v(v-1)}{k(k-1)}$.*

Dokaz. Sve incidentne parove (x, B) možemo prebrojati na dva načina. Kroz svaku od v točaka prolazi r blokova, pa imamo $v \cdot r$ incidentnih parova. Na svakom od b blokova leži k točaka, te imamo $b \cdot k$ incidentnih parova. Izjednačimo oba slučaja $v \cdot r = b \cdot k$. Uvrstimo r iz prethodne propozicije i dobivamo $b = \lambda \cdot \dfrac{v(v-1)}{k(k-1)}$. □

Ponekad se r i b navode kao parametri dizajna, tj. imamo (v, b, r, k, λ) dizajn. Dizajne možemo reprezentirati matricama.

Definicija 2.5. *Neka je $\boldsymbol{D} = (\mathcal{T}, \mathcal{B})$ konačna incidencijska struktura gdje je $\mathcal{T} = \{x_1, ..., x_v\}$ i $\mathcal{B} = \{B_1, ..., B_b\}$.* Incidencijska matrica *od $\boldsymbol{D}$ je $v \times b$ matrica $A = [a_{ij}]$ definirana s*

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

S I označimo jediničnu matricu reda v, a J matricu popunjenu jedinicama reda v i s j_v, j_b jednoretčane matrice popunjene jedinicama koje imaju v i b stupaca.

Teorem 2.6. *Neka je A matrica tipa $v \times b$ popunjena nulama i jedinicama. Matrica A je incidencijska matrica dizajna s parametrima (v, b, r, k, λ) ako i samo ako vrijedi $j_v \cdot A = k j_b$ i $A \cdot A^\tau = (r-\lambda)I + \lambda J$.*

Dokaz. Množenjem matrica j_v i A dobivamo sume stupaca matrice A. Zato je jednakost $j_v \cdot A = k j_b$ ekvivalentna činjenici da u incidencijskoj strukturi koju predstavlja matrica A na svakom bloku leži točno k točaka. U matrici $A \cdot A^\tau$ 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. Ako je $i = j$, tada predstavlja broj blokova kroz i-tu točku. Matrica $(r-\lambda)I + \lambda J$ ima brojeve r na dijagonali i λ izvan dijagonale. Jednakost $A \cdot A^\tau = (r-\lambda)I + \lambda J$ vrijedi ako i samo ako kroz svaku točku incidencijske strukture prolazi točno r blokova, a kroz svake dvije točke prolazi točno λ blokova. Ove dvije jednakosti zadovoljavaju definiciju 2.1 i propoziciju 2.3. Prema tome, incidencijska struktura koju predstavlja matrica A je 2-dizajn s parametrima (v, b, r, k, λ). □

U sljedećoj lemi ćemo odrediti determinantu matrice iz prethodnog teorema.

Lema 2.7. *Determinanta matrice* $(r-\lambda)I+\lambda J$ *jednaka je* $(r-\lambda)^{v-1}(r+(v-1)\lambda)$.

Dokaz. Matrica $(r-\lambda)I+\lambda J$ ima brojeve r na dijagonali i λ izvan dijagonale. U prvom koraku izračunavanja determinante svim retcima od drugog do zadnjeg oduzmemo prvi redak:

$$\begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{vmatrix} = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda-r & r-\lambda & 0 & \cdots & 0 \\ \lambda-r & 0 & r-\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda-r & 0 & 0 & \cdots & r-\lambda \end{vmatrix}.$$

Zbroj drugog do zadnjeg stupca dodamo prvom stupcu:

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

Izlučimo $r-\lambda$ iz svih redaka osim prvog:

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

Razvijemo determinantu po prvom stupcu:

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

Determinanta jedinične matrice jednaka je 1, pa je konačni rezultat $(r-\lambda)^{v-1}(r+(v-1)\lambda)$. □

Prema propoziciji 2.3, $\lambda(v-1) = r(k-1)$. Odatle slijedi $r + (v-1)\lambda = rk$. Prema tome determinanta iz prethodne leme jednaka je $rk(r-\lambda)^{v-1}$. Dakle, determinanta je različita od nule. Iz propozicija 2.3 i 2.4 slijedi da za postojanje dizajna s parametrima (v, b, r, k, λ) mora vrijediti $k-1$ dijeli $\lambda(v-1)$ i $k(k-1)$ dijeli $\lambda v(v-1)$. Sljedeći teorem daje još jedan nuždan uvjet za postojanje dizajna.

Teorem 2.8. (Fisherova nejednakost). *Ako postoji dizajn s parametrima* (v, b, r, k, λ)*, onda je* $v \leq b$.

Dokaz. Neka je A incidencijska matrica dizajna s parametrima (v, b, r, k, λ). Kako je determinanta matrice $A \cdot A^\tau$ različita od nule, bilo koja dva retka (stupca) nisu proporcionalna i bilo koji redak (stupac) nije jednak linearnoj kombinaciji preostalih redaka (stupaca). Tada je matrica $A \cdot A^\tau$ punog ranga v. Rang od A je v jer kod množenja matrica rang se ne povećava. Kako je rang manji ili jednak od broja stupaca matrice A, vrijedi $v \leq b$. □

Kasnije ćemo pokazati i općenitiji teorem. Za parametre $(16, 6, 1)$ imamo $b = 8$. Prema Fisherovoj nejednakosti ne postoji dizajn s tim parametrima. Posebno će nam biti zanimljivi dizajni za koje vrijedi jednakost u Fisherovoj nejednakosti.

Definicija 2.9. *Dizajni koji imaju jednako mnogo točaka i blokova nazivaju se* simetrični dizajni.

Za primjer imamo već spomenutu Fanovu ravninu koja ima 7 točaka i 7 blokova. Kod simetričnih dizajna svaka dva bloka sijeku se točno u λ točaka.

Teorem 2.10. *Neka je* $\boldsymbol{D}$ *simetrični* (v, k, λ) *dizajn sa skupom blokova* $\mathcal{B} = \{B_1, ..., B_v\}$*. Tada za svaka dva bloka* $B_i \neq B_j$ *vrijedi* $|B_i \cap B_j| = \lambda$.

Dokaz. Neka je A incidencijska matrica simetričnog dizajna $\mathbf{D}$. Tada je A kvadratna matrica reda v. Kako je A ranga v, slijedi da je regularna matrica, tj. postoji inverzna matrica A^{-1}. Kako je $\mathbf{D}$ simetrični dizajn, $r = k$. Sada jednakost $A \cdot A^\tau = (k-\lambda)I + \lambda J$ pomnožimo s lijeva matricom A^{-1}:

$$A^\tau = (k-\lambda)A^{-1} + \lambda A^{-1}J. \tag{1}$$

Sume redaka od A jednake su k i A je matrica reda v, pa vrijedi $AJ = kJ$. Tu jednakost pomnožimo s lijeva s A^{-1} i dobivamo $A^{-1}J = \frac{1}{k}J$. Uvrštavanjem u (1) slijedi

$$A^\tau = (k-\lambda)A^{-1} + \frac{\lambda}{k}J. \tag{2}$$

Sume stupaca od A su k, pa je $JA = kJ$. Pomnožimo s A zdesna (2) i uvrstimo JA, pa dobivamo

$$A^\tau \cdot A = (k - \lambda)I + \lambda J. \tag{3}$$

Na mjestu (i, j) u matrici $A^\tau \cdot A$ nalazi se skalarni produkt i-tog i j-tog stupca matrice A. Ako je $i \neq j$, skalarni produkt predstavlja broj točaka koje sadrže i-ti i j-ti blok od $\mathbf{D}$. Prema (3) u matrici $A^\tau \cdot A$ na svim mjestima izvan dijagonale nalaze se brojevi λ. To znači da je kardinalnost presjeka svaka dva različita bloka simetričnog dizajna $\mathbf{D}$ jednaka λ. □

Upoznat ćemo dvije konstrukcije koje od simetričnog dizajna prave nesimetrični dizajn.

Propozicija 2.11. *Neka je $\boldsymbol{D}$ simetrični (v, k, λ) dizajn s $\lambda \geq 2$ i B bilo koji njegov blok. Incidencijska struktura dobivena uklanjanjem bloka B i uzimanjem svih točaka incidentnih s njim je nesimetrični $(k, \lambda, \lambda - 1)$ dizajn.*

Dokaz. Ukupan broj točaka jednak je kardinalnosti bloka B, tj. k. U preostalim blokovima imamo samo točke koje leže na bloku B, pa zbog teorema 2.10 kardinalnost tih blokova je λ. Tada kroz svake dvije točke prolazi jedan blok manje nego u $\mathbf{D}$. Prema tome imamo 2-$(k, \lambda, \lambda - 1)$ dizajn. □

Taj nesimetrični dizajn nazivamo *derivirani dizajn* od $\mathbf{D}$ u bloku B i označavamo sa $\mathbf{D}_B$.

Propozicija 2.12. *Neka je $\boldsymbol{D}$ simetrični (v, k, λ) dizajn s $k \geq \lambda + 2$ i B bilo koji njegov blok. Incidencijska struktura dobivena uklanjanjem bloka B i svih točaka incidentnih s njim je nesimetrični $(v - k, k - \lambda, \lambda)$ dizajn.*

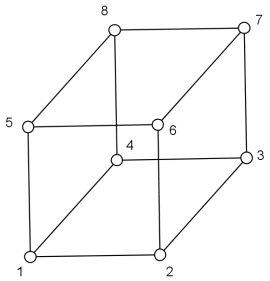
Dokaz. Kako je k kardinalnost svakog bloka od $\mathbf{D}$, ukupan broj točaka je $v - k$. Svake dvije točke su sadržane u λ blokova (uklonjene su točke koje su ležale na bloku B). Kako je $\mathbf{D}$ simetrični dizajn, svaka dva različita bloka od $\mathbf{D}$ sijeku se u λ točaka. Tada je iz preostalih blokova uklonjeno λ točaka. Dobivena struktura je $(v - k, k - \lambda, \lambda)$ dizajn. □

Dizajn dobiven u prethodnoj propoziciji nazivamo *rezidualni dizajn* od $\mathbf{D}$ u bloku B i označavamo sa $\mathbf{D}^B$. Dizajne možemo i generalizirati.

Definicija 2.13. *Neka je $t \geq 0$.* 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.

Dizajn iz definicije 2.1 zapravo je 2-dizajn, tj. dizajn s $t = 2$. Kada govorimo o t-dizajnima prvenstveno mislimo na dizajne za $t > 2$.

Primjer 2.14. *Neka je* $\mathcal{T} = \{1, 2, 3, 4, 5, 6, 7, 8\}$, *a* $\mathcal{B} = \{\{1, 2, 4, 5\}, \{2, 1, 3, 6\}, \{3, 2, 4, 7\}, \{4, 1, 3, 8\}, \{5, 1, 6, 8\}, \{6, 2, 5, 7\}, \{7, 3, 6, 8\}, \{8, 4, 5, 7\}, \{1, 2, 8, 7\}, \{3, 4, 6, 5\}, \{2, 3, 5, 8\}, \{1, 4, 6, 7\}, \{1, 5, 3, 7\}, \{2, 6, 4, 8\}\}$. *Grafički točke možemo prikazati kao vrhove kocke. Prvih 8 blokova sastoje se od vrha kocke i tri njemu susjedna vrha. Preostalih 6 blokova sastoje se od vrhova na dva nasuprotna brida kocke. Bilo koja tri vrha kocke sadržana su u jednom bloku, tj. imamo* 3-$(8, 4, 1)$ *dizajn.*



Slika 3: 3-(8,4,1) dizajn

Sljedeći teorem je generalizacija propozicija 2.3 i 2.4 na t-dizajne.

Teorem 2.15. *Neka je incidencijska struktura* $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ *dizajn s parametrima* t-(v, k, λ). *Tada je* $\boldsymbol{D}$ *ujedno* s-(v, k, λ_s) *dizajn, za svaki* $s \in \{0, ..., t\}$ *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. Promotrimo skup

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

Elemente skupa možemo prebrojati na dva načina. Na $\binom{v-s}{t-s}$ načina možemo izabrati skup T koji sadrži skup S, a blok B koji sadrži skup T

na λ načina. To je ukupno $\binom{v-s}{t-s} \cdot \lambda$ elemenata. Blok B koji sadrži skup S možemo izabrati na $\lambda(S)$ načina, a skup T koji je sadržan u skupu S na $\binom{k-s}{t-s}$ načina. Imamo $\lambda(S) \cdot \binom{k-s}{t-s}$ elemenata. Kada izjednačimo oba načina prebrojavanja dobivamo

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

Kako $\lambda(S)$ ovisi o broju elemenata s, a ne ovisi o izboru skupa S označavamo ga s λ_s. □

Za $t = 2$ i $s = 1$ imamo broj blokova kroz proizvoljnu točku, tj.

$$\lambda_1 = \lambda \cdot \frac{\binom{v-1}{1}}{\binom{k-1}{1}} = \lambda \cdot \frac{v-1}{k-1} = r.$$

Za $t = 2$ i $s = 0$ imamo broj blokova koji sadrže prazan skup, $\lambda_0 = \lambda \cdot \frac{v(v-1)}{k(k-1)} = b$. Sad ćemo definirati još jednu generalizaciju dizajna, kod koje blokovi ne moraju biti jednake veličine.

Definicija 2.16. *Neka je λ pozitivan cijeli broj.* U parovima balansirani dizajn *(skraćeno PBD)* indeksa λ *je incidencijska struktura $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ tako da je $\mathcal{T} \neq \emptyset$, svaki $x \in \mathcal{T}$ je incidentan s više od λ blokova i za sve različite $x, y \in \mathcal{T}$ postoji točno λ blokova koji su incidentni s x i y.*

Možemo primijetiti da u parovima balansirani dizajn nije nužno dizajn, jer ne mora zadovoljavati drugo svojstvo u definiciji 2.1. To je struktura na kojoj ćemo definirati pojam rastavljivosti.

Primjer 2.17. *Incidencijska struktura $(\mathcal{T}, \mathcal{B})$ gdje je $\mathcal{T} = \{1, 2, 3\}$ i $\mathcal{B} = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$ je PBD indeksa 1.*

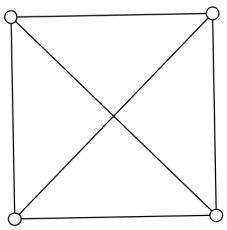
Sada ćemo se upoznati s incidencijskom strukturom koja je bliska našem poimanju geometrije ravnine.

Definicija 2.18. *Incidencijska struktura $\mathcal{A} = (\mathcal{T}, \mathcal{B}, I)$ naziva se* afinom ravninom*, ako su zadovoljeni aksiomi:*
(1) za svake dvije točke x, y postoji točno jedan pravac B tako da vrijedi xIB

i yIB
(2) za svaki pravac L *i svaku točku* a *koja nije incidentna s* L *postoji točno jedan pravac* M *takav da je* aIM *i* M *nema zajedničkih točaka s* L
(3) postoje tri različite nekolinearne točke.

Kod afine ravnine za blok koristimo naziv *pravac*. Na skupu pravaca $\mathcal{B}$ zadajemo relaciju paralelnosti $||$ tako da je $L||M$ ako i samo ako je $L = M$ ili L i M nemaju zajedničkih točaka.

Primjer 2.19. *Iz aksioma slijedi da afina ravnina na svakom pravcu ima barem dvije točke, a ukupno ima barem 4 točke i barem 6 pravaca. To možemo prikazati u obliku paralelograma s dijagonalama koje nemaju presječnu točku. Prema tome dijagonale su paralelni pravci. Vidimo da je zadovoljena definicija dizajna, pa je to primjer* 2-$(4, 2, 1)$ *dizajna.*



Slika 4: Afina ravnina reda 2

Već smo spomenuli da na skupu $\mathcal{B}$ imamo relaciju paralelnosti.

Propozicija 2.20. *Relacija paralelnosti na skupu pravaca* $\mathcal{B}$ *afine ravnine* $\mathcal{A}$ *je relacija ekvivalencije.*

Dokaz. Refleksivnost: $(\forall B \in \mathcal{B})$ $B||B$ jer je $B = B$.
Simetričnost: ako je $B_1||B_2$ tada B_1 i B_2 nemaju zajedničkih točaka. Slijedi da B_2 i B_1 nemaju zajedničkih, pa je $B_2||B_1$.
Tranzitivnost: iz $B_1||B_2$ i $B_2||B_3$ i primjenom simetričnosti imamo da B_2 nema zajedničkih točaka s B_1 i B_3. Po aksiomu (2) iz definicije afine ravnine svaka točka koja nije incidentna s B_2 je incidentna samo s jednim pravcem koji nema zajedničkih točaka s B_2. Prema tome B_1 i B_3 nemaju zajedničkih točaka, tj. $B_1||B_3$. □

Klase ekvivalencije su klase paralelnih pravaca. U prethodnom primjeru imamo tri para paralelnih pravaca, tj. tri paralelne klase s po 2 pravca. Ovo svojstvo će nam biti važno kada se upoznamo s rastavljivim dizajnima.

Recimo i to da je afina ravnina 2-dizajn s parametrima $(n^2, n, 1)$ gdje je n red dizajna (red dizajna je broj $n = r - \lambda$). Tako je primjer 2.19 afina ravnina reda 2. Prema propoziciji 2.12 afina ravnina je rezidualni dizajn simetričnog $(n^2 + n + 1, n + 1, 1)$ dizajna koji nazivamo *projektivnom ravninom reda* n. Fanova ravnina je projektivna ravnina reda 2. Tada je afina ravnina reda 2 rezidualni dizajn Fanove ravnine.

3 O pojmu rastavljivosti dizajna

Blok incidentan sa svim točkama dizajna nazivamo *potpuni blok*. U definiciji pojma rastavljivosti takve blokove tretiramo posebno.

Definicija 3.1. *Neka je* $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ *PBD indeksa* λ *i neka je* $\mathcal{C}$ *podskup skupa svih blokova* $\mathcal{B}$. *Skup* $\mathcal{C}$ *naziva se* klasa rastavljivosti *ako vrijedi:*
(i) skup $\mathcal{C}$ *sadrži samo nepotpune blokove i postoji pozitivni cijeli broj* $\alpha(\mathcal{C})$ *tako da je svaka točka sadržana u točno* $\alpha(\mathcal{C})$ *blokova skupa* $\mathcal{C}$*, ili*
(ii) skup $\mathcal{C}$ *se sastoji od jednog potpunog bloka. U tom slučaju je* $\alpha(\mathcal{C}) = 1$.
Particija skupa svih blokova $\mathcal{B}$ *u klase rastavljivosti naziva se* rastav *dizajna* $\boldsymbol{D}$.

Definicija 3.2. *Ako kroz svaku točku PBD-a indeksa* λ *prolazi konstantan broj blokova* r*, nazivamo ga* (r, λ)-dizajn.

Propozicija 3.3. *PBD indeksa* λ *dopušta rastav ako i samo ako je* (r, λ)*-dizajn.*

Dokaz. Ako PBD indeksa λ dopušta rastav $\mathcal{R}$, tada kroz svaku njegovu točku prolazi $r = \sum_{\mathcal{C} \in \mathcal{R}} \alpha(\mathcal{C})$ blokova. Po prethodnoj definiciji, PBD je (r, λ)-dizajn. Obratno, ako je PBD (r, λ)-dizajn, svaka njegova točka sadržana je u r blokova iz $\mathcal{B}$. Prema tome svaki (r, λ)-dizajn dopušta rastav koji sadrži jednu klasu rastavljivosti, tj. $\mathcal{C} = \mathcal{B}$. □

Definicija 3.4. *Klasa rastavljivosti* $\mathcal{C}$ *u parovima balansiranog dizajna* $\boldsymbol{D}$ *naziva se* klasa paralelnosti *ako je* $\alpha(\mathcal{C}) = 1$. *Particija skupa svih blokova dizajna* $\boldsymbol{D}$ *u klase paralelnosti naziva se* paralelizam dizajna $\mathbf{D}$. *Dizajn koji dopušta paralelizam naziva se* rastavljivi dizajn.

Incidencijska struktura iz primjera 2.17 je rastavljivi PBD indeksa 1. Svaka klasa paralelnosti sadrži jednočlani podskup i njegov komplement u skupu $\mathcal{T}$. U nastavku ćemo proučiti rastavljive 2-dizajne, tj. 2-dizajne koji dopuštaju paralelizam. Kao primjer rastavljivog 2-dizajna imamo već spomenute afine ravnine.

Propozicija 3.5. *Svaka afina ravnina je rastavljivi* 2-$(n^2, n, 1)$ *dizajn za neki* $n \in \mathbb{N}$, $n \geq 2$.

Dokaz. Već smo istaknuli da je afina ravnina 2-$(n^2, n, 1)$ dizajn gdje je n red dizajna. Kako je $n = r - \lambda$, a r broj blokova kroz svaku točku afine ravnine i λ broj blokova koji sadrže svake dvije točke, n je prirodan broj. Rekli smo da afina ravnina ima barem 4 točke. Kroz svake dvije točke prolazi jedan pravac, pa kroz svaku točku prolaze barem 3 pravca, tj. $n \geq 2$. U

propoziciji 2.20 dokazali smo da je relacija paralelnosti na skupu pravaca relacija ekvivalencije. Klase ekvivalencije su klase paralelnih pravaca. Svaka točka pripada točno jednom pravcu iz svake klase. Prema tome svaka afina ravnina dopušta paralelizam, pa je rastavljivi 2-$(n^2, n, 1)$ dizajn. □

Još jedan primjer je incidencijska struktura $(\mathcal{T}, \mathcal{B})$ gdje je $\mathcal{T}$ skup kardinalnosti $2k$ i $\mathcal{B}$ skup svih k-članih podskupova skupa $\mathcal{T}$. Primijetimo da za $k = 2$ imamo afinu ravninu reda 2. Općenito, ovo je 2-$(2k, k, \binom{2k-2}{k-2})$ dizajn.

Propozicija 3.6. *Sve klase paralelnosti rastavljivog* 2-(v, k, λ) *dizajna imaju istu kardinalnost* v/k.

Dokaz. Svaka točka je sadržana u jednom bloku iz svake klase paralelnosti. Prema tome jedna klasa paralelnosti sadrži sve točke. Kako svi blokovi imaju istu kardinalnost k, slijedi da sve klase imaju kardinalnost v/k. □

Možemo se uvjeriti na primjeru afine ravnine reda 2 tj. 2-$(4, 2, 1)$ dizajna. Na početku smo rekli da u svakoj klasi paralelnosti ima dva pravca, a to slijedi iz $v = 4$ i $k = 2$.

Propozicija 3.7. *Ako postoji rastavljivi* 2-(v, k, λ) *dizajn, tada je* $\lambda(v-1) \equiv 0 (mod\ k-1)$ *i* $v \equiv 0 (mod\ k)$.

Dokaz. Prvi dio uvjeta slijedi iz identiteta $\lambda(v-1) = r(k-1)$. Drugi dio uvjeta slijedi iz propozicije 3.6. □

Sljedeća propozicija pokazuje da su za $k = 2$ uvjeti propozicije 3.7 dovoljni za postojanje rastavljivog 2-dizajna. U dokazu će nam trebati još jedan pojam koji do sada nismo definirali.

Definicija 3.8. Latinski kvadrat reda n *je* $n \times n$ *matrica popunjena elementima* n*-članog skupa* X *takva da je svaki redak i stupac permutacija od* X.

Lema 3.9. *Za svaki parni* n *postoji simetrični latinski kvadrat* L *reda* n *takav da je za svaki* i, j, $L(i, j) = L(j, i)$ *i* $L(i, i) = n$.

Dokaz. Neka je n paran pozitivan cijeli broj. Definiramo latinski kvadrat A reda $n-1$ s $A(i, j) = r$ ako i samo ako $i + j \equiv r (\text{mod } n-1)$ i $1 \leq r \leq n-1$. Zbog komutativnosti zbrajanja A je simetričan. Za $i = j$, $1 \leq i, j \leq n-1$, $i + j$ su parni brojevi koji pri dijeljenju s $n-1$ daju $n-1$ različitih ostataka.

Prema tome, A na dijagonali ima sve različite brojeve. Sada definiramo latinski kvadrat L reda n na sljedeći način:

$$L(i,j) = \begin{cases} A(i,j) & \text{ako } i \neq j, i \neq n, j \neq n, \\ A(j,j) & \text{ako } i = n, j \neq n, \\ A(i,i) & \text{ako } i \neq n, j = n, \\ n & \text{ako } i = j. \end{cases}$$

Kako je A simetričan i na dijagonali ima različite brojeve, ovako definiran L je simetrični latinski kvadrat s brojevima n na dijagonali. □

Propozicija 3.10. *Za svaki parni v i svaki $\lambda \geq 1$ postoji rastavljivi 2-$(v, 2, \lambda)$ dizajn.*

Dokaz. Dovoljno je pokazati da postoji rastavljivi 2-$(v, 2, 1)$ dizajn. Ako je $\lambda > 1$, uzmemo λ kopija rastavljivog 2-$(v, 2, 1)$ dizajna i tako dobijemo rastavljivi 2-$(v, 2, \lambda)$ dizajn. Neka je v paran, $|\mathcal{T}| = \{1, 2, ..., v\}$ i $\mathcal{B}$ skup svih dvočlanih podskupova od $\mathcal{T}$. Incidencijska struktura $\mathbf{D} = (\mathcal{T}, \mathcal{B})$ je 2-$(v, 2, 1)$ dizajn. Još trebamo pokazati da je $\mathbf{D}$ rastavljivi dizajn. Neka je L simetrični latinski kvadrat reda v gdje je $L(i,i) = v$ za $i = 1, 2, ..., v$. Prema prethodnoj lemi postoji takav latinski kvadrat. Za $k = 1, 2, ..., v-1$, neka je $\mathcal{C}_k = \{\{i,j\} \in \mathcal{B} : L(i,j) = k\}$. Za svaki $\{i,j\} \in \mathcal{B}$, $L(i,j) = L(j,i) \neq v$, pa je skup $\mathcal{C}_k$ dobro definiran. Svi podskupovi $\{i,j\}$ od $\mathcal{C}_k$ imaju međusobno različite elemente, zato što kod latinskog kvadrata svi retci i stupci nemaju ponavljanja elemenata. U podskupovima $\{i,j\}$ su sadržani svi elementi skupa $\mathcal{T}$, pa su skupovi $\mathcal{C}_k$ klase paralelnosti dizajna $\mathbf{D}$. Dakle, $\mathbf{D}$ dopušta paralelizam $\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_{v-1}$, pa je rastavljivi dizajn. □

Primjer rastavljivog 2-$(v, 2, 1)$ dizajna može se naći gotovo na svim sportskim natjecanjima gdje u skupini igra paran broj ekipa (npr. svjetsko prvenstvo u nogometu). Ekipe predstavljaju točke dizajna, dvije ekipe koje igraju međusobno predstavljaju 2-člani blok. Paralelne klase opisuju kola (runde) natjecanja. U svakom kolu svaka ekipa igra jednu utakmicu. Razmotrimo sada postojanje rastavljivog 2-$(v, 3, 1)$ dizajna. Prisjetimo se Kirkmanova problema:
Petnaest učenica šeta svaki dan, u pet redova po tri učenice. Mogu li se učenice svrstati tako da se u sedam dana svake dvije učenice nađu zajedno u istom redu točno jedanput?
Uočavamo da tražimo rastavljivi 2-$(15, 3, 1)$ dizajn. Učenice predstavljaju točke dizajna, redovi u kojima šetaju predstavljaju blokove dizajna, a dani šetnje predstavljaju klase paralelnosti. Svaka klasa paralelnosti ima 5 blokova.

Iz propozicije 3.7 slijedi da ako postoji 2-$(v, 3, 1)$ dizajn, tada je $v \equiv 1 (\mathrm{mod}\ 2)$ i $v \equiv 0 (\mathrm{mod}\ 3)$. Ova dva uvjeta nam daju nužan uvjet za postojanje rastavljivog 2-$(v, 3, 1)$ dizajna, $v \equiv 3 (\mathrm{mod}\ 6)$. Prema sljedećem teoremu, taj uvjet je ujedno dovoljan.

Teorem 3.11. *Ako je* $v \equiv 3 (mod\ 6)$*, tada postoji rastavljivi* 2-$(v, 3, 1)$ *dizajn.*

Dokaz ovog teorema je izvan dosega naših dosadašnjih razmatranja, pa ćemo ga izostaviti. Rastavljive 2-$(v, 3, 1)$ dizajne nazivamo *Kirkmanovi sustavi trojki*. Zaključujemo da je moguća šetnja iz Kirkmanova problema.

4 Fisherova i Boseova nejednakost

Teorem 4.1. (Neuniformna Fisherova nejednakost). *Neka je $\mathcal{T}$ neprazan konačan skup i $\mathcal{B}$ familija podskupova od $\mathcal{T}$ takva da presjek bilo koja dva različita skupa od $\mathcal{B}$ ima istu kardinalnost. Tada je $|\mathcal{B}| \leq |\mathcal{T}|$.*

Dokaz. Neka je λ pozitivni cijeli broj takav da $|A \cap B| = \lambda$, za $A \neq B$ u $\mathcal{B}$. Tada je za $A \in \mathcal{B}$, $|A| \geq \lambda$. Ako je $|A| = \lambda$, tada je presjek svaka dva različita skupa u familiji $\mathcal{B}$ skup A. Ako skupovima u $\mathcal{B}$ oduzmemo skup A, dobivamo familiju u parovima disjunktnih podskupova skupa $\mathcal{T}\backslash A$. Kardinalnost te familije ne prelazi $|\mathcal{T}\backslash A| + 1$, tj. $|\mathcal{B}| \leq |\mathcal{T}\backslash A| + 1 = |\mathcal{T}| - \lambda + 1 \leq |\mathcal{T}|$.
Sada pretpostavimo da je $|A| > \lambda$ za svaki $A \in \mathcal{B}$. U ovom dijelu dokaza koristit ćemo linearnu algebru. Kako je $\mathcal{B}$ konačna familija podskupova od $\mathcal{T}$, odabrat ćemo odgovarajući konačnodimenzionalni vektorski prostor i elementima familije $\mathcal{B}$ pridružiti vektore iz tog prostora. Neka je $\mathcal{T} = \{1, 2, ..., v\}$. Svaki podskup X od $\mathcal{T}$ zamijenimo uređenom v-torkom $(x_1, x_2, ..., x_v)$ gdje je $x_i = 1$ ako je $i \in X$ i $x_i = 0$ ako $i \notin X$. Sada definiramo vektorski prostor V nad $\mathbb{Q}$ linearnih polinoma $a_0 + a_1x_1 + a_2x_2 + ... + a_vx_v$. Svakom podskupu A od $\mathcal{B}$ pridružimo linearni polinom $f_A = \sum_{i \in A} x_i - \lambda$. Tada je $f_A(X) = \sum_{i \in A \cap X} 1 - \lambda = |A \cap X| - \lambda$ za $X \subseteq \mathcal{T}$. Za svaki $A, B \in \mathcal{B}$ vrijedi:

$$f_A(B) = \begin{cases} 0, & \text{ako je } B \neq A, \\ |B| - \lambda, & \text{ako je } B = A. \end{cases} \tag{4}$$

Skup $\{f_A : A \in \mathcal{B}\}$ je podskup vektorskog prostora V. Pokazat ćemo da je linearno neovisan. Primijenimo obje strane jednakosti $\sum_{A \in \mathcal{B}} \alpha_A f_A = 0$ u proizvoljnom $B \in \mathcal{B}$ i koristeći (4) dobivamo $\alpha_B(|B| - \lambda) = 0$. Kako je $|B| > \lambda$ za svaki $B \in \mathcal{B}$, $\alpha_B = 0$. Svi skalari α_A, $A \in \mathcal{B}$ su jednaki nuli, pa je skup $\{f_A : A \in \mathcal{B}\}$ linearno neovisan. Pretpostavimo da se konstantan polinom 1 može prikazati kao linearna kombinacija polinoma f_A, $A \in \mathcal{B}$, tj. da vrijedi:

$$1 = \sum_{A \in \mathcal{B}} \alpha_A f_A, \tag{5}$$

za neke koeficijente α_A. Primijenimo obje strane jednakosti (5) u $B \in \mathcal{B}$ i koristeći (4), dobivamo $\alpha_B(|B| - \lambda) = 1$. Odatle je $\alpha_A = \frac{1}{|A| - \lambda}$. Uvrstimo α_A u (5) i imamo

$$1 = \sum_{A \in \mathcal{B}} \frac{1}{|A| - \lambda} f_A.$$

Prethodnu jednakost primijenimo u praznom skupu. Kako je $f_A(\emptyset) = |A \cap$

$\emptyset| - \lambda = -\lambda$, dobivamo

$$1 = \sum_{A \in \mathcal{B}} \frac{-\lambda}{|A| - \lambda}.$$

To ne može vrijediti, jer je desna strana jednakosti negativna. Prema tome skup $\{f_A : A \in \mathcal{B}\} \cup \{1\}$ je linearno neovisan. Kako je skup $\{f_A : A \in \mathcal{B}\} \cup \{1\}$ podskup od V i $\dim V = |\mathcal{T}|+1$ slijedi da je $|\mathcal{B}|+1 \leq |\mathcal{T}|+1$, tj. $|\mathcal{B}| \leq |\mathcal{T}|$. $\square$

Da bismo neuniformnu Fisherovu nejednakost primijenili na PBD-ove upoznat ćemo se s još jednim pojmom.

Definicija 4.2. Dual *incidencijske strukture* $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ *je incidencijska struktura* $\boldsymbol{D}^{\tau} = (\mathcal{B}, \mathcal{T}, I^{\tau})$ *koju dobijemo zamjenom uloge točaka i blokova. Pritom je* $I^{\tau} = \{(B, x) | (x, B) \in I\}$.

Dual PBD-a je incidencijska struktura kod koje se bilo koja dva različita bloka sijeku u točno λ točaka. Ta incidencijska struktura zadovoljava neuniformnu Fisherovu nejednakost. Tada za PBD-ove vrijedi Fisherova nejednakost (generalizacija teorema 2.8): broj točaka ne prelazi broj blokova, tj. $|\mathcal{B}| \geq |\mathcal{T}|$. Ako PBD dopušta rastav, tada vrijedi i poboljšanje Fisherove nejednakosti poznato kao *Boseova nejednakost*. Da bismo dobili Boseovu nejednakost, opet ćemo koristiti linearnu algebru.
Neka je $\mathbf{D} = (\mathcal{T}, \mathcal{B}, I)$ PBD indeksa λ koji dopušta skup u parovima disjunktnih klasa rastavljivosti $\mathcal{R}$. Svakom bloku $B \in \mathcal{B}$ pridružimo varijablu x_B. Dizajnu $\mathbf{D}$ pridružimo vektorski prostor $Pol(\mathbf{D})$ linearnih polinoma s racionalnim koeficijentima u varijablama x_B. Za svaki linearni polinom $f = \sum_{B \in \mathcal{B}} a_B x_B + c$ definiramo djelovanje na skupu točaka $\mathcal{T}$ sa:

$$f(x) = \sum_{B \ni x} a_B + c, \text{ za svaki } x \in \mathcal{T}. \tag{6}$$

Za svaku točku $x \in \mathcal{T}$ definiramo polinom $f_x \in Pol(\mathbf{D})$ s

$$f_x = \sum_{B \ni x} x_B - \lambda. \tag{7}$$

Tada za sve točke $x, y \in \mathcal{T}$ vrijedi

$$f_x(y) = \begin{cases} 0 & \text{ako } x \neq y, \\ r(x) - \lambda & \text{ako } x = y. \end{cases} \tag{8}$$

Prema (6) imamo $f_x(y) = \sum_{B \ni x,y} 1 - \lambda$. Po definiciji PBD-a svake dvije točke su sadržane u λ blokova, pa je $f_x(y) = \lambda - \lambda = 0$. Kako je $r(x)$ broj

blokova iz $\mathcal{B}$ koji sadrže točku x, iz (6) slijedi $f_x(x) = \sum_{B \ni x} 1 - \lambda = r(x) - \lambda$. Za svaku klasu rastavljivosti $\mathcal{C} \in \mathcal{R}$, definiramo polinom $g_{\mathcal{C}} \in Pol(\mathbf{D})$:

$$g_{\mathcal{C}} = \sum_{B \in \mathcal{C}} x_B - \alpha(\mathcal{C}). \tag{9}$$

Tada je $g_{\mathcal{C}}(x) = 0$ za svaki $x \in \mathcal{T}$, jer iz (6) slijedi $g_{\mathcal{C}}(x) = \sum_{x \in B \in \mathcal{C}} 1 - \alpha(\mathcal{C}) = \alpha(\mathcal{C}) - \alpha(\mathcal{C}) = 0$.

Propozicija 4.3. *Skup polinoma* $S = \{f_x : x \in \mathcal{T}\} \cup \{g_{\mathcal{C}} : \mathcal{C} \in \mathcal{R}\}$ *je linearno neovisan.*

Dokaz. Pretpostavimo da je

$$\sum_{x \in \mathcal{T}} a_x f_x + \sum_{\mathcal{C} \in \mathcal{R}} b_{\mathcal{C}} g_{\mathcal{C}} = 0, \ a_x, b_{\mathcal{C}} \in \mathbb{Q}.$$

Na obe strane jednakosti djelujemo u točki $y \in \mathcal{T}$, te koristeći (8) i $g_{\mathcal{C}}(y) = 0$ dobivamo $a_y(r(y) - \lambda) = 0$. Kako je po definiciji PBD-a svaka točka incidentna s više od λ blokova, slijedi $a_y = 0$ za svaki $y \in \mathcal{T}$. Sada imamo

$$\sum_{\mathcal{C} \in \mathcal{R}} b_{\mathcal{C}} g_{\mathcal{C}} = 0.$$

Ako je $B \in \mathcal{C}$, tada je koeficijent na lijevoj strani ove jednakosti uz x_B jednak $b_{\mathcal{C}}$. To znači da je $b_{\mathcal{C}} = 0$ za svaki $\mathcal{C} \in \mathcal{R}$. Prema tome svi skalari su jednaki nuli, pa je skup S linearno neovisan. □

Teorem 4.4. (Boseova nejednakost). *Neka je* $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ *PBD indeksa* λ *koji dopušta skup* $\mathcal{R}$ *u parovima disjunktnih klasa rastavljivosti. Tada vrijedi* $|\mathcal{B}| \geq |\mathcal{T}| + |\mathcal{R}| - 1$.

Dokaz. Iz definicije vektorskog prostora $Pol(\mathbf{D})$ slijedi $\dim Pol(\mathbf{D}) = |\mathcal{B}| + 1$, jer je dimenzija vektorskog prostora jednaka broju elemenata u bazi vektorskog prostora. Zbog linearne neovisnosti skup $\{f_x : x \in \mathcal{T}\} \cup \{g_{\mathcal{C}} : \mathcal{C} \in \mathcal{R}\}$ generira potprostor vektorskog prostora $Pol(\mathbf{D})$ dimenzije $|\{f_x : x \in \mathcal{T}\} \cup \{g_{\mathcal{C}} : \mathcal{C} \in \mathcal{R}\}| = |\mathcal{T}| + |\mathcal{R}|$. Dimenzija potprostora vektorskog prostora je manja ili jednaka dimenziji vektorskog prostora, tj. $|\mathcal{T}| + |\mathcal{R}| \leq |\mathcal{B}| + 1$. Odatle slijedi $|\mathcal{B}| \geq |\mathcal{T}| + |\mathcal{R}| - 1$. □

Kako svaki (r, λ) dizajn dopušta rastav koji sadrži jednu klasu rastavljivosti, iz Boseove nejednakosti slijedi Fisherova nejednakost za (r, λ) dizajne. Kod afine ravnine imamo $|\mathcal{T}| = n^2$, $|\mathcal{B}| = n^2 + n$. Znamo da je svaka točka sadržana u jednom bloku iz svake klase paralelnosti, a kroz svaku točku prolazi $n + 1$ blokova tj. imamo $n + 1$ klasa paralelnosti. Tako je $|\mathcal{R}| = n + 1$.

Uočavamo da za afinu ravninu imamo jednakost u Boseovoj nejednakosti. Kako bismo dobili nužan i dovoljan uvjet jednakosti u Boseovoj nejednakosti upoznat ćemo pojam afinog rastava.

Definicija 4.5. *Neka je* $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ *PBD indeksa* λ. *Rastav* $\mathcal{R}$ *dizajna* $\boldsymbol{D}$ *naziva se* afinim *ako kardinalnost svakog bloka i kardinalnost presjeka bilo koja dva različita bloka zavise samo o klasama rastavljivosti kojima ti blokovi pripadaju.*

Teorem 4.6. *Ako je* $\mathcal{R}$ *afini rastav u parovima balansiranog dizajna* $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$, *tada je* $|\mathcal{B}| = |\mathcal{T}| + |\mathcal{R}| - 1$.

Dokaz. Neka je $\mathbf{D} = (\mathcal{T}, \mathcal{B}, I)$ PBD koji dopušta afini rastav $\mathcal{R} = \{\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_t\}$. Ako $\mathbf{D}$ ima jedan ili više potpunih blokova, tada uklanjanjem njih smanjuju se $|\mathcal{B}|$ i $|\mathcal{R}|$ za istu vrijednost. Stoga ćemo pretpostaviti da $\mathbf{D}$ nema potpuni blok. Neka je $|B| = k_i$ za svaki blok $B \in \mathcal{C}_i$ i $|A \cap B| = m_{ij}$ za svaka dva različita bloka $A \in \mathcal{C}_i$ i $B \in \mathcal{C}_j$. Neka je $\langle S \rangle$ potprostor vektorskog prostora $Pol(\mathbf{D})$ generiran polinomima $f_x, x \in \mathcal{T}$ i $g_i = g_{\mathcal{C}i}, 1 \leq i \leq t$. Prema propoziciji 4.3 ti polinomi su linearno neovisni, tako je $\dim\langle S \rangle = |\mathcal{T}| + |\mathcal{R}|$. Dovoljno je dokazati da je $\langle S \rangle = Pol(\mathbf{D})$, jer je $\dim Pol(\mathbf{D}) = |\mathcal{B}| + 1$. Promotrimo polinom

$$h = \sum_{x \in \mathcal{T}} f_x - \sum_{i=1}^{t} k_i g_i. \tag{10}$$

Zapišimo h u obliku $h = \sum_B a_B x_B + c$. Neka je $A \in \mathcal{C}_j, 1 \leq j \leq t$. Iz (10) slijedi $a_A = |A| - k_j$. Kako je $A \in \mathcal{C}_j$ imamo $|A| = k_j$, što znači $a_A = 0$ i h je konstanta. Kako su polinomi f_x, g_i linearno neovisni, $h \neq 0$, i stoga su svi konstantni polinomi u potprostoru $\langle S \rangle$. Neka je $A \in \mathcal{C}_j$ i $1 \leq j \leq t$. Sada promotrimo polinom

$$h_A = \sum_{x \in A} f_x - \sum_{i=1}^{t} m_{ij} g_i. \tag{11}$$

Neka je $h_A = \sum_B a_B x_B + c$. Iz (11) slijedi $a_A = |A| - m_{jj} = k_j - m_{jj}$. Ako je $k_j - m_{jj} = 0$, tada je $|A| = |B| = |A \cap B|$ za svaka dva bloka A i B u $\mathcal{C}_j$. To je kontradikcija s pretpostavkom da $\mathbf{D}$ nema potpuni blok. Dakle, $a_A \neq 0$. Neka je $B \in \mathcal{C}_k$ različit od A. Tada iz (11) vrijedi $a_B = |A \cap B| - m_{kj} = 0$. Sada imamo $h_A = a_A x_A + c$. Konstanta c je u $\langle S \rangle$ i $a_A \neq 0$, pa je $x_A \in \langle S \rangle$. To vrijedi za svaki blok A, tj. $\langle S \rangle = Pol(\mathbf{D})$. □

Lema 4.7. *Neka je* $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ *PBD indeksa* λ *i* $\mathcal{R}$ *skup u parovima disjunktnih klasa rastavljivosti od* $\boldsymbol{D}$. *Ako je* $|\mathcal{B}| = |\mathcal{T}| + |\mathcal{R}| - 1$, *tada je* $\mathcal{R}$ *rastav od* $\boldsymbol{D}$.

Dokaz. Neka je $|\mathcal{B}| = |\mathcal{T}| + |\mathcal{R}| - 1$. Skup $S = \{f_x : x \in \mathcal{T}\} \cup \{g_C : \mathcal{C} \in \mathcal{R}\}$ je baza vektorskog prostora $Pol(\mathbf{D})$, jer svaki linearno neovisan skup čiji je broj elemenata jednak dimenziji vektorskog prostora je baza. Svaki linearni polinom iz $Pol(\mathbf{D})$ ima jedinstven prikaz u bazi $\{f_x : x \in \mathcal{T}\} \cup \{g_C : \mathcal{C} \in \mathcal{R}\}$. Za $A \in \mathcal{B}$ prikažimo x_A u toj bazi:

$$x_A = \sum_{x \in \mathcal{T}} a_x^A f_x + \sum_{\mathcal{C} \in \mathcal{R}} b_{\mathcal{C}}^A g_{\mathcal{C}}. \tag{12}$$

Obje strane jednakosti (12) primijenimo u točki $y \in \mathcal{T}$ i dobivamo

$$a_y^A = \begin{cases} \frac{1}{r(y)-\lambda} & , \text{ako } y \in A, \\ 0 & , \text{ako } y \notin A. \end{cases} \tag{13}$$

Sada (13) uvrstimo u (12)

$$x_A = \sum_{x \in A} \frac{f_x}{r(x) - \lambda} + \sum_{\mathcal{C} \in \mathcal{R}} b_{\mathcal{C}}^A g_{\mathcal{C}}. \tag{14}$$

Pretpostavimo da skup $\mathcal{R}$ nije particija skupa svih blokova $\mathcal{B}$. Neka blok B ne pripada ni jednoj klasi rastavljivosti u $\mathcal{R}$ i neka je blok A različit od B. Uspoređujući koeficijente uz x_B na obe strane jednakosti (14) dobivamo

$$0 = \sum_{x \in A \cap B} \frac{1}{r(x) - \lambda}. \tag{15}$$

Kako je $r(x) - \lambda > 0$ za svaku točku $x \in \mathcal{T}$, (15) implicira da je $A \cap B = \emptyset$, za svaki blok A različit od B. To je nemoguće, jer kroz svaku točku od $\mathbf{D}$ prolaze barem dva bloka. Dakle, blok B pripada nekoj klasi rastavljivosti u $\mathcal{R}$. Prema tome skup $\mathcal{R}$ je particija skupa svih blokova $\mathcal{B}$, tj. rastav od $\mathbf{D}$. □

Ovu ćemo lemu iskoristiti da dobijemo dovoljan uvjet da je familija skupova s konstantnom veličinom presjeka skup blokova simetričnog dizajna.

Propozicija 4.8. *Neka su v i λ pozitivni cijeli brojevi i neka je $\mathcal{B}$ familija od v podskupova skupa $\mathcal{T}$ kojeg je kardinalnost v tako da je $|A \cap B| = \lambda$ za različite $A, B \in \mathcal{B}$ i $|B| > \lambda$ za svaki $B \in \mathcal{B}$. Pretpostavimo još da postoji i neprazni podskup Z skupa $\mathcal{T}$ i pozitivni cijeli broj k takav da je $|B \cap Z| = k$ za svaki $B \in \mathcal{B}$. Tada je $Z = \mathcal{T}$ i $(\mathcal{T}, \mathcal{B})$ je simetrični (v, k, λ) dizajn.*

Dokaz. Neka je $\mathbf{D}$ dualna incidencijska struktura od $(\mathcal{T}, \mathcal{B})$. Kako je $|B| > \lambda$ za svaki $B \in \mathcal{B}$, $\mathbf{D}$ je PBD indeksa λ. Označimo s A_x blok od $\mathbf{D}$ koji korespondira točki $x \in \mathcal{T}$. Tada je $A_x = \{B \in \mathcal{B} : x \in B\}$. Kako je $|B \cap Z| = k$ za svaki $B \in \mathcal{B}$, svaka točka u $\mathbf{D}$ sadržana je u k blokova iz skupa $\mathcal{C} = \{A_x : x \in Z\}$. Tada je $\mathcal{C}$ klasa rastavljivosti u $\mathbf{D}$. Kako $\mathbf{D}$ ima $v + |\mathcal{R}| - 1$ blokova gdje $\mathcal{R}$ sadrži jedan potpuni blok $\{\mathcal{C}\}$, iz prethodne leme slijedi da je $\mathcal{R}$ rastav od $\mathbf{D}$. Tada $\{\mathcal{C}\}$ sadrži sve blokove A_x od $\mathbf{D}$, što korespondira svim točkama skupa $\mathcal{T}$. Stoga je $Z = \mathcal{T}$, što dalje implicira da svi skupovi u familiji $\mathcal{B}$ imaju kardinalnost k. Prema tome $(\mathcal{T}, \mathcal{B})$ je simetrični (v, k, λ) dizajn. □

Sljedeći teorem karakterizira dizajne koji dostižu jednakost u Boseovoj nejednakosti.

Teorem 4.9. *Neka je $\boldsymbol{D} = (\mathcal{T}, \mathcal{B}, I)$ PBD indeksa λ i $v = |\mathcal{T}|$. Neka je $\mathcal{R}$ rastav od $\boldsymbol{D}$ takav da je $|\mathcal{B}| = v + |\mathcal{R}| - 1$ i neka je r broj blokova koji prolaze kroz svaku točku $x \in \mathcal{T}$. Tada vrijedi:*
(i) $\mathcal{R}$ je afini rastav od $\boldsymbol{D}$;
(ii) za svaka dva različita bloka A i B u klasi rastavljivosti $\mathcal{C} \in \mathcal{R}$, $|A \cap B| = k(\mathcal{C}) - r + \lambda$, gdje je $k(\mathcal{C})$ kardinalnost svakog bloka u $\mathcal{C}$;
(iii) za svaka dva bloka A i B u različitim klasama rastavljivosti $\mathcal{C}_1$ i $\mathcal{C}_2$, $|A \cap B| = k(\mathcal{C}_1)k(\mathcal{C}_2)/v$;
(iv) za svaku klasu rastavljivosti $\mathcal{C} \in \mathcal{R}$, $k(\mathcal{C})|\mathcal{C}| = v\alpha(\mathcal{C})$;
(v) dualna incidencijska struktura svakoj klasi rastavljivosti $\mathcal{C} \in \mathcal{R}$ je 2-$(|\mathcal{C}|, \alpha(\mathcal{C}), k(\mathcal{C}) - r + \lambda)$ dizajn;
(vi) $\mathcal{R}$ je jedinstveni afini rastav od $\boldsymbol{D}$.

Dokaz. Kako je $|\mathcal{B}| = v + |\mathcal{R}| - 1$, isto kao u lemi 4.7 skup $\{f_x : x \in \mathcal{T}\} \cup \{g_{\mathcal{C}} : \mathcal{C} \in \mathcal{R}\}$ je baza vektorskog prostora $Pol(\mathbf{D})$. Prema propoziciji 3.3, $\mathbf{D}$ je (r, λ)-dizajn. Iz jednakosti (14) slijedi

$$(r - \lambda)x_A = \sum_{x \in A} f_x - \sum_{\mathcal{C} \in \mathcal{R}} b_{\mathcal{C}}^A g_{\mathcal{C}}. \tag{16}$$

Za svaki blok B neka je $\mathcal{C}(B)$ klasa rastavljivosti koja sadrži blok B. Uspoređujući koeficijente uz x_A na obe strane jednakosti (16) dobivamo

$$b_{\mathcal{C}(A)}^A = |A| - r + \lambda. \tag{17}$$

Neka su A i B dva različita bloka. Uspoređujući koeficijente uz x_B na obje strane jednakosti (16) dobivamo

$$b_{\mathcal{C}(B)}^A = |A \cap B|. \tag{18}$$

Ako je $\mathcal{C}(A) = \mathcal{C}(B)$, tada iz (17) i (18) slijedi

$$|A| - r + \lambda = |A \cap B|. \tag{19}$$

Zamjenom A i B dobivamo $|B| - r + \lambda = |A \cap B|$, pa je $|A| = |B|$. Time smo dokazali da bilo koja dva bloka u istoj klasi rastavljivosti imaju istu kardinalnost. Sada nam (19) implicira (ii). Kako je svaka točka sadržana u $\alpha(\mathcal{C})$ blokova od $\mathcal{C}$ i prema (ii) presjek svaka dva različita bloka u $\mathcal{C}$ je $k(\mathcal{C}) - r + \lambda$, vrijedi tvrdnja (v).
Neka su $\mathcal{C}_1$ i $\mathcal{C}_2$ dvije različite klase rastavljivosti. Fiksiramo blok $A \in \mathcal{C}_1$ i prebrojavamo na dva načina parove (x, B) gdje je $B \in \mathcal{C}_2$ i $x \in A \cap B$. Kroz svaku točku koja leži na bloku A prolazi $\alpha(\mathcal{C}_2)$ blokova iz $\mathcal{C}_2$. S druge strane iz (18) imamo da svaki blok $B \in \mathcal{C}_2$ presjeca blok A u istom broju točaka koji je jednak $b^A_{\mathcal{C}_2(B)}$. Sada dobivamo

$$k(\mathcal{C}_1)\alpha(\mathcal{C}_2) = |\mathcal{C}_2| \cdot |A \cap B|. \tag{20}$$

Prebrojimo na dva načina parove (B, x) gdje je $B \in \mathcal{C}, x \in B$. Kardinalnost svakog bloka u $\mathcal{C}$ je $k(\mathcal{C})$ i u $\mathcal{C}$ imamo $|\mathcal{C}|$ blokova. S druge strane svaka točka je sadržana u $\alpha(\mathcal{C})$ blokova od $\mathcal{C}$ i ukupan broj točaka je v. Prema tome $k(\mathcal{C})|\mathcal{C}| = \alpha(\mathcal{C})v$, tj. vrijedi tvrdnja (iv). Tvrdnja (iii) slijedi iz (iv) i jednakosti (20). Kako svi blokovi iz iste klase rastavljivosti imaju istu kardinalnost i prema (ii) i (iii) zadovoljena je definicija afinog rastava, pa vrijedi tvrdnja (i). Još nam preostaje dokazati tvrdnju (vi).
Pretpostavimo da postoji još jedan afini rastav $\mathcal{R}'$ od $\mathbf{D}$ koji je različit od $\mathcal{R}$. Neka blokovi B_1 i B_2 pripadaju istoj klasi rastavljivosti $\mathcal{C} \in \mathcal{R}$ i različitim klasama rastavljivosti $\mathcal{C}_1$ i $\mathcal{C}_2$ u $\mathcal{R}'$. Prema (ii) vrijedi $|B_1 \cap B_2| = k - r + \lambda$ gdje je $k = k(\mathcal{C})$ (B_1 i B_2 su dva različita bloka u $\mathcal{C}$). Kako je $k(\mathcal{C}_1) = k(\mathcal{C}_2) = k$, tada prema (iii) slijedi $|B_1 \cap B_2| = k^2/v$ (B_1 i B_2 su blokovi u različitim klasama rastavljivosti $\mathcal{C}_1$ i $\mathcal{C}_2$). Sada imamo

$$k - r + \lambda = \frac{k^2}{v}. \tag{21}$$

Formirajmo particiju $\mathcal{R}''$ skupa $\mathcal{B}$ zamjenom klasa rastavljivosti $\mathcal{C}_1$ i $\mathcal{C}_2$ u $\mathcal{R}'$ s $\mathcal{C}' = \mathcal{C}_1 \cup \mathcal{C}_2$. Pokazat ćemo da je $\mathcal{R}''$ također afini rastav od $\mathbf{D}$. Neka su A i B dva različita bloka u $\mathcal{B}$. Ako $A, B \in \mathcal{C}_1$ ili $A, B \in \mathcal{C}_2$ tada prema (ii), $|A \cap B| = k - r + \lambda$. Ako je $A \in \mathcal{C}_1$ i $B \in \mathcal{C}_2$, prema (iii), $|A \cap B| = k^2/v$. Koristeći (21) zaključujemo, $|A \cap B| = k - r + \lambda$ za sve $A \neq B$ u $\mathcal{C}'$. Ako je $A \in \mathcal{C}'$ i $B \notin \mathcal{C}'$, prema (iii), $|A \cap B| = k|B|/v$. Znači kardinalnost presjeka bilo koja dva različita bloka u $\mathcal{B}$ zavisi samo o njihovim klasama rastavljivosti u $\mathcal{R}''$. Po definiciji 4.5, $\mathcal{R}''$ je afini rastav od $\mathbf{D}$. Iz teorema 4.6 slijedi $|\mathcal{R}''| = |\mathcal{R}'|$, što je kontradikcija s načinom na koji smo formirali skup $\mathcal{R}''$. □

5 Afino α-rastavljivi dizajni

Definicija 5.1. *Neka je α pozitivni cijeli broj.* Afino α-rastavljivi u parovima balansirani dizajn *je PBD koji dopušta afini rastav $\mathcal{R}$ takav da je $\alpha(\mathcal{C}) = \alpha$ za sve $\mathcal{C} \in \mathcal{R}$.*

Sljedeći teorem nam daje nužne uvjete za parametre afino α-rastavljivog PBD-a.

Teorem 5.2. *Neka je $\boldsymbol{D} = (\mathcal{T}, \mathcal{B})$ afino α-rastavljivi PBD indeksa λ i $\mathcal{R}$ njegov afini rastav. Ako je $\alpha = 1$ i $\boldsymbol{D}$ nema potpuni blok, tada je $\boldsymbol{D}$ 2-dizajn. Ako $\boldsymbol{D}$ nije 2-dizajn, tada postoje pozitivni cijeli brojevi u, m, c_1 i c_2 takvi da vrijedi:*
(i) $r - \lambda = m\alpha$ i $v = mu$;
(ii) svaka klasa rastavljivosti u $\mathcal{R}$ ima kardinalnost c_1 ili c_2;
(iii) $c_1 + c_2 = u + 1$ i $c_1 c_2 = u\alpha$;
(iv) svi blokovi svake klase rastavljivosti kardinalnosti c_1 imaju kardinalnost $k_1 = mc_2$ i svi blokovi svake klase rastavljivosti kardinalnosti c_2 imaju kardinalnost $k_2 = mc_1$.

Dokaz. Neka je $\mathbf{D} = (\mathcal{T}, \mathcal{B})$ afino α-rastavljivi PBD indeksa λ i $\mathcal{R}$ njegov afini rastav. Po teoremu 4.9(v), za svaki $\mathcal{C} \in \mathcal{R}$, dualna incidencijska struktura je 2-$(|\mathcal{C}|, \alpha, k(\mathcal{C}) - r + \lambda)$ dizajn. Za taj dizajn kroz svaku točku prolazi $k(\mathcal{C})$ blokova, jer je $k(\mathcal{C})$ kardinalnost svakog bloka u $\mathcal{C}$. Iz propozicije 2.3 imamo da za 2-(v, k, λ) dizajn vrijedi $\lambda(v-1) = r(k-1)$. Ako primjenimo tu jednakost za 2-$(|\mathcal{C}|, \alpha, k(\mathcal{C}) - r + \lambda)$ dizajn, dobivamo

$$(k(\mathcal{C}) - r + \lambda)(|\mathcal{C}| - 1) = k(\mathcal{C})(\alpha - 1).$$

Koristeći teorem 4.9(iv) pojednostavimo prethodnu jednakost

$$(r - \lambda)|\mathcal{C}|^2 - (\alpha v + r - \lambda)|\mathcal{C}| + \alpha^2 v = 0. \tag{22}$$

Ako je $\alpha = 1$, tada prema (22), $|\mathcal{C}| = v/(r-\lambda)$ ili $|\mathcal{C}| = 1$. Kako $\mathbf{D}$ nema potpuni blok, $|\mathcal{C}| = v/(r-\lambda)$ za svaku klasu rastavljivosti $\mathcal{C}$. Teorem 4.9(iv) implicira da svaki blok u $\mathcal{C}$ ima kardinalnost $r - \lambda$, a to znači i svaki blok u $\mathbf{D}$. Stoga, $\mathbf{D}$ je 2-dizajn.
Pretpostavimo da $\mathbf{D}$ nije 2-dizajn. Tada (22) ima dva različita rješenja c_1 i c_2. Prema Vieteovim formulama, $c_1 + c_2 = (\alpha v + r - \lambda)/(r - \lambda)$ i $c_1 c_2 = \alpha^2 v/(r - \lambda)$. Kako je $\mathbf{D}$ PBD indeksa λ, $r - \lambda > 0$. Prema tome, c_1 i c_2 su pozitivni cijeli brojevi. Ako je $|\mathcal{C}| = c_i, i = 1, 2$, tada prema 4.9(iv) svaki blok iz $\mathcal{C}$ ima kardinalnost $k_i = \alpha v/c_i$. Tada je $k_1 + k_2 = \alpha v(c_1 + c_2)/(c_1 c_2) = v + (r - \lambda)/\alpha$.

Odatle slijedi da je $m = (r - \lambda)/\alpha$ pozitivan cijeli broj. Uvrstimo m u (22) i dobivamo

$$m|\mathcal{C}|^2 - (v + m)|\mathcal{C}| + \alpha v = 0. \tag{23}$$

Po Vieteovim formulama iz (23), $c_1 + c_2 = (v + m)/m$. Kako su c_1 i c_2 pozitivni cijeli brojevi, to znači m dijeli v. Zapišemo v u obliku $v = mu$, gdje je u pozitivni cijeli broj i uvrstimo u (23)

$$|\mathcal{C}|^2 - (u + 1)|\mathcal{C}| + \alpha u = 0. \tag{24}$$

Primjenimo Vieteove formule u (24) i dobivamo tvrdnju (iii). Dokažimo i tvrdnju (iv). Primjenom teorema 4.9(iv), $k_1 = \alpha v/c_1 = \alpha mu/c_1 = mc_1c_2/c_1 = mc_2$. Analogno dobivamo $k_2 = mc_1$. □

Napomena 5.3. *Za svaki α i $u = 2(2\alpha - 1)$ kvadratna jednadžba u (24) ima rješenja $|\mathcal{C}| = c_1 = 2\alpha$ i $|\mathcal{C}| = c_2 = 2\alpha - 1$. Za svaki parni m, dobivamo dopustiv skup parametara afino α-rastavljivog PBD-a indeksa $m\alpha$ koji ima $v = 2m(2\alpha - 1)$ točaka, $2m - 1$ klasa rastavljivosti koje sadrže 2α blokova kardinalnosti $m(2\alpha - 1)$, i jednu klasu rastavljivosti koja sadrži $2\alpha - 1$ blokova kardinalnosti $2m\alpha$. Prema tome takav PBD ima $4m\alpha - 1$ blokova. U sljedećem primjeru imamo PBD za $\alpha = 2$ i $m = 2$.*

Primjer 5.4. *Promotrimo incidencijsku strukturu $\boldsymbol{D} = (\mathcal{T}, \mathcal{B})$ gdje je $\mathcal{T} = \{1, 2, ..., 12\}$ i $\mathcal{B}$ sadrži sljedeće blokove:*

$\{1,2,5,6,9,10\}$	$\{1,2,7,8,9,11\}$	$\{1,3,5,7,9,12\}$	$\{1,2,3,4,5,6,7,8\}$
$\{1,4,5,8,11,12\}$	$\{1,3,6,8,10,12\}$	$\{1,4,6,7,10,11\}$	$\{1,2,3,4,9,10,11,12\}$
$\{2,3,6,7,11,12\}$	$\{2,4,5,7,10,12\}$	$\{2,3,5,8,10,11\}$	$\{5,6,7,8,9,10,11,12\}$
$\{3,4,7,8,9,10\}$	$\{3,4,5,6,9,11\}$	$\{2,4,6,8,9,12\}$	

Napisali smo ih tako da blokovi u svakom stupcu pripadaju istoj klasi rastavljivosti. Svaka točka iz $\mathcal{T}$ sadržana je u dva bloka svake klase rastavljivosti, pa je $\alpha = 2$. Svake dvije točke sadržane su u 4 bloka iz $\mathcal{B}$, tj. $\lambda = 4$. Znači $\boldsymbol{D}$ je afino 2-rastavljivi PBD indeksa 4. Da $\boldsymbol{D}$ nije 2-dizajn vidimo na prvi pogled, zato što ima blokove različitih veličina.

Nama će biti najzanimljiviji PBD-ovi koji dopuštaju afini rastav za $\alpha = 1$. Po teoremu 5.2 ako takav PBD nema potpuni blok, tada je 2-dizajn. Takve dizajne nazivamo *afino rastavljivi dizajni*. Sljedeća propozicija nam pokazuje kako parametri afino rastavljivog dizajna mogu biti izraženi u ovisnosti o dva povezana parametra.

Propozicija 5.5. *Neka je $\boldsymbol{D}$ afino rastavljivi (v, b, r, k, λ) dizajn. Neka je s kardinalnost klase paralelnosti i μ kardinalnost presjeka dva bloka iz različitih*

klasa paralelnosti. Tada $s-1$ *dijeli* $\mu-1$ *i*

$$v=s^2\mu,\ b=\frac{s(s^2\mu-1)}{s-1},\ r=\frac{s^2\mu-1}{s-1},\ k=s\mu,\ \lambda=\frac{s\mu-1}{s-1}. \tag{25}$$

Dokaz. Prema propoziciji 3.6, $v=sk$. Iz teorema 4.9(iii), $k^2=\mu v$. Te dvije jednakosti daju $v=s^2\mu$ i $k=s\mu$. Kako je dizajn $\mathbf{D}$ afino rastavljiv, $b=v+r-1$, pa je $bk=vk+rk-k$. Prema propoziciji 2.4, $bk=vr$ i sada imamo

$$r=\frac{(v-1)k}{v-k}=\frac{s^2\mu-1}{s-1}.$$

Prema propoziciji 2.3, $\lambda(v-1)=r(k-1)$ i stoga vrijedi

$$\lambda=\frac{r(k-1)}{v-1}=\frac{s\mu-1}{s-1}.$$

Kada imamo poznate v i r možemo odrediti i b:

$$b=\frac{s(s^2\mu-1)}{s-1}.$$

Iz predzadnje jednakosti imamo $s\mu-1=\lambda(s-1)$, tj. $s-1$ dijeli $s\mu-1$. Možemo zapisati $s\mu-1=s(\mu-1)+s-1$. Kako $s-1$ ne dijeli s, tada $s-1$ dijeli $\mu-1$. □

Već smo uvjerili da je afina ravnina dizajn koji dostiže Boseovu nejednakost, pa je primjer afino rastavljivog dizajna. Sada ćemo se upoznati s generalizacijom afine ravnine, *n-dimenzionalnom afinom geometrijom.*

Primjer 5.6. *Za n-dimenzionalnu afinu geometriju koristimo oznaku* $AG(n,q)$. *To je konačna geometrija, pa je pripadni vektorski prostor konačnodimenzionalan i definiran je nad poljem* $\mathbb{F}_q$ *reda q, gdje je q prim potencija. Nama je od interesa da unutar te geometrije postoje dizajni. Te dizajne čine točke i d-ravnine (vektori i translati d-dimenzionalnih potprostora n-dimenzionalnog vektorskog prostora nad* $\mathbb{F}_q$*). Takve dizajne označavamo s* $AG_d(n,q)$. *Njihovi parametri su* $(q^n, q^d, \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q)$, *gdje* $\begin{bmatrix} n \\ d \end{bmatrix}_q$ *označava broj d-dimenzionalnih potprostora n-dimenzionalnog vektorskog prostora nad* $\mathbb{F}_q$ *i jednak je*

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

U n-dimenzionalnom vektorskom prostoru nad $\mathbb{F}_q$ *ukupan broj vektora je* q^n *i translati d-dimenzionalnih potprostora sadrže isti broj vektora kao d-dimezionalni potprostori,* q^d. *Ako translatiramo d-dimenzionalni potprostor*

za vektor x, tada su vektori x i y translatirani vektori od nulvektora i $y-x$. Prema tome broj translata d-dimenzionalnih potprostora koji sadrže vektore x i y jednak je broju d-dimenzionalnih potprostora koji sadrže vektor $y-x$. Takvi d-dimenzionalni potprostori generirani su s d linearno neovisnih vektora među kojima je i $y-x$. U n-dimenzionalnom vektorskom prostoru ukupan broj takvih d-torki vektora je $(q^n-q)(q^n-q^2)\cdots(q^n-q^{d-1})$. Prvi vektor je $y-x$, za drugi vektor možemo odabrati q^n-q vektora koji nisu proporcionalni s $y-x$, za treći vektor možemo odabrati q^n-q^2 vektora koji nisu u potprostoru generiranom s prethodna dva vektora itd. Na isti način možemo odrediti ukupan broj tih d-torki vektora u d-dimenzionalnom potprostoru, gdje je ukupan broj vektora q^d. Tada je taj broj jednak $(q^d-q)(q^d-q^2)\cdots(q^d-q^{d-1})$. Sada je ukupan broj d-dimenzionalnih potprostora koji sadrže vektor $y-x$ jednak

$$\frac{(q^n-q)(q^n-q^2)\cdots(q^n-q^{d-1})}{(q^d-q)(q^d-q^2)\cdots(q^d-q^{d-1})}=\frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-d+1}-1)}{(q^{d-1}-1)(q^{d-2}-1)\cdots(q-1)}=\begin{bmatrix}n-1\\d-1\end{bmatrix}_q.$$

Zaključujemo da je broj translata d-dimenzionalnih potprostora koji sadrže vektore x i y jednak $\begin{bmatrix}n-1\\d-1\end{bmatrix}_q$. Na skupu d-ravnina možemo zadati relaciju paralelnosti (kao što smo napravili za $d=1$ kod afine ravnine). Sada su nam paralelne d-ravnine translati istog d-dimenzionalnog potprostora. Ta relacija je relacija ekvivalencije i particionira skup d-ravnina u klase paralelnosti. Stoga su dizajni unutar n-dimenzionalne afine geometrije rastavljivi dizajni. Nama je posebno zanimljiv dizajn $AG_{n-1}(n,q)$, kojeg čine točke i $(n-1)$-ravnine (hiperravnine). To je afino rastavljivi dizajn. Svake dvije neparalelne hiperravnine sijeku se u ravnini dimenzije $n-2$. Klase paralelnosti u $AG_{n-1}(n,q)$ su skupovi od q paralelnih hiperravnina. Parametri tog dizajna su $(q^n, q^{n-1}, \frac{q^{n-1}-1}{q-1})$. Za $n=2$ imamo afinu ravninu reda q.

Sada ćemo konstruirati simetrični dizajn koristeći afino rastavljivi dizajn.

Teorem 5.7. *Ako postoji afino rastavljivi (v,b,r,k,λ) dizajn, tada postoji simetrični $(v(r+1), kr, k\lambda)$ dizajn koji dopušta simetričnu incidencijsku matricu.*

Dokaz. Neka je $\mathbf{D}$ afino rastavljivi (v,b,r,k,λ) dizajn sa skupom točaka $\mathcal{T}=\{x_1,...,x_v\}$ i klasama paralelnosti $\mathcal{C}_1,...,\mathcal{C}_r$. Za $h=1,2,...,r$, neka je M_h $(0,1)$-matrica reda v takva da se na mjestu (i,j) nalazi 1 ako i samo ako su točke x_i i x_j u istom bloku klase paralelnosti C_h. Matrice M_h su simetrične, jer ako su x_i i x_j u istom bloku klase paralelnosti C_h, tada su x_j i x_i u

istom bloku. Ako je μ kardinalnost presjeka dva bloka u $\mathbf{D}$ iz različitih klasa paralelnosti, tada za $h, l = 1, ..., r$ vrijedi

$$M_h M_l^\tau = \begin{cases} \mu J, & \text{ako } l \neq h, \\ kM_h, & \text{ako } l = h. \end{cases} \tag{26}$$

U svakom retku matrice M_h, ako su u j-tim stupcima jedinice, točke x_j su sadržane u jednom bloku iz klase paralelnosti h. Isto vrijedi i za matricu M_l. Ako je $l \neq h$, u matrici $M_h M_l^\tau$ na mjestu (i, j) nalazi se skalarni produkt i-tog retka matrice M_h i j-tog retka matrice M_l. Tada skalarni produkt predstavlja presjek dva bloka iz klasa paralelnosti h i l, pa je $M_h M_l^\tau = \mu J$. Broj jedinica u svakom retku matrica M_h predstavlja broj točaka koje sadrže blokovi u klasama paralelnosti C_h. Svi blokovi imaju kardinalnost k. Ako je $l = h$, u matrici $M_h M_l^\tau$ na mjestu (i, j) nalazi se skalarni produkt i-tog i j-tog retka matrice M_h. Ako su ti retci jednaki na mjestu (i, j) nalazi se broj k, a ako su različiti broj 0 (u klasi paralelnosti svaka točka je sadržana u jednom bloku). Prema tome, $M_h M_l^\tau = kM_h$. Ako je A incidencijska matrica dizajna $\mathbf{D}$, tada po teoremu 2.6 vrijedi

$$A \cdot A^\tau = (r - \lambda)I + \lambda J. \tag{27}$$

Prema tome matrica $A \cdot A^\tau$ ima brojeve r na dijagonali i brojeve λ izvan dijagonale. Kada zbrojimo sve matrice M_h na dijagonali imamo broj klasa paralelnosti r, kako su svake dvije točke sadržane u λ blokova iz svih klasa paralelnosti, izvan dijagonale imamo brojeve λ. Tada vrijedi

$$A \cdot A^\tau = \sum_{h=1}^{r} M_h. \tag{28}$$

Iz jednakosti (27) i (28) slijedi

$$\sum_{h=1}^{r} M_h = (r - \lambda)I + \lambda J. \tag{29}$$

Neka je M_{r+1} nul matrica reda v i L simetrični latinski kvadrat reda $r + 1$. Tablica zbrajanja u grupi $(\mathbb{Z}/n\mathbb{Z}, +)$, tzv. grupi ostataka modulo n je simetrični latinski kvadrat reda n, jer je to konačna abelova grupa. Prema tome postoji simetrični latinski kvadrat za svaki $n \in \mathbb{N}$. Definiramo blok matricu $N = [N_{ij}]$ reda $v(r + 1)$ na sljedeći način:

$$N_{ij} = M_h \text{ ako i samo ako } L(i, j) = h.$$

Tada za $j = 1, 2, ..., r+1$, koristeći jednakosti (26) i (29) dobivamo

$$\sum_{h=1}^{r+1} N_{jh} N_{jh}^{\tau} = \sum_{h=1}^{r+1} kM_h = k \sum_{h=1}^{r+1} M_h = (kr - k\lambda)I + k\lambda J.$$

Dakle, podmatrice reda v koje se nalaze na dijagonali blok matrice $N \cdot N^{\tau}$ imaju brojeve kr na dijagonali i $k\lambda$ izvan dijagonale. Zbog latinskog kvadrata u svakom retku i stupcu blok matrice N imamo jednu nul podmatricu. Prema tome za različite $i, j \in \{1, 2, ..., r+1\}$ u skalarnom produktu i-tog i j-tog retka blok matrice N sumiramo i dvije nul podmatrice. Tada koristeći jednakost (26) imamo

$$\sum_{h=1}^{r+1} N_{ih} N_{jh}^{\tau} = (r-1)\mu J.$$

Iz propozicije 5.5, $(r-1)\mu = (\frac{s^2\mu - 1}{s-1} - 1)\mu = s\mu(\frac{s\mu - 1}{s-1}) = k\lambda$. Stoga podmatrice koje se ne nalaze na dijagonali blok matrice $N \cdot N^{\tau}$ imaju na svim mjestima brojeve $k\lambda$. Tada matrica $N \cdot N^{\tau}$ ima brojeve kr na dijagonali i $k\lambda$ izvan dijagonale. Kako matrice M_h u svakom stupcu imaju k jedinica, matrica N u svakom stupcu ima kr jedinica. Koristeći teorem 2.6 zaključujemo da je N incidencijska matrica simetričnog $(v(r+1), kr, k\lambda)$ dizajna. Kako su M_h simetrične matrice i latinski kvadrat je simetričan, N je simetrična matrica. □

Primjer 5.8. *Ilustrirajmo primjerom kako smo konstruirali simetrični dizajn u prethodnom teoremu. Koristiti ćemo već poznati primjer* $(4, 6, 3, 2, 1)$ *dizajna (afinu ravninu reda 2). To je afino rastavljivi dizajn. Neka je skup točaka* $\mathcal{T} = \{x_1, x_2, x_3, x_4\}$. *Tada imamo klase paralelnosti* $\mathcal{C}_1 = \{\{x_1, x_2\}, \{x_3, x_4\}\}$, $\mathcal{C}_2 = \{\{x_1, x_3\}, \{x_2, x_4\}\}$ *i* $\mathcal{C}_3 = \{\{x_1, x_4\}, \{x_2, x_3\}\}$. *Sada ispišimo matrice* M_h *za* $h = 1, 2, 3$,

$$M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, M_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, M_3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Matrica M_{r+1}, *tj. u našem primjeru* M_4 *je nul matrica*

$$M_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Simetrični latinski kvadrat je reda 4 i može izgledati ovako:

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}.$$

Možemo ispisati matricu N

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

Na mjestu (i, i) u blok matrici $N \cdot N^\tau$ nalazi se skalarni produkt i-tog retka sa samim sobom blok matrice N. Odredimo mjesto $(1, 1)$. Imamo $N_{11} = M_1, N_{12} = M_2, N_{13} = M_3$ i $N_{14} = M_4$. Koristeći (26) dobivamo

$$\begin{bmatrix} 2 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix} + \begin{bmatrix} 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{bmatrix} + \begin{bmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 2 & 2 & 2 \\ 2 & 6 & 2 & 2 \\ 2 & 2 & 6 & 2 \\ 2 & 2 & 2 & 6 \end{bmatrix}.$$

Zbog latinskog kvadrata u svakom retku blok matrice N pojavljuju se sve podmatrice M_h. Tada na svim mjestima na dijagonali blok matrice $N \cdot N^\tau$ imamo podmatrice $\begin{bmatrix} 6 & 2 & 2 & 2 \\ 2 & 6 & 2 & 2 \\ 2 & 2 & 6 & 2 \\ 2 & 2 & 2 & 6 \end{bmatrix}$.

Odredimo mjesto $(1, 2)$ u blok matrici $N \cdot N^\tau$. Na mjestu $(1, 2)$ nalazi se

skalarni produkt prvog i drugog retka blok matrice N. Kardinalnost presjeka svaka dva bloka iz različitih klasa paralelnosti jednaka je 1. Imamo $N_{21} = M_2, N_{22} = M_3, N_{23} = M_4, N_{24} = M_1$ i koristeći (26):

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix}.$$

U svakom retku i stupcu blok matrice N nalazi se po jedna nul podmatrica. Prema tome na svim mjestima izvan dijagonale blok matrice $N \cdot N^\tau$ imamo podmatrice $\begin{bmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix}$.
Tada matrica $N \cdot N^\tau$ ima brojeve 6 na dijagonali i 2 izvan dijagonale. Kako matrice M_h u svakom stupcu imaju 2 jedinice, matrica N u svakom stupcu ima 6 jedinica. Dimenzija matrice N je 16×16. Tada je N incidencijska matrica simetričnog $(16, 6, 2)$ dizajna. Vidimo da je latinski kvadrat simetričan i matrice M_h su simetrične, pa je N simetrična matrica.

6 Rastavljivi dizajni i ekvidistantni kodovi

Na kraju našeg proučavanja rastavljivih dizajna istražit ćemo njihovu povezanost s ekvidistantnim kodovima. Kod za ispravljanje pogrešaka je pojam iz teorije kodiranja koja se bavi problemom prijenosa informacija. Neka je Q konačan skup od q elemenata. Elemente skupa Q zovemo *simbolima*, a skup Q *abecedom*. Uređene n-torke elemenata iz Q zovemo *vektorima*, iako Q^n nije uvijek vektorski prostor. Neka su $x = (x_1, ..., x_n)$ i $y = (y_1, ..., y_n)$ vektori iz Q^n. *Hammingovu udaljenost* vektora definiramo s

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

Sada možemo definirati kod.

Definicija 6.1. Kod *s parametrima* (n, m, d, q) *je podskup* $C \subseteq Q^n$. *Pritom je* n duljina *koda,* $m = |C|$ *je broj* kodnih riječi, $d = min\{d(x, y) | x, y \in C, x \neq y\}$ *je* minimalna udaljenost *koda, a* $q = |Q|$ *je broj simbola.*

Kod možemo identificirati s $m \times n$ matricom čiji su retci kodne riječi. Tu matricu ćemo označavati istim slovom C.

Definicija 6.2. Ekvidistanti kod *je kod čije su svake dvije riječi na minimalnoj udaljenosti.*

Ekvidistantne kodove možemo povezati s $\{1, -1\}$-matricima kod kojih je skalarni produkt svaka dva retka i stupca jednak nuli.

Definicija 6.3. Hadamardova matrica *reda* n *je kvadratna matrica* H *s unosima iz skupa* $\{1, -1\}$ *takva da je* $H \cdot H^\tau = nI_n$.

Ako postoji Hadamardova matrica reda $n > 2$, onda je n djeljiv s 4 (vidi [4, str. 24]). Za Hadamardove matrice koje u prvom retku i stupcu imaju samo jedinice kažemo da su u standardnom obliku. Kod identificiran s Hadamardovom matricom ima simbole -1 i 1. Ako -1 zamijenimo s 0, to je *binarni kod* nad abecedom $\{0, 1\}$. Parametri binarnog koda zadovoljavaju sljedeću nejednakost.

Propozicija 6.4. (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 ove propozicije je u skripti [4, str. 78]. Iz Hadamardovih matrica dobivamo ekvidistantne kodove koji dostižu nejednakost u prethodnoj propoziciji.

Teorem 6.5. *Ako postoji Hadamardova matrica reda $n \geq 4$, onda postoje ekvidistantni 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. Kako je skalarni produkt bilo koja dva retka Hadamardove matrice jednak 0, broj jednakih unosa isti je kao broj različitih unosa. Tada je Hammingova udaljenost jednaka $\frac{n}{2}$ za svaka dva retka. Prema tome iz Hadamardove matrice dobivamo ekvidistantni $(n, n, \frac{n}{2}, 2)$ kod. Kako je $d = \frac{n}{2}$, za taj kod ne vrijedi Plotkinova ocjena. Ako iz Hadamardove matrice u standardnom obliku izbacimo prvi stupac, dobivamo ekvidistantni $(n-1, n, \frac{n}{2}, 2)$ kod. Prema propoziciji 6.4 taj kod dostiže Plotkinovu ocjenu. Njegova identificirajuća matrica ima jednak broj jedinica i minus jedinica u prvom stupcu. Ako fiksiramo jedan od simbola u prvom stupcu i izbacimo taj stupac, a retke proglasimo kodnim riječima (postupak skraćivanja koda), dobivamo ekvidistantni $(n-2, \frac{n}{2}, \frac{n}{2}, 2)$ kod. Taj kod također dostiže Plotkinovu ocjenu. □

Ekvidistantne kodove možemo dobiti i iz rastavljivih dizajna. Za to nam je potreban još jedan pomoćni rezultat.

Definicija 6.6. *Ako je C (n, m, d, q) kod, tada*

$$\overline{d} = \frac{1}{\binom{m}{2}} \sum_{x,y \in C} d(x, y)$$

nazivamo srednja udaljenost *koda C.*

Lema 6.7. *Srednja udaljenost $\overline{d}$ (n, m, d, q) koda C zadovoljava nejednakost*

$$\overline{d} \leq \frac{mn(q-1)}{(m-1)q},$$

a jednakost vrijedi ako i samo ako se svaki element abecede pojavljuje m/q puta u svakom stupcu matrice C.

Dokaz. Neka su simboli $i = 0, 1, ..., q-1$. Za $j = 1, 2, ..., n$ označimo s a_{ij} broj pojavljivanja simbola i u j-tom stupcu matrice C. Tada sumu svih Hammingovih udaljenosti koda C možemo dobiti tako da za matricu $C = [c_{kj}]$ brojimo elemente skupova $S_j = \{(k, l) : c_{kj} \neq c_{lj}, 1 \leq k < l \leq m\}$ za $j = 1, 2, ..., n$. Možemo odrediti broj elemenata skupova $S'_j = \{(k, l) : c_{kj} = c_{lj}, 1 \leq k < l \leq m\}$, jer za simbol i broj pojavljvanja u j-tom stupcu je a_{ij}, pa je $|S'_j| = \sum_{i=0}^{q-1} \binom{a_{ij}}{2}$. Kako je za svaki $j = 1, 2, ..., n$, $|S_j| + |S'_j| = \binom{m}{2}$, tada vrijedi

$$\sum_{j=1}^{n} |S_j| = \sum_{j=1}^{n} \left(\binom{m}{2} - \sum_{i=0}^{q-1} \binom{a_{ij}}{2} \right).$$

Kako je lijeva strana prethodne jednakosti suma svih Hammingovih udaljednosti koda C, imamo

$$\sum_{x,y\in C} d(x,y) = \sum_{j=1}^{n} \left(\binom{m}{2} - \sum_{i=0}^{q-1} \binom{a_{ij}}{2} \right).$$

Primijetimo da je $\sum_{i=0}^{q-1} a_{ij} = m$ i izračunamo sume koje možemo

$$\sum_{x,y\in C} d(x,y) = \frac{nm(m-1)}{2} + \frac{nm}{2} - \frac{1}{2} \sum_{j=1}^{n} \sum_{i=0}^{q-1} a_{ij}^2. \tag{30}$$

Za vektore $a, b \in \mathbb{R}^d$ vrijedi nejednakost Schwarz-Cauchy-Bunjakovskog:

$$|a \cdot b|^2 \leq \|a\|^2 \cdot \|b\|^2 .$$

Za $d = nq$ primijenimo prethodnu nejednakost na vektore $(a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{qn})$, $(1, \ldots, 1)$ i dobivamo

$$\sum_{j=1}^{n} \sum_{i=0}^{q-1} a_{ij}^2 \geq \frac{1}{nq} \left(\sum_{j=1}^{n} \sum_{i=0}^{q-1} a_{ij} \right)^2 .$$

Pomnožimo obje strane nejednakosti s $1/nq$:

$$\frac{1}{nq} \sum_{j=1}^{n} \sum_{i=0}^{q-1} a_{ij}^2 \geq \left(\frac{1}{nq} \sum_{j=1}^{n} \sum_{i=0}^{q-1} a_{ij} \right)^2 = \left(\frac{m}{q} \right)^2 . \tag{31}$$

Uvrstimo (31) u (30) i dobivamo

$$\sum_{x,y\in C} d(x,y) \leq \frac{nm^2(q-1)}{2q}.$$

Iskoristimo definiciju 6.6 i dobijemo traženu nejednakost

$$\overline{d} \leq \frac{mn(q-1)}{(m-1)q}.$$

U (31) vrijedi jednakost ako i samo ako je a_{ij} konstanta. Tada je $a_{ij} = m/q$ za sve $i = 0, 1, ..., q-1$ i $j = 1, 2, ..., n$. Iz toga zaključujemo da se svaki element abecede u svakom stupcu matrice C pojavljuje m/q puta. □

Definicija 6.8. *Ekvidistantni* (n, m, d, q) *kod naziva se* maksimalni *ako je*

$$d = \frac{mn(q-1)}{(m-1)q}.$$

Teorem 6.9. *Maksimalni ekvidistantni* (n, m, d, q) *kod postoji ako i samo ako postoji rastavljivi* $(m, nq, n, m/q, n-d)$ *dizajn.*

Dokaz. Neka je $N = [N_1\ N_2\ ...\ N_n]$ incidencijska matrica rastavljivog $(m, nq, n, m/q, n-d)$ dizajna $\mathbf{D}$, gdje su $N_1, N_2, ..., N_n$ podmatrice koje korespondiraju različitim klasama paralelnosti u $\mathbf{D}$. Prema propoziciji 3.6 sve klase paralelnosti od $\mathbf{D}$ imaju kardinalnost q. Tada svaka podmatrica N_j ima q stupaca. Indeksirat ćemo ih s $0, 1, ..., q-1$. Sada definiramo matricu $C = [c_{ij}]$ nad abecedom $\mathcal{A} = \{0, 1, ..., q-1\}$ s

$$c_{ij} = l \text{ ako i samo ako je na mjestu } (i, l) \text{ jedinica u matrici } N_j.$$

Tada je $l \in \{0, 1, ..., q-1\}$. Primijetimo da matrica C ima m redaka (broj točaka od $\mathbf{D}$) i n stupaca (broj klasa paralelnosti u $\mathbf{D}$). Ako kodne riječi x i y korespondiraju s i-tim i h-tim retcima matrice C $(i \neq h)$, tada je $n - d(x, y)$ broj stupaca od C koji imaju jednak simbol u i-tim i h-tim retcima. Ako je $c_{ij} = c_{hj} = l$, tada je $(i, l) = 1$ i $(h, l) = 1$ u podmatrici N_j. Prema tome, $n - d(x, y)$ je i broj stupaca u matrici N koji imaju jedinice u i-tim i h-tim retcima. Kako je to broj blokova od $\mathbf{D}$ koji sadrže točke koje korespondiraju kodnim riječima x i y, broj $n - d(x, y)$ je jednak za sve različite x i y, tj. $d(x, y) = d$. Vidimo da je C ekvidistantni (n, m, d, q) kod. Svi blokovi od $\mathbf{D}$ sadrže m/q točaka. Stoga u svim stupcima matrica N_j, $j = 1, 2, ..., n$ imamo m/q jedinica. Indeks svakog stupca od N_j je jedan simbol abecede $\mathcal{A}$. Zaključujemo da se svaki simbol od $\mathcal{A}$ pojavljuje m/q puta u svakom stupcu od C, pa je kod C maksimalan.
Obratno, pretpostavimo da imamo maksimalni ekvidistantni (n, m, d, q) kod C s matricom $C = [c_{ij}]$ nad abecedom $\mathcal{A} = \{0, 1, ..., q-1\}$. Za $j = 1, 2, ..., n$ definiramo $(0, 1)$-matricu N_j dimenzije $m \times q$ (sa stupcima indeksiranim s $0, 1, ..., q-1$), u kojoj je na mjestu (i, l) jedinica ako i samo ako je $c_{ij} = l$. Formiramo matricu $N = [N_1\ N_2\ ...\ N_n]$. Tada matrica N ima m redaka i nq stupaca. Kako je kod C maksimalan, svaki l pojavljuje se m/q puta u svakom stupcu matrice C. Prema tome u podmatrici N_j, $j = 1, 2, ..., n$ u svakom stupcu imamo m/q jedinica, tj. u matrici N svaki stupac sadrži m/q jedinica. U svakom retku podmatrice N_j imamo jednu jedinicu u stupcu l, što znači da u matrici N u svakom retku imamo n jedinica. Kako je kod ekvidistantan, svaka dva retka matrice C imaju jednake simbole u $n - d$ stupaca. Tada svaka dva retka u matrici N imaju jedinice u $n - d$ stupaca.

Konačno zaključujemo da je matrica N incidencijska matrica rastavljivog $(m, nq, n, m/q, n-d)$ dizajna čije podmatrice N_j korespondiraju različitim klasama paralelnosti. □

Primjer 6.10. *Znamo da postoji rastavljivi* $(4, 6, 3, 2, 1)$ *dizajn. U primjeru 5.8 ispisali smo klase paralelnosti:* $\mathcal{C}_1 = \{\{x_1, x_2\}, \{x_3, x_4\}\}$, $\mathcal{C}_2 = \{\{x_1, x_3\}, \{x_2, x_4\}\}$, $\mathcal{C}_3 = \{\{x_1, x_4\}, \{x_2, x_3\}\}$. *Sada će nam klasama* $\mathcal{C}_j$, $j = 1, 2, 3$ *korespondirati matrice* N_j*:*

$$N_1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}, N_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, N_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Možemo ispisati matricu

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

Kao u prethodnom teoremu iz matrica N_j *formiramo matricu*

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

Matrica C *ima 4 retka i 3 stupca. Prema tome kod* C *sadrži 4 kodne riječi duljine 3. Imamo dva simbola: 0 i 1. Uočavamo da je Hammingova udaljenost svake dvije kodne riječi jednaka 2. U svakom stupcu 0 i 1 se pojavljuju po 2 puta. Dakle, matricu* C *identificiramo s maksimalnim ekvidistantnim* $(3, 4, 2, 2)$ *kodom. Kako je kod binaran, možemo ga dobiti i iz Hadamardove matrice reda 4.*

Literatura

[1] N. Antonić, *Linearna algebra 1*, predavanja iz akademske godine 2008./2009.

[2] Y.I. Ionin, M.S. Shrikhande, *Combinatorics of symmetric designs*, Cambridge University Press, 2006.

[3] D.R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer-Verlag, 2004.

[4] J. Šiftar, V. Krčadinac, *Konačne geometrije*, skripta, PMF-Matematički odjel, 2013. Dostupno na http://web.math.pmf.unizg.hr/nastava/kg/index.php.

[5] Wikipedia, *Kirkman's schoolgirl problem*, dostupno na https://en.wikipedia.org/wiki/Kirkman%27s_schoolgirl_problem (lipanj 2015.).

Sažetak

Motivacija za pisanje diplomskog rada bila je Kirkmanov problem 15 učenica. Jedna od interpretacija tog problema je rastavljivi dizajn. Na početku smo se upoznali s dizajnima i iznijeli osnovne rezultate koji vrijede za dizajne. Generalizacija dizajna je u parovima balansirani dizajn (PBD). Na toj incidencijskoj strukturi definiramo pojam rastavljivosti. Jedan nuždan uvjet za postojanje dizajna je Fisherova nejednakost. Dizajni koji dostižu Fisherovu nejednakost su simetrični dizajni. Za rastavljive dizajne vrijedi poboljšanje te nejednakosti, Boseova nejednakost. Nama su posebno zanimljivi dizajni koji dostižu Boseovu nejednakost. To su afino rastavljivi dizajni. Koristeći afino rastavljive dizajne možemo konstruirati simetrične dizajne. Na kraju diplomskog rada povezali smo rastavljive dizajne s još jednom zanimljivom strukturom, ekvidistantnim kodovima.

Summary

Kirkman's schoolgirl problem motivated the writing of this graduate work. It is a famous example of a resolvable design. At the beginning we made an introduction to designs and gave some basic results that apply to designs. The incidence structure on which we define the notion of resolution is pairwise balanced design (PBD). One necessary condition for the existence of a design is Fisher's inequality. Designs that attain the equality in Fisher's inequality are symmetric designs. If a PBD admits a resolution, a stronger result known as Bose's inequality holds. We are interested in designs attaining the equality in Bose's inequality. These are affine resolvable designs. We can construct symmetric designs using affine resolvable designs. In the end we explored the connections between equidistant codes and resolvable designs.

Životopis

Rođen sam u Kotor-Varošu, Bosna i Hercegovina, 1.2.1982. Osnovnu i srednju školu završio sam u Požegi. Završio sam prirodoslovno-matematičku gimnaziju. Nakon srednje škole radio sam povremeno u šumarstvu. Studij matematike u Zagrebu upisao sam 2008. godine. Završio sam preddiplomski studij Matematika; smjer: nastavnički 2012. godine i upisao diplomski studij istog smjera. Metodičku praksu iz matematike odradio sam u Osnovnoj školi Ivana Gorana Kovačića i Tehničkoj školi Ruđera Boškovića u Zagrebu.