Sveučilište u Zagrebu
Prirodoslovno–matematički fakultet
Matematički odjel

Vedran Krčadinac

Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$

Magistarski rad

Zagreb, listopad 1999.

Predgovor

Steinerovi 2-dizajni proučavaju se više od 150 godina. Njihovo ime donekle je nepravedno vezano uz švicarskog geometričara J.Steinera, jer ih je prije njega uveo engleski matematičar T.P.Kirkman. Da nepravda bude veća, Kirkman je u članku iz 1847. riješio problem egzistencije za $k = 3$, dok je Steiner samo postavio problem 1853. godine (ne znajući za Kirkmanov rad).

Sredinom 20. stoljeća ponovo oživljava interes za slične konačne strukture. Poticaj djelomično dolazi iz biologije i drugih eksperimentalnih znanosti, gdje se dizajni koriste za planiranje eksperimenata. U šezdesetim godinama H.Hanani riješio je problem egzistencije Steinerovih 2-dizajna za $k = 4$ i $k = 5$. Najveći napredak ostvaren je u sedamdesetim godinama, kad je R.M.Wilson dokazao da su nužni uvjeti egzistencije ujedno i "asimptotički dovoljni", za svaki $k \geq 3$.

Tema ovog rada su Steinerovi 2-dizajni s parametrima $S(k, 2k^2 - 2k + 1)$. Oni su među Steinerovim 2-dizajnima karakterizirani svojstvom da pravaca ima dvostruko više nego točaka, ili određenom "hiperboličkom negacijom" Euklidovog petog postulata. Mogli bi ih stoga zvati konačne hiperboličke ravnine. Problem egzistencije tih dizajna otvoren je za svaki $k \geq 6$, jer su parametri izvan dosega Wilsonove asimptotičke teorije. Danas su poznata svega 34 primjera s $k = 3$, 4 i 5.

U prvom dijelu rada detaljno proučavamo poznate primjere. Promatramo njihove pune grupe automorfizama, poddizajne i skoro-rezolucije. Osim toga dokazujemo neka svojstva zajednička svim $S(k, 2k^2 - 2k + 1)$ dizajnima, posebno njihove veze s drugim konačnim strukturama – simetričnim $(2k^2 - 3k + 1)_k$ konfiguracijama i eliptičkim poluravninama.

U sklopu rada razvijamo algoritam za klasifikaciju konačnih objekata do na izomorfizam. Algoritam su E.Spence i drugi koristili u mnogim posebnim slučajevima. U radu algoritam opisujemo i dokazujemo na općenit način. Razvijamo niz programskih alata za provedbu algoritma i primjenjujemo ga na klasifikaciju Steinerovih 2-dizajna $S(3, 13)$, $S(3, 15)$ i $S(4, 25)$. Osim toga razrađujemo primjenu algoritma na orbitne strukture, što nam kasnije omogućuje konstrukciju novih $S(5, 41)$ dizajna.

Najveći dio rada posvećen je upravo pokušajima konstrukcije novih $S(k, 2k^2 - 2k + 1)$ dizajna. Koristimo dvije osnovne metode, konstrukciju pomoću diferencijskih familija i konstrukciju pomoću grupa automorfizama. Prvom metodom dobivamo uglavnom negativne rezultate. Među njima su dva nova, nepostojanje $(113, 8, 1)$ diferencijske familije i nepostojanje radikalnih $(2k^2 - 2k + 1, k, 1)$ diferencijskih familija za $6 \leq k \leq 2000$. Drugom metodom dobivamo devet novih $S(5, 41)$ dizajna, pretpostavivši djelovanje grupe automorfizama reda 3. U dokazu je algoritam za klasifikaciju odigrao ključnu

ulogu, zbog izuzetno velikog broja neizomorfnih orbitnih struktura. Također dobivamo niz negativnih rezultata za $k = 6$, 7 i 8, na primjer nepostojanje $S(6, 61)$ dizajna s grupom automorfizama reda 25.

Velik broj dokaza u radu zasniva se na proračunima na računalu. Radu je priložen CD koji sadrži korištene programe, pisane u programskom jeziku C. Na CD-u su pohranjeni rezultati i međurezultati proračuna, često preveliki da bi ih u cijelosti reproducirali na papiru. Na CD-u se nalazi i tekst rada u PDF i HTML formatu, koji sadrži veze (linkove) na relevantne datoteke. Na primjer, kad govorimo o dizajnu $S3.1$, ime je vezano uz tablicu u kojoj su sabrana njegova svojstva. Preko tablice možemo pristupiti mjestu gdje je dizajn pohranjen u obliku incidencijske matrice ili u drugom obliku.

Za nastanak rada zaslužni su mnogi pojedinci, kojima bih na ovom mjestu želio izraziti zahvalnost. Prvenstveno zahvaljujem voditelju rada, dr. Jurju Šiftaru na pozornom praćenju mog rada još od studentskih dana. Pod njegovim sam vodstvom napisao diplomski rad, kao i studentski rad nagrađen Rektorovom nagradom. Zahvaljujem dr. Mariu Pavčeviću na velikom interesu koji je pokazao za rad i na mnogim korisnim sugestijama i primjedbama. Dio rada nastao je za vrijeme studijskog boravka na Sveučilištu u Glasgowu. Zahvaljujem dr. Tedu Spenceu na ljubaznosti i gostoprimstvu, a *British Scholarship Trust*-u i Ministarstvu znanosti i tehnologije na financiranju boravka. Zahvaljujem članovima Geometrijskog seminara, na kojem sam u obliku predavanja izložio velik dio rada.

Na "prženju" CD-a zahvaljujem dr. Goranu Igalyju, a na pomoći pri tiskanju rada Matiji Baliću. Zahvaljujem voditelju i osoblju Računskog centra na pruženoj podršci, kao i cjelokupnom "računalno orijentiranom" dijelu Matematičkog odjela na toleriranju mojih sveprisutnih programa koji usporavaju sustav. Zahvaljujem supruzi Jeleni na strpljivom podnošenju tipkanja po tastaturi u kasne sate, a roditeljima i bratu na žustrom bodrenju bez kojeg bi rad sigurno nastao puno kasnije.

Sadržaj

1 Uvod

1.1 Osnovni rezultati teorije dizajna

Definicija 1.1 Incidencijska struktura *sastoji se od skupa točaka $\mathcal{P}$, skupa pravaca $\mathcal{L}$ i relacije incidencije $I \subseteq \mathcal{P} \times \mathcal{L}$. Ako je $(T, \ell) \in I$ kažemo da točka T leži na pravcu ℓ, odnosno da ℓ prolazi kroz T i pišemo $T\, I\, \ell$.*

Napomena 1.2 Skup svih točaka koje leže na pravcu ℓ označavamo (ℓ). Za incidencijsku strukturu kod koje su skupovi tog oblika međusobno različiti kažemo da je *jednostavna*. Pravce jednostavne incidencijske strukture možemo identificirati s pripadnim skupovima točaka, a I s relacijom "biti element" $\in$. U daljnjem ćemo pod incidencijskom strukturom uvijek razumijevati jednostavnu incidencijsku strukturu.

Definicija 1.3 *Za incidencijsku strukturu kažemo da je $t{-}(v, k, \lambda)$* **dizajn** *ako ima svojstva:*

(1) *Ukupni broj točaka je v.*

(2) *Svaki pravac sadrži k točaka.*

(3) *Svaki t-člani skup točaka sadržan je u λ pravaca.*

Napomena 1.4 Da bi izbjegli trivijalne primjere u ovom radu promatramo samo dizajne s $t < k < v$. Dizajni se najviše proučavaju u dva specijalna slučaja, $t = 2$ i $\lambda = 1$. Dizajne s $t = 2$ zovemo 2-*dizajni* ili *blok dizajni*. U tom slučaju pravci se obično nazivaju *blokovi*, a parametri bilježe (v, k, λ). Dizajne s $\lambda = 1$ zovemo *Steinerovi sistemi*, a parametre zapisujemo u obliku $S(t, k, v)$. Dizajne koji pripadaju jednoj i drugoj familiji (s parametrima $2{-}(v, k, 1)$) zovemo *Steinerovi* 2-*dizajni* $S(k, v)$.

Propozicija 1.5 *Ako je incidencijska struktura $t{-}(v, k, \lambda)$ dizajn, onda je i $s{-}(v, k, \lambda_s)$ dizajn, za $\lambda_s = \dfrac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}\lambda, \quad 0 \leq s \leq t$.*

Dokaz. Neka je $(\mathcal{P}, \mathcal{L}, \in)$ $t-(v,k,\lambda)$ dizajn, a $\mathcal{S} \subseteq \mathcal{P}$ bilo koji s-člani skup točaka. Prebrojimo na dva načina elemente skupa

$$\{(\mathcal{T}, \ell) \ \mid \ \mathcal{T} \subseteq \mathcal{P} \setminus \mathcal{S},\ |\mathcal{T}| = t-s,\ \ell \in \mathcal{L},\ \mathcal{S} \cup \mathcal{T} \subseteq \ell\}.$$

Ako broj pravaca koji sadrže $\mathcal{S}$ označimo x, broj elemenata skupa jednak je umnošku $x \cdot \binom{k-s}{t-s}$. S druge strane, za dani $\mathcal{T}$ u skupu ima λ parova, pa je broj elemenata jednak $\binom{v-s}{t-s} \cdot \lambda$. Izjednačavanjem slijedi $x = \dfrac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}\lambda$, što očito ne ovisi o izboru skupa $\mathcal{S}$.

■

Napomena 1.6 λ_0 je broj pravaca koji sadrže prazan skup, dakle ukupan broj pravaca. Označavamo ga b. λ_1 je broj pravaca kroz bilo koju točku, koji označavamo r.

Korolar 1.7 *Za (v,k,λ) blok dizajn vrijedi $r = \frac{v-1}{k-1}\lambda$ i $b = \frac{v(v-1)}{k(k-1)}\lambda$.*

Definicija 1.8 *Neka su $\mathcal{P} = \{T_1, \ldots, T_v\}$ točke, a $\mathcal{L} = \{\ell_1, \ldots, \ell_b\}$ pravci incidencijske strukture.* **Incidencijska matrica** *te strukture je $v \times b$ matrica*

$$A = [a_{ij}], \qquad a_{ij} = \begin{cases} 1, & \text{ako je } T_i \, I \, \ell_j \\ 0, & \text{inače} \end{cases}$$

Propozicija 1.9 *Neka je $A \in M_{vb}(\{0,1\})$ $v \times b$ matrica s unosima 0 ili 1. A je incidencijska matrica (v,k,λ) blok dizajna ako i samo ako zadovoljava*

(1) $A \cdot A^\tau = (r-\lambda)I_v + \lambda J_v$

(2) $J_v \cdot A = kJ_{v,b}$

Pritom je I_v jedinična matrica reda v, a J_v i $J_{v,b}$ matrice čiji su svi unosi jedinice, dimenzija $v \times v$ i $v \times b$.

Dokaz. Uvjet (2) ekvivalentan je svojstvu da pravci sadrže po k točaka. Uvjet (1) ekvivalentan je svojstvima da je svaka točka sadržana u r pravaca, a svaki par točaka u λ pravaca.

■

Propozicija 1.10 (Fisherova nejednakost) *Broj točaka (v,k,λ) blok dizajna nije veći od broja pravaca, $v \leq b$.*

Dokaz. Incidencijska matrica A blok dizajna zadovoljava

$$\det(AA^\tau) = \det((r-\lambda)I_v + \lambda J_v) = (r-\lambda)^{v-1}\left[r + (v-1)\lambda\right] \neq 0.$$

Matrica AA^τ je regularna, pa je matrica A ranga v. Njezin broj stupaca b ne može biti manji od ranga v.

■

Korolar 1.11 *Parametri Steinerovog 2-dizajna $S(k,v)$ zadovoljavaju*

$$v \geq k^2 - k + 1.$$

Dokaz. Slijedi iz Fisherove nejednakosti i korolara 1.7.

Napomena 1.12 Fisherova nejednakost je nuždan uvjet za postojanje $t-(v,k,\lambda)$ dizajna ($t \geq 2$). Drugi nuždan uvjet je da su brojevi $\lambda_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}\lambda$ prirodni, za $0 \leq s \leq t$. Ako su ispunjeni nužni uvjeti za parametre $t-(v,k,\lambda)$, zovemo ih *dopustivim.*

1.2 Djelovanje grupa

Definicija 1.13 *Neka je G grupa s neutralnim elementom 1, a X skup. Kažemo da G* **djeluje** *na X ako je zadana funkcija $G \times X \to X$, $(g,x) \mapsto gx$ takva da za svaki $x \in X$ i $g,h \in G$ vrijedi $1x = x$ i $g(hx) = (gh)x$.*

Napomena 1.14 Točnije, kažemo da grupa G djeluje na skup X *s lijeva.* Djelovanje *zdesna* je funkcija $X \times G \to X$ sa svojstvima $x1 = x$ i $x(gh) = (xg)h$, za svaki $x \in X$, $g,h \in G$. Pod pojmom djelovanja razumijevamo djelovanje s lijeva, osim ako naglasimo suprotno.

Napomena 1.15 Ako je $g = 1$ jedini element sa svojstvom $gx = x$, za svaki $x \in X$, kažemo da je djelovanje *vjerno.* U suprotnom možemo definirati normalnu podgrupu $N = \{\, g \in G \mid gx = x, \text{ za svaki } x \in X \,\}$ i zamijeniti G s kvocijentnom grupom. G/N uz prirodnu definiciju također djeluje na X, i to vjerno. U ovom radu sva djelovanja bit će vjerna.

Primjer 1.16 Svaka grupa $(G,\cdot)$ djeluje na samu sebe, uz definiciju $(g,h) \mapsto g \cdot h$. Takvo djelovanje zovemo *lijevim translacijama.* G djeluje lijevim translacijama i na partitivni skup $\mathcal{P}(G)$. Budući da se pritom čuva kardinalni broj, G također djeluje na skup k-članih podskupova $\mathcal{P}_k(G)$.

Definicija 1.17 *Neka G djeluje na X i neka je $x \in X$.* **Stabilizator** *od x je podgrupa $G_x = \{g \in G \mid gx = x\} < G$.* **Staza** *ili* **orbita** *od x je skup $x^G = \{gx \mid g \in G\} \subseteq X$.*

Propozicija 1.18 *Kardinalni broj orbite jednak je indeksu stabilizatora, $|x^G| = [G : G_x]$. U konačnom slučaju to je ekvivalentno s $|G| = |G_x| \cdot |x^G|$.*

Dokaz. Vrijedi $gx = hx \iff (h^{-1}g)x = x \iff h^{-1}g \in G_x \iff g$ i h pripadaju istoj lijevoj klasi modulo G_x. Zato je $gG_x \mapsto gx$ dobro definirana bijekcija sa skupa lijevih klasa na orbitu x^G. ■

Lema 1.19 (Burnside) *Neka G djeluje na konačan skup X. Ako s n označimo broj orbita, a s $f(g)$ broj elemenata skupa $\{x \in X \mid gx = x\}$, onda vrijedi*

$$|G| \cdot n = \sum_{g \in G} f(g).$$

Dokaz. Prebrojimo na dva načina članove skupa

$$\{(g, x) \in G \times X \mid gx = x\}.$$

Za čvrsti g broj parova u skupu je $f(g)$. Zato je ukupan broj parova jednak sumi $\sum_{g \in G} f(g)$. S druge strane, za čvrsti x broj parova je $|G_x|$, pa je ukupan broj parova

$$\sum_{x \in X} |G_x| = (\text{propozicija } 1.18) = \sum_{x \in X} \frac{|G|}{|x^G|} = |G| \cdot \sum_{x \in X} \frac{1}{|x^G|} = |G| \cdot n$$

Formula slijedi izjednačavanjem. ■

Definicija 1.20 *Neka je $S = (\mathcal{P}, \mathcal{L}, I)$ incidencijska struktura. Za grupu G koja djeluje na točke i pravce tako da vrijedi $T\ I\ \ell \iff gT\ I\ g\ell$, za $g \in G$, $T \in \mathcal{P}$, $\ell \in \mathcal{L}$ kažemo da je* **grupa automorfizama** *od S.*

Definicija 1.21 *Incidencijske strukture $S_1 = (\mathcal{P}_1, \mathcal{L}_1, I_1)$, $S_2 = (\mathcal{P}_2, \mathcal{L}_2, I_2)$ su* **izomorfne** *ako postoje bijekcije $\varphi : \mathcal{P}_1 \to \mathcal{P}_2$, $\psi : \mathcal{L}_1 \to \mathcal{L}_2$ koje čuvaju incidenciju, tj. takve da za $P \in \mathcal{P}_1$, $\ell \in \mathcal{L}_1$ vrijedi $P\ I_1\ \ell \iff \varphi(P)\ I_2\ \psi(\ell)$. Par (φ, ψ) zovemo* **izomorfizam**. *Skup svih izomorfizama s incidencijske strukture S na samu sebe zovemo* **puna grupa automorfizama** *od S i označavamo* $\mathrm{Aut}(S)$.

Propozicija 1.22 $\mathrm{Aut}(S)$ *je grupa automorfizama od* S*. Svaka grupa automorfizama od* S *ulaže se u* $\mathrm{Aut}(S)$*.*

Dokaz. $\mathrm{Aut}(S)$ djeluje na točke i pravce na prirodan način,

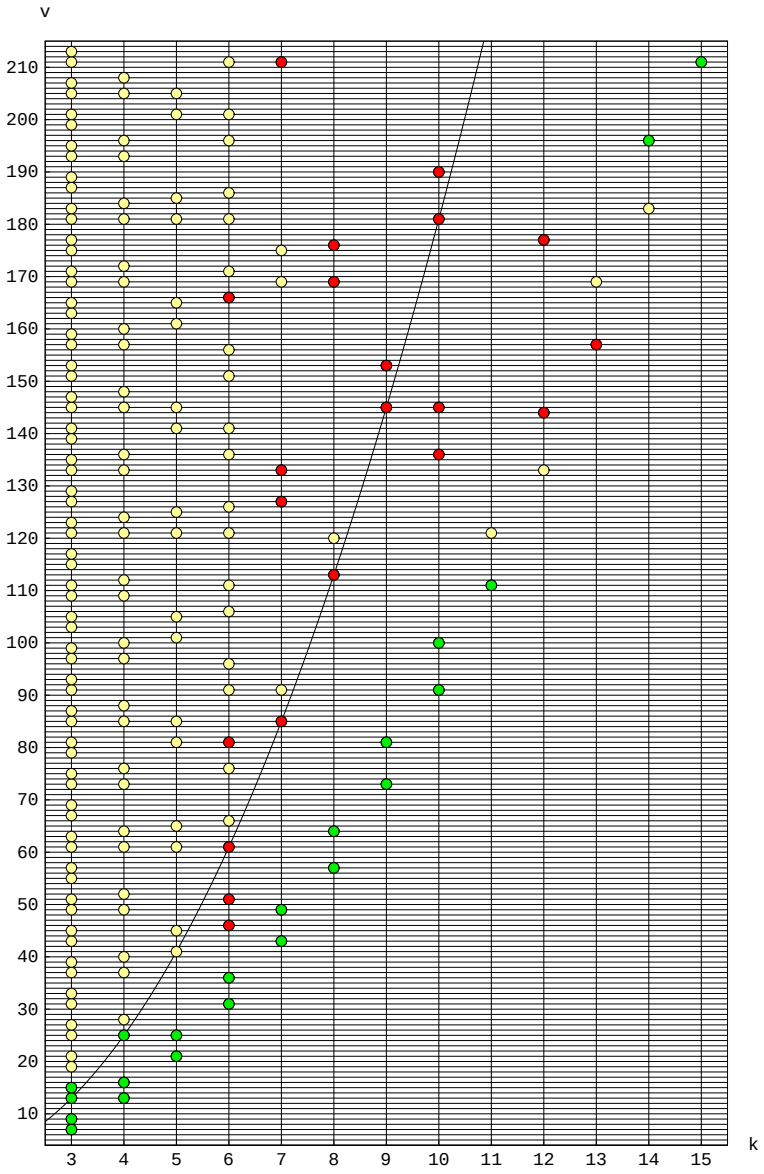
$$(\varphi, \psi)T = \varphi(T), \quad (\varphi, \psi)\ell = \psi(\ell).$$

Po definiciji pritom se čuva incidencija. Ako je G grupa automorfizama od S i $g \in G$, definiramo funkcije $\varphi_g : \mathcal{P} \to \mathcal{P}$, $\varphi_g(T) = gT$ i $\psi_g : \mathcal{L} \to \mathcal{L}$, $\psi_g(\ell) = g\ell$. Par (φ_g, ψ_g) je element iz $\mathrm{Aut}(S)$, a pridruživanje $g \mapsto (\varphi_g, \psi_g)$ ulaganje grupa. ■

2 Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$

2.1 Osnovna svojstva i primjeri

Tema ovog rada je jedna familija Steinerovih 2-dizajna. Na slici 1 prikazani su dopustivi parametri $S(k, v)$ za $3 \leq k \leq 15$ i $5 \leq v \leq 215$.



Slika 1: Dopustivi parametri Steinerovih 2-dizajna.

Zelenom bojom označeni su parametri za koje je provedena klasifikacija (tj. poznat je točan broj dizajna s tim parametrima). Žutom bojom označeni su parametri za koje dizajni postoje, a crvenom parametri za koje je problem egzistencije otvoren.

Parametri dizajna koje proučavamo leže na paraboli $v = 2k^2 - 2k + 1$. Dopustivi su za svaki $k \geq 3$. Vidimo da su dizajni klasificirani za $k = 3$ i 4, postoje za $k = 5$, a za $k \geq 6$ ne zna se da li postoje. Osim preko parametara možemo ih karakterizirati na još nekoliko načina.

Propozicija 2.1 *Steinerov 2-dizajn ima parametre oblika $S(k, 2k^2 - 2k + 1)$ ako i samo ako je ispunjen bilo koji od sljedećih uvjeta:*

(1) *Broj pravaca dvostruko je veći od broja točaka ($b = 2v$).*

(2) *Broj pravaca kroz bilo koju točku dvostruko je veći od broja točaka na bilo kojem pravcu ($r = 2k$).*

(3) *Za bilo koju točku T i pravac ℓ koji nisu incidentni, broj pravaca kroz T koji sijeku ℓ jednak je broju pravaca kroz T disjunktnih s ℓ.*

Dokaz. Parametri Steinerovog 2-dizajna zadovoljavaju $r = \frac{v-1}{k-1}$ i $b = \frac{v(v-1)}{k(k-1)}$ (korolar 1.7). Zbog toga su uvjeti (1) i (2) ekvivalentni s $v = 2k^2 - 2k + 1$. Uvjet (3) ekvivalentan je uvjetu (2), jer je broj pravaca kroz T koji sijeku ℓ jednak k. ■

U sljedećoj tablici navedeni su svi poznati Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$. U elektroničkoj verziji ovog dokumenta unosi u tablici ujedno su linkovi na odgovarajuće objekte.

Prvi stupac sadrži oznaku dizajna i njegov prikaz u tri formata: kao skup pravaca (`m`), kao incidencijska matrica (`inc`) i kao bipartitni graf (`dre`). Graf je zapisan u obliku koji prepoznaje `dreadnaut`, sučelje za `nauty`. To je program pomoću kojeg možemo izračunati punu grupu automorfizama dizajna (vidi str. 31).

Drugi stupac sadrži apstraktan prikaz pune grupe automorfizama i njezin red. Grupe su analizirane pomoću programa GAP [17], sustava za računalnu algebru specijaliziranog za diskretne algebarske strukture. Unos u drugom stupcu vezan je uz datoteku u GAP–formatu koja sadrži grupu.

U trećem i četvrtom stupcu navedeni su multiskupovi duljina staza na točkama, odnosno pravcima (pod djelovanjem pune grupe automorfizama). Izračunati su također pomoću programa `dreadnaut`.

Dizajn	Puna grupa automorfizama	$\mathcal{P}$-orbite	$\mathcal{L}$-orbite
	$k = 3$		
$S3.1$ (m, inc, dre)	$\mathbb{Z}_3.\mathbb{Z}_{13}$ (39)	13	13, 13
$S3.2$ (m, inc, dre)	D_6 (6)	1, 3, 3, 6	1, 1, 4×3, 6, 6
	$k = 4$		
$S4.1$ (m, inc, dre)	$\mathbb{Z}_3 \times PSL_2(7)$ (504)	1, 24	8, 42
$S4.2$ (m, inc, dre)	$\mathbb{Z}_2.(\mathbb{Z}_3.(\mathbb{Z}_5 \times \mathbb{Z}_5))$ (150)	25	25, 25
$S4.3$ (m, inc, dre)	$\mathbb{Z}_3 \times (\mathbb{Z}_3.\mathbb{Z}_7)$ (63)	1, 3, 21	1, 7, 21, 21
$S4.4$ (m, inc, dre)	$\mathbb{Z}_3.\mathbb{Z}_7$ (21)	1, 3, 3×7	1, 4×7, 21
$S4.5$ (m, inc, dre)	$\mathbb{Z}_3 \times \mathbb{Z}_3$ (9)	1, 3, 3, 9, 9	1, 1, 4×3, 4×9
$S4.6$ (m, inc, dre)	$\mathbb{Z}_3 \times \mathbb{Z}_3$ (9)	1, 3, 3, 9, 9	1, 1, 4×3, 4×9
$S4.7$ (m, inc, dre)	$\mathbb{Z}_3 \times \mathbb{Z}_3$ (9)	1, 3, 3, 9, 9	1, 1, 4×3, 4×9
$S4.8$ (m, inc, dre)	D_6 (6)	1, 4×3, 6, 6	1, 1, 8×3, 4×6
$S4.9$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	1, 8×3	1, 1, 16×3
$S4.10$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	1, 8×3	1, 1, 16×3
$S4.11$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	1, 8×3	1, 1, 16×3
$S4.12$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	1, 8×3	1, 1, 16×3
$S4.13$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	4×1, 7×3	5×1, 15×3
$S4.14$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	4×1, 7×3	5×1, 15×3
$S4.15$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	1, 8×3	1, 1, 16×3
$S4.16$ (m, inc, dre)	$\mathbb{Z}_3$ (3)	1, 8×3	1, 1, 16×3
$S4.17$ (m, inc, dre)	$\langle\,\rangle$ (1)	25×1	50×1
$S4.18$ (m, inc, dre)	$\langle\,\rangle$ (1)	25×1	50×1
	$k = 5$		
$S5.1$ (m, inc, dre)	$\mathbb{Z}_5.\mathbb{Z}_{41}$ (205)	41	41, 41
$S5.2$ (m, inc, dre)	$\mathbb{Z}_2.A_5$ (120)	5, 6, 30	1, 6, 15, 30, 30
$S5.3$ (m, inc, dre)	$\mathbb{Z}_2.A_5$ (120)	5, 6, 30	1, 6, 15, 30, 30
$S5.4$ (m, inc, dre)	$\mathbb{Z}_2.A_4$ (24)	1, 4, 6, 6, 24	1, 3, 3×6, 3×12, 24
$S5.5$ (m, inc, dre)	$\mathbb{Z}_3.Q_8$ (24)	1, 8, 8, 24	4, 6, 3×24
$S5.6$ (m, inc, dre)	$\mathbb{Z}_2.D_{10}$ (20)	1, 4×5, 20	1,1,4×5,10,10,20,20
$S5.7$ (m, inc, dre)	$\mathbb{Z}_3 \times D_6$ (18)	2, 3, 18, 18	1, 3×9, 3×18
$S5.8$ (m, inc, dre)	$\mathbb{Z}_3 \times D_6$ (18)	2, 3, 18, 18	1, 3×9, 3×18
$S5.9$ (m, inc, dre)	$\mathbb{Z}_3 \times D_6$ (18)	2, 3, 18, 18	1, 3×9, 3×18

Tablica 1: Poznati Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$.

Dizajn	Puna grupa automorfizama	$\mathcal{P}$-orbite	$\mathcal{L}$-orbite
$S5.10$ (m, inc, dre)	$\mathbb{Z}_3 \times D_6$ (18)	2, 3, 18, 18	1, 3×9, 3×18
$S5.11$ (m, inc, dre)	D_{12} (12)	2,3,6,6,12,12	1,3×3,6×6,3×12
$S5.12$ (m, inc, dre)	$\mathbb{Z}_3 \times \mathbb{Z}_3$ (9)	1, 1, 3, 4×9	1, 9×9
$S5.13$ (m, inc, dre)	$\mathbb{Z}_6$ (6)	1, 2, 2, 6×6	1, 3×3, 12×6
$S5.14$ (m, inc, dre)	$\mathbb{Z}_6$ (6)	2, 3, 6×6	1, 3×3, 12×6

Tablica 1: Poznati Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$ (nastavak).

U tablici smo za opis strukture pune grupe automorfizama koristili niz oznaka. Direktan produkt grupa označavamo križićem '×', a semidirektan produkt točkom. Slijede oznake za grupe korištene u tablici:

- $\mathbb{Z}_n$ – ciklička grupa reda n
- D_{2n} – diedralna grupa reda $2n$
- $PSL_n(q)$ – projektivna specijalna linearna grupa (kvocijent grupe $n \times n$ matrica determinante 1 nad $GF(q)$ s njezinim centrom, skalarnim matricama)
- A_n – alternirajuća grupa stupnja n (na n slova)
- Q_8 – kvaternionska grupa reda 8

2.2 Podstrukture

Definicija 2.2 *Neka je $S = (\mathcal{P}, \mathcal{L}, I)$ incidencijska struktura. Za $S' = (\mathcal{P}', \mathcal{L}', I')$ kažemo da je* **podstruktura** *od S ako je $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{L}' \subseteq \mathcal{L}$ i $I' = I \cap (\mathcal{P}' \times \mathcal{L}')$. Ako je $\mathcal{P}' \subset \mathcal{P}$ kažemo da je S'* **prava podstruktura** *od S.*

U situaciji kad je zadana incidencijska struktura S i njezina podstruktura S' točke i pravce podstrukture zovemo *nutarnjim*. Pravce koji ne pripadaju podstrukturi ali prolaze kroz neku nutarnju točku zovemo *rubni pravci*, a preostale *vanjski pravci*. Dualno, točku koja ne pripada podstrukturi zovemo *rubna točka* ako leži na nekom pravcu podstrukture, a inače *vanjska točka*.

Definicija 2.3 *Za podstrukturu dizajna kažemo da je* **poddizajn** *ako je i sama dizajn.*

Poddizajni Steinerovih 2-dizajna također su Steinerovi 2-dizajni. Neka su v, b, r, k parametri Steinerovog 2-dizajna, a v', b', r', k' njegovog poddizajna. Očito vrijedi $v' \leq v$ i $k' \leq k$. Promotrimo najprije slučaj $k = k'$.

Propozicija 2.4 *Ako Steinerov 2-dizajn $S(k, v)$ ima pravi poddizajn $S(k, v')$, onda je $v' \leq r$.*

Dokaz. Promotrimo pravce kroz točku T koja ne pripada poddizajnu. Na svakom od njih leži najviše jedna točka poddizajna. U suprotnom bi pravac bio nutarnji, pa bi zbog $k = k'$ točka T pripadala poddizajnu. Zato broj točaka poddizajna nije veći od broja pravaca kroz T, $v' \leq r$. ■

Propozicija 2.5 *Steinerov 2-dizajn $S(k, 2k^2 - 2k + 1)$ ne može imati pravi poddizajn s parametrima $S(k, v')$.*

Dokaz. Pretpostavimo da postoji poddizajn $S(k, v')$. Iz korolara 1.11 primjenjenog na poddizajn i iz prethodne propozicije dobivamo

$$k^2 - k + 1 \leq v' \leq r = 2k \qquad \Longrightarrow \qquad k^2 - 3k + 1 \leq 0$$

Slijedi $k \leq \frac{3+\sqrt{5}}{2} < 3$, a u ovom radu promatramo samo 2-dizajne s $k \geq 3$. ■

U općenitoj situaciji ($k' \leq k$) vrijede sljedeće ocjene za broj točaka pravog poddizajna.

Lema 2.6 *Neka je S' pravi poddizajn Steinerovog 2-dizajna S. Tada vrijedi:*

$$v' \leq r\,(k' - 1) + 1$$

$$(v')^2 - (rk' + 1)v' + bk' \geq 0$$

Dokaz. Označimo broj nutarnjih, rubnih i vanjskih pravaca redom s b_N, b_R i b_V. Prema korolaru 1.7 vrijedi

$$b_N = \frac{v'(v' - 1)}{k'(k' - 1)}$$

Prebrojavanjem incidentnih parova (nutarnja točka, pravac) dobivamo jednadžbu $v'r = b_R + k'b_N$. Očito je $b_N + b_R + b_V = b$. Rješavanjem slijedi

$$b_R = \frac{v'\,(r\,(k' - 1) + 1 - v')}{k' - 1}$$

$$b_V = \frac{(v')^2 - (rk' + 1)v' + bk'}{k'}$$

Nejednakosti dobivamo iz $b_R \geq 0$ i $b_V \geq 0$.

■

Pomoću prethodne leme možemo odrediti koji su poddizajni načelno mogući u dizajnima sa zadanim parametrima. Promotrimo pobliže poznate dizajne iz serije koju proučavamo, $S(3, 13)$, $S(4, 25)$ i $S(5, 41)$.

Propozicija 2.7 *Steinerovi 2-dizajni $S(3, 13)$ nemaju pravih poddizajna.*

Dokaz. Slijedi iz propozicije 2.5.

■

Propozicija 2.8 *Ako Steinerov 2-dizajn $S(4, 25)$ ima pravi poddizajn, njegovi parametri su $S(3, 7)$ (tj. radi se o projektivnoj ravnini reda dva).*

Dokaz. Poddizajni $S(4, v')$ nisu mogući zbog 2.5. Za poddizajne $S(3, v')$ iz leme 2.6 dobivamo ocjene $v' \leq 17$ i $(v')^2 - 25v' + 150 \geq 0$. Nejednakosti zadovoljavaju tri dopustiva v', 7, 9 i 15.

U slučaju poddizajna $S(3, 15)$ broj vanjskih pravaca bio bi $b_V = 0$ (vidi dokaz leme 2.6). Neka je T točka koja ne pripada poddizajnu. Označimo broj nutarnjih pravaca kroz T s r_N, a rubnih s r_R. Vanjskih pravaca nema, pa je $r_N + r_R = r = 8$. Rubni pravci sadrže po jednu točku poddizajna, a nutarnji po tri, iz čega slijedi $3r_N + r_R = v' = 15$. Rješavanjem jednadžbi dobivamo kontradikciju, $r_N = \frac{7}{2}$ i $r_R = \frac{9}{2}$. Dakle, ne postoje $S(3, 15)$ poddizajni.

Za poddizajn $S(3, 9)$ ukupni broj vanjskih pravaca je $b_V = 2$. Neka su r_N, r_R i r_V broj nutarnjih, rubnih i vanjskih pravaca kroz točku T koja ne pripada poddizajnu. Brojevi zadovoljavaju $r_N + r_R + r_V = r = 8$ i $3r_N + r_V = v' = 9$, iz čega oduzimanjem slijedi $2r_N = 1 + r_V$. Očito je $0 \leq r_V \leq b_V = 2$; broj r_N je prirodan samo za $r_R = 1$. Dakle, kroz proizvoljnu ne-nutarnju točku prolazi točno jedan vanjski pravac. To je kontradikcija, jer dva vanjska pravca mogu pokriti najviše 8 od ukupno $v - v' = 16$ točaka izvan poddizajna.

Preostaje jedino mogućnost poddizajna $S(3, 7)$.

■

U tablici 2 vidimo koliko stvarno ima poddizajna u pojedinim $S(4, 25)$ dizajnima. Rezultati su dobiveni programom `subsearch`, koji sustavno traži poddizajne sa zadanim parametrima.

Propozicija 2.9 *Ako Steinerov 2-dizajn $S(5, 41)$ ima pravi poddizajn, njegovi parametri su $S(3, 7)$, $S(3, 9)$, $S(3, 19)$ ili $S(3, 21)$.*

Dizajn	# $S(3,7)$	Dizajn	# $S(3,7)$	Dizajn	# $S(3,7)$
$\mathcal{S}4.1$	24	$\mathcal{S}4.7$	3	$\mathcal{S}4.13$	3
$\mathcal{S}4.2$	0	$\mathcal{S}4.8$	0	$\mathcal{S}4.14$	3
$\mathcal{S}4.3$	24	$\mathcal{S}4.9$	3	$\mathcal{S}4.15$	0
$\mathcal{S}4.4$	3	$\mathcal{S}4.10$	3	$\mathcal{S}4.16$	0
$\mathcal{S}4.5$	12	$\mathcal{S}4.11$	3	$\mathcal{S}4.17$	1
$\mathcal{S}4.6$	3	$\mathcal{S}4.12$	0	$\mathcal{S}4.18$	1

Tablica 2: Poddizajni u Steinerovim 2-dizajnima $S(4,25)$.

Dokaz. Zbog propozicije 2.5 ne postoje poddizajni $S(5,v')$. Lema 2.6 za $S(4,v')$ daje ocjene $v' \leq 31$ i $(v')^2 - 41v' + 328 \geq 0$, koje ne zadovoljava ni jedan dopustivi v'. Za poddizajne $S(3,v')$ dobivamo samo jedan uvjet, $v' \leq 21$. Dolaze u obzir $v' = 7, 9, 13, 15, 19$ i 21.

Obzirom na poddizajn $S(3,15)$ dva pravca su vanjska ($b_V = 2$). Kao i u dokazu propozicije 2.8, neka su r_N, r_R i r_V broj nutarnjih, rubnih i vanjskih pravaca kroz neku točku izvan poddizajna. Vrijedi $r_N + r_R + r_V = r = 10$ i $3r_N + r_R = v' = 15$. Oduzimanjem dobivamo $2r_N = 5 + r_V$, iz čega slijedi $r_V = 1$ (jer r_N mora biti prirodan i $0 \leq r_V \leq b_V = 2$). Dakle, kroz svaku točku koja ne pripada poddizajnu prolazi jedan vanjski pravac. To je kontradikcija jer dva vanjska pravca pokrivaju najviše 10 točaka.

U slučaju poddizajna $S(3,13)$ broj vanjskih pravaca je $b_V = 4$. Brojevi r_N, r_R i r_V zadovoljavaju $r_N + r_R + r_V = 10$ i $3r_N + r_R = 13$, iz čega slijedi $2r_N = 3 + r_V$. Sad je $0 \leq r_V \leq 4$, pa imamo dvije mogućnosti: $r_V = 1$ ili $r_V = 3$. Označimo s v_1 broj točaka izvan poddizajna kroz koje prolazi jedan vanjski pravac, a s v_2 broj točaka kroz koje prolaze tri vanjska pravca. Očito je $v_1 + v_2 = v - v' = 28$. Prebrojavanjem incidentnih parova (točka izvan poddizajna, vanjski pravac) slijedi $v_1 + 3v_2 = b_V \cdot k = 20$. Rješavanjem dobivamo kontradikciju, $v_2 = -4$. Dakle, ne postoje niti $S(3,13)$ poddizajni. ■

U tablici 3 vidimo broj $S(3,7)$ i $S(3,9)$ poddizajna u poznatim $S(5,41)$ dizajnima. Program `subsearch` nažalost nije dovoljno brz za prebrojavanje $S(3,19)$ i $S(3,21)$ poddizajna.

Među podstrukturama Steinerovog 2-dizajna poddizajni su karakterizirani sljedećim uvjetima:

(a) Na pravcima podstrukture leži konstantan broj točaka podstrukture.

(b) Kroz točke podstrukture prolazi konstantan broj pravaca podstrukture.

Dizajn	# $S(3,7)$	# $S(3,9)$	Dizajn	# $S(3,7)$	# $S(3,9)$
$S5.1$	0	0	$S5.8$	0	18
$S5.2$	120	30	$S5.9$	36	0
$S5.3$	0	0	$S5.10$	0	0
$S5.4$	48	0	$S5.11$	6	12
$S5.5$	0	6	$S5.12$	36	0
$S5.6$	40	0	$S5.13$	18	0
$S5.7$	36	0	$S5.14$	0	0

Tablica 3: Poddizajni u Steinerovim 2-dizajnima $S(5,41)$.

(c) Svake dvije točke podstrukture spojene su pravcem koji pripada podstrukturi.

Zanemarivanjem posljednjeg uvjeta dolazimo do podstruktura koje su konfiguracije.

Definicija 2.10 *Za incidencijsku strukturu od v točaka i b pravaca kažemo da je (v_r, b_k)* **konfiguracija** *ako zadovoljava:*

(1) *Na svakom pravcu leži k točaka.*

(2) *Kroz svaku točku prolazi r pravaca.*

(3) *Svake dvije točke spojene su najviše jednim pravcem.*

Nužni uvjeti postojanja (v_r, b_k) konfiguracije su $vr = bk$ i $v \geq r(k-1)+1$. Ako je $v = b$ (ili ekvivalentno $r = k$) kažemo da je konfiguracija *simetrična* i parametre bilježimo v_r.

Definicija 2.11 *Neka je $S = (\mathcal{P}, \mathcal{L}, I)$ incidencijska struktura, a $\ell \in \mathcal{L}$ pravac. Podstruktura $S^{(\ell)}$ sastoji se od točaka $\mathcal{P}' = \mathcal{P} \setminus (\ell)$ i pravaca $\mathcal{L}' = \{\ell' \in \mathcal{L} \mid \ell \text{ i } \ell' \text{ su disjunktni}\}$.*

Propozicija 2.12 *U Steinerovom 2-dizajnu S s parametrima v, b, r, k podstruktura $S^{(\ell)}$ je $((v-k)_{r-k}, (b-k(r-1)-1)_k)$ konfiguracija.*

Dokaz. Broj točaka u $S^{(\ell)}$ očito je $|\mathcal{P}| - |(\ell)| = v - k$. Kroz svaku točku na ℓ prolazi još $r-1$ pravaca, pa ℓ siječe ukupno $k(r-1)$ pravaca (i naravno sam sebe). Pravci podstrukture su oni koji ne sijeku ℓ; ima ih $b-k(r-1)-1$.

Kroz svaku točku podstrukture prolazi $r-k$ pravaca podstrukture (od ukupno r pravaca njih k su spojnice s točkama na ℓ). Pravci podstrukture disjunktni su s ℓ, pa sve točke na njima pripadaju podstrukturi. Dakle, svaki pravac podstrukture sadrži k točaka podstrukture.

Konačno, uvjet (3) iz definicije konfiguracije zadovoljen je u svakoj podstrukturi Steinerovog 2-dizajna.

■

Korolar 2.13 *Steinerov 2-dizajn S ima parametre oblika $S(k, 2k^2-2k+1)$ ako i samo ako su konfiguracije $S^{(\ell)}$ simetrične. Parametri tih konfiguracija su $(2k^2-3k+1)_k$.*

Propozicija 2.14 *Neka pravci ℓ_1 i ℓ_2 incidencijske strukture S pripadaju istoj orbiti pod djelovanjem pune grupe automorfizama $\mathrm{Aut}(S)$. Tada su konfiguracije $S^{(\ell_1)}$ i $S^{(\ell_2)}$ izomorfne.*

Dokaz. Neka je $S^{(\ell_1)} = (\mathcal{P}_1, \mathcal{L}_1, I_1)$ i $S^{(\ell_2)} = (\mathcal{P}_2, \mathcal{L}_2, I_2)$. Po pretpostavci postoji automorfizam $\alpha \in \mathrm{Aut}(S)$ takav da je $\ell_2 = \alpha(\ell_1)$. Funkcije $\alpha|_{\mathcal{P}_1} : \mathcal{P}_1 \to \mathcal{P}_2$ i $\alpha|_{\mathcal{L}_1} : \mathcal{L}_1 \to \mathcal{L}_2$ su dobro definirane bijekcije, a par $(\alpha|_{\mathcal{P}_1}, \alpha|_{\mathcal{L}_1})$ izomorfizam između $S^{(\ell_1)}$ i $S^{(\ell_2)}$.

■

Obrat propozicije ne vrijedi. U dizajnu $S3.2$ postoje pravci koji induciraju izomorfne konfiguracije, ali pripadaju različitim orbitama.

Definicija 2.15 *Neka je C (v_r, b_k) konfiguracija.* **Konfiguracijski graf** *$\mathcal{G}(C)$ ima za vrhove točke od C, a za bridove parove točaka koje nisu spojene pravcem u C.*

Graf (v_r, b_k) konfiguracije je d-regularan, za $d = v - r(k-1) - 1$. Parametar d naziva se *defekt*. Konfiguracije defekta nula podudaraju se sa Steinerovim 2-dizajnima.

Definicija 2.16 *Neka je C simetrična $(2k^2-3k+1)_k$ konfiguracija.* **Rastav na klike** *konfiguracijskog grafa $\mathcal{G}(C)$ je particija skupa vrhova na potpune podgrafove K_{k-1}. Za dva rastava na klike kažemo da su* **ortogonalni** *ako ne sadrže isti brid od $\mathcal{G}(C)$.*

Teorem 2.17 (Gropp) *Simetrična $(2k^2-3k+1)_k$ konfiguracija C je oblika $C = S^{(\ell)}$ za neki Steinerov 2-dizajn S ako i samo ako graf $\mathcal{G}(C)$ dopušta k međusobno ortogonalnih rastava na klike.*

Dokaz. Pretpostavimo da je $C = S^{(\ell)}$ za pravac ℓ Steinerovog 2-dizajna $S(k, 2k^2 - 2k + 1)$. Svakoj točki T na ℓ odgovara rastav na klike grafa $\mathcal{G}(C)$: pravci kroz T (različiti od ℓ) čine particiju konfiguracije na $2k-1$ blokova od po $k-1$ točaka. Unutar jednog bloka točke nisu spojene pravcima konfiguracije, jer su spojene pravcem koji siječe ℓ (u točki T). Prema tome, blokovi su potpuni podgrafovi grafa $\mathcal{G}(C)$.

Rastavi na klike koji odgovaraju dvjema različitim točkama su ortogonalni. U suprotnom bi sadržali isti brid grafa $\mathcal{G}(C)$, tj. neki blok prvog rastava i neki blok drugog rastava imali bi dvije zajedničke točke. To bi značilo da se odgovarajući pravci sijeku u dvije točke, što u Steinerovom 2-dizajnu nije moguće.

Za obrat neka su $R^{(i)} = \{B_1^{(i)}, \ldots, B_{2k-1}^{(i)}\}$, $i = 1, \ldots, k$ međusobno ortogonalni rastavi na klike grafa $\mathcal{G}(C)$. Proširujemo konfiguraciju točkama $1, 2, \ldots, k$, pravcem $\ell = \{1, \ldots, k\}$ i pravcima $B_j^{(i)} \cup \{i\}$. Za nove pravce incidencija je relacija pripadanja $\in$. Pokazuje se da je proširena struktura S Steinerov 2-dizajn $S(k, 2k^2 - 2k + 1)$ i da je $C = S^{(\ell)}$. ■

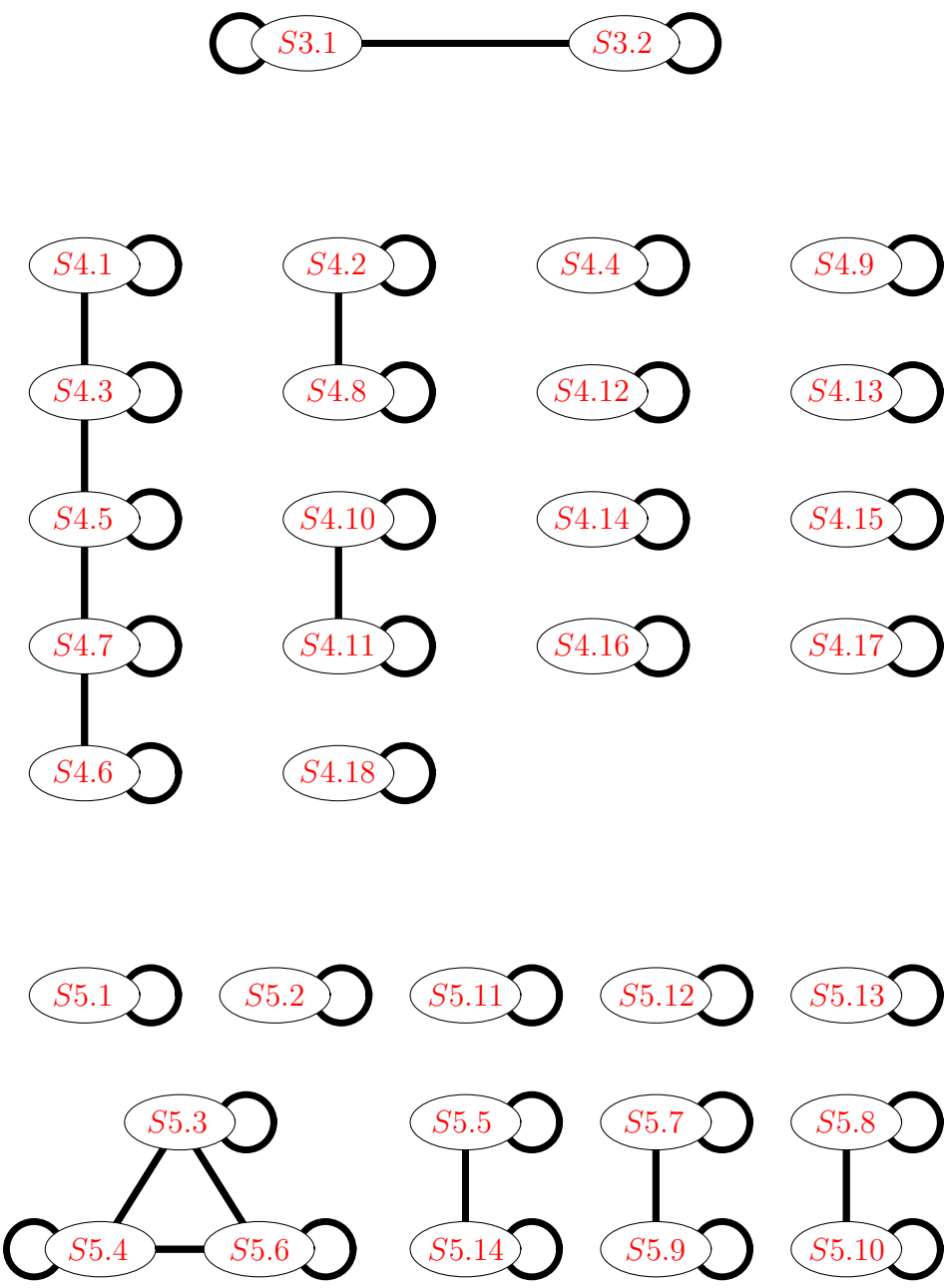
Napomena 2.18 Prema [6], H.Gropp je teorem izložio 1986. na kombinatoričkoj konferenciji u Cataniji (Italija). Predložio je klasifikaciju $S(4, 25)$ dizajna pomoću simetričnih konfiguracija 21_4.

Gropp je proveo klasifikaciju za $k = 3$. Najprije je klasificirao konfiguracije 10_3, kojih ima ukupno 10 (među njima je Desarguesova konfiguracija). Zatim ih je, koristeći teorem 2.17 proširivao do $S(3, 13)$ dizajna. Jednu od konfiguracija moguće je proširiti do $S3.1$ i $S3.2$, jedna se proširuje samo do $S3.1$, šest samo do $S3.2$, a dvije (uključujući Desarguesovu) nije moguće proširiti. Zaključujemo da su $S3.1$ i $S3.2$ jedini $S(3, 13)$ dizajni.

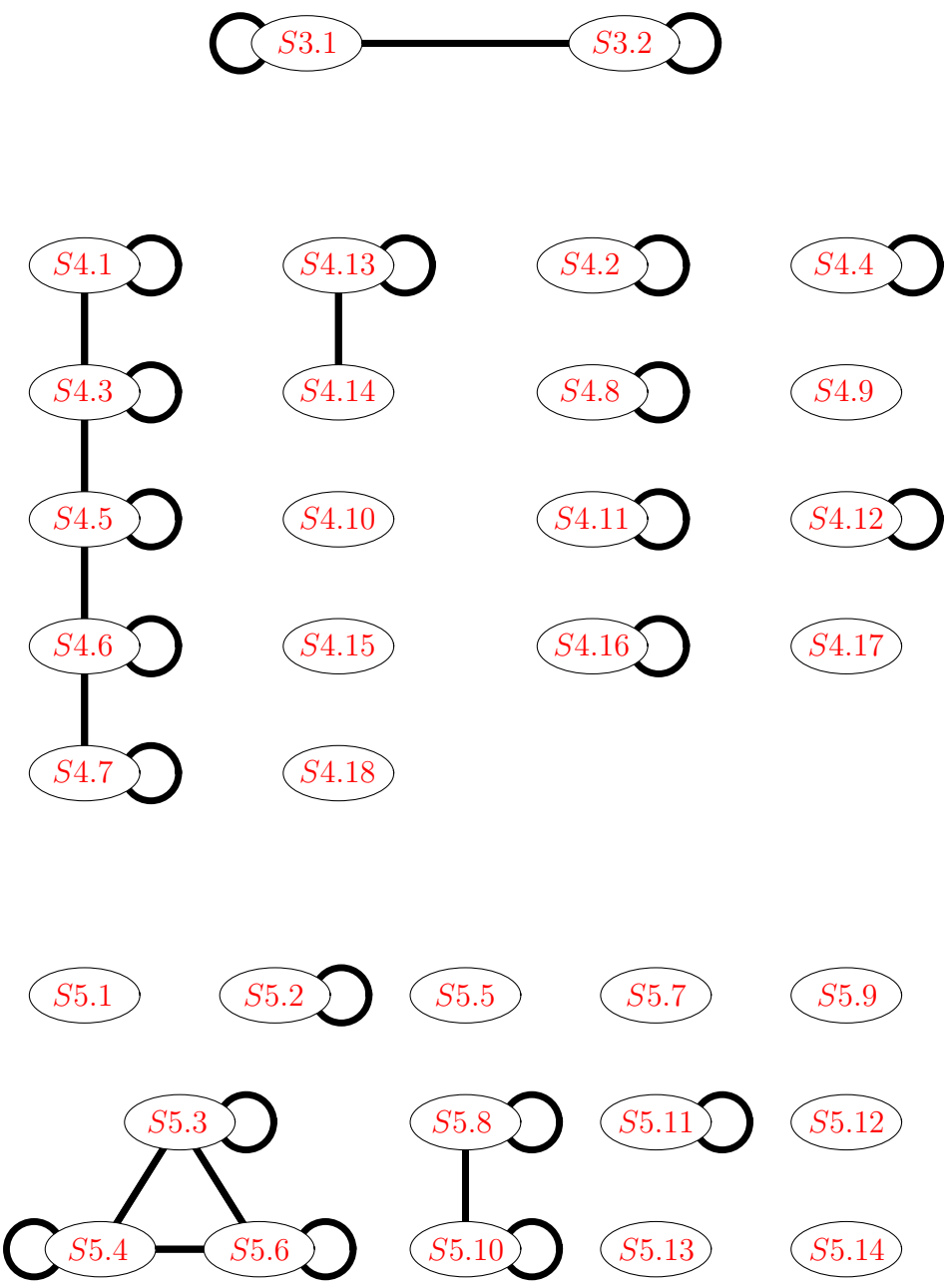
Međutim, čini se da ideja nije provediva za $k = 4$, zbog prevelikog broja neizomorfnih 21_4 konfiguracija. Dizajne $S(4, 25)$ klasificirao je E.Spence 1996. godine, na drugi način (vidi 3.26).

Steinerove 2-dizajne $S(k, 2k^2 - 2k + 1)$ možemo pomoću $(2k^2 - 3k + 1)_k$ konfiguracija organizirati u graf $\mathcal{G}$. Vrhovi grafa su neizomorfni $S(k, 2k^2 - 2k + 1)$ dizajni. Vrhovi S_1 i S_2 spojeni su bridom ako postoje pravci ℓ_1 u S_1 i ℓ_2 u S_2 takvi da su konfiguracije $S_1^{(\ell_1)}$ i $S_2^{(\ell_2)}$ izomorfne. Očito je svaki vrh spojen sam sa sobom, tj. graf $\mathcal{G}$ sadrži sve petlje. Nadalje, povezani mogu biti samo dizajni s istim parametrima. Poznati dio grafa prikazan je na slici 2.

Na sličan način definiramo graf $\mathcal{G}^d$. Vrhovi S_1 i S_2 spojeni su bridom ako su konfiguracije $S_1^{(\ell_1)}$ i $(S_2^{(\ell_2)})^d$ izomorfne, za pravce ℓ_1 iz S_1 i ℓ_2 iz S_2. Pritom je C^d dualna konfiguracija od C, dobivena zamjenom uloge točaka i pravaca (transponiranjem incidencijske matrice). Poznati dio grafa vidimo na slici 3.



Slika 2: Graf $\mathcal{G}$.



Slika 3: Graf $\mathcal{G}^d$.

Od poznatog dizajna S možemo konstruirati sve dizajne u istoj komponenti povezanosti grafa $\mathcal{G}$ ili $\mathcal{G}^d$. Konstruiramo konfiguracije $S^{(\ell)}$ (ili njima dualne), eliminiramo izomorfne i preostale konfiguracije proširujemo na sve moguće načine do $S(k, 2k^2 - 2k + 1)$ dizajna. Tako dobivamo dizajne koji su sa S povezani bridom u $\mathcal{G}$ ili $\mathcal{G}^d$. Postupak ponavljamo dok ne prijeđemo čitavu komponentu povezanosti.

Napisao sam niz programa za provedbu tog postupka. Program `extract` konstruira incidencijske matrice konfiguracija, a `incfilter` propušta samo neizomorfne (vidi str. 32). Za proširivanje konfiguracija napisao sam program `embed`. Program traži ortogonalne rastave na klike konfiguracijskog grafa i primjenjuje konstrukciju iz teorema 2.17. S algoritamskog stanovišta problem se svodi na višestruko traženje klika (potpunih podgrafova) u prikladno definiranim grafovima. Prvo tražimo $(k-1)$-klike u konfiguracijskom grafu. U drugom koraku definiramo graf čiji su vrhovi pronađene $(k-1)$-klike, pri čemu su bridom spojene one koje su disjunktne. Klika od $2k-1$ vrhova u tom grafu ekvivalentna je rastavu na klike konfiguracijskog grafa. Konačno, definiramo graf čiji su vrhovi rastavi na klike, a bridovi parovi međusobno ortogonalnih rastava na klike. U trećem koraku tražimo k-klike u tom grafu, što nam daje skupove od k međusobno ortogonalnih rastava na klike konfiguracijskog grafa.

Postupak je već za $k = 5$ prilično dugotrajan, ali broj konfiguracija koje treba proširivati nije prevelik. Od dizajna S možemo dobiti najviše onoliko neizomorfnih konfiguracija koliko je $\mathrm{Aut}(S)$-orbita na pravcima, i isto toliko dualnih (propozicija 2.14).

Na ovaj način prvi put su konstruirani neki od $S(4, 25)$ dizajna. Prema [8], A.Y.Petrenyuk je konstruirao dizajne povezane sa $S4.1$, $S4.2$ i $S4.3$ i tako dobio četiri nova dizajna. A.Rosa i R.Mathon konstruirali su jedan novi $S(5, 41)$ dizajn. Krenuli su od dizajna koji posjeduju automorfizam reda 5 (vidi teorem 5.31) i dobili dizajn $S5.4$. Primjenom transformacije na dizajne prvi put konstruirane u ovom radu (teorem 5.33) ne dobivaju se novi $S(5, 41)$ dizajni.

2.3 Paralelizam i rezolucije

Za pravce incidencijske strukture kažemo da su *paralelni* ako se podudaraju ili ako nemaju zajedničkih točaka. Dualno, točke su *paralelne* ako se podudaraju ili ako nisu spojene pravcem. U Steinerovom 2-dizajnu ne postoje parovi paralelnih točaka, ali mogu postojati parovi paralelnih pravaca.

Definicija 2.19 *Neka je $S = (\mathcal{P}, \mathcal{L}, I)$ incidencijska struktura.* **Klasa paralelizma** *u S je skup međusobno paralelnih pravaca koji čine particiju skupa $\mathcal{P}$*

(tj. pokrivaju sve točke). **Rezolucija** *od S je particija skupa pravaca $\mathcal{L}$ na međusobno disjunktne klase paralelizma. Za incidencijsku strukturu koja dopušta rezoluciju kažemo da je* **rješiva**.

Pretpostavimo da u Steinerovom 2-dizajnu $S(k, v)$ postoji klasa paralelizma. Očito tada k dijeli v. Ako postoji rezolucija, broj pravaca u klasi paralelizma $\frac{v}{k}$ dijeli ukupni broj pravaca b. Tako dobivamo nužne uvjete za postojanje rješivog $S(k, v)$ dizajna, $v \equiv 0 \pmod{k}$ i $v \equiv 1 \pmod{k-1}$. Parametri ih zadovoljavaju ako i samo ako su oblika $S(k, k(mk - m + 1))$.

Uvrštavanjem $m = 1$ dobivamo parametre afinih ravnina $S(k, k^2)$. Poznato je da svaka afina ravnina ima jedinstvenu rezoluciju. Najmanji dopustivi parametri za rješivi Steinerov 2-dizajn koji nije afina ravnina su $S(3, 15)$. Postoji 80 takvih dizajna (primjer 3.25), od čega je 4 rješivo. T.P.Kirkman je u svom poznatom problemu 15 djevojčica zapravo tražio rješive $S(3, 15)$ dizajne.

Parametri dizajna koje proučavamo, $S(k, 2k^2 - 2k + 1)$ ne zadovoljavaju nužne uvjete za rješivost. Modificirat ćemo pojam rezolucije tako da bude prikladan za naše dizajne.

Definicija 2.20 *Neka je $S = (\mathcal{P}, \mathcal{L}, I)$ incidencijska struktura, a $T \in \mathcal{P}$ točka.* **Skoro-klasa paralelizma** *u S je skup međusobno paralelnih pravaca koji čine particiju skupa $\mathcal{P} \setminus \{T\}$ (tj. pokrivaju sve točke osim T).* **Skoro-rezolucija** *od S obzirom na T je particija skupa pravaca koji ne sadrže T ($\mathcal{L} \setminus (T)$) na međusobno disjunktne skoro-klase paralelizma. Za incidencijsku strukturu koja dopušta skoro-rezoluciju kažemo da je* **skoro-rješiva** *(obzirom na T).*

Ako u Steinerovom 2-dizajnu postoji skoro-klasa paralelizma, k dijeli $v - 1$. Ako postoji skoro-rezolucija, $\frac{v-1}{k}$ dijeli $b - r$. Slijede nužni uvjeti za skoro-rješivost Steinerovog 2-dizajna, $v \equiv 1 \pmod{k}$ i $v \equiv 1 \pmod{k-1}$. Parametri ih zadovoljavaju ako i samo ako su oblika $S(k, mk^2 - mk + 1)$.

Uvrštavanjem $m = 1$ dobivamo parametre projektivnih ravnina $S(k, k^2 - k + 1)$. Za razliku od afinih ravnina koje su rješive, projektivne ravnine nisu skoro-rješive. Svaka dva pravca projektivne ravnine sijeku se u jednoj točki, pa uopće ne postoje parovi paralelnih pravaca.

Za $m = 2$ dobivamo parametre dizajna koje proučavamo, $S(k, 2k^2 - 2k + 1)$. Tablica 4 sadrži podatke o broju skoro-klasa paralelizma i skoro-rezolucija u svim poznatim primjerima.

Vidimo da je jedino dizajn $S4.1$ skoro-rješiv, i to samo obzirom na specijalnu točku koja je orbita pune grupe automorfizama. Podaci u tablici dobiveni su pomoću programa `nrsearch`. Problem pronalaženja (skoro) rezolucija svodi se na dvostruko traženje klika, slično kao u programu `embed`. Da bi

Dizajn	# s.k.p.	# s.r.	Dizajn	# s.k.p.	# s.r.
$S3.1$	13	0	$S4.16$	0	0
$S3.2$	8	0	$S4.17$	0	0
$S4.1$	28	11	$S4.18$	0	0
$S4.2$	25	0	$S5.1$	0	0
$S4.3$	0	0	$S5.2$	0	0
$S4.4$	0	0	$S5.3$	0	0
$S4.5$	3	0	$S5.4$	0	0
$S4.6$	1	0	$S5.5$	0	0
$S4.7$	3	0	$S5.6$	0	0
$S4.8$	9	0	$S5.7$	0	0
$S4.9$	0	0	$S5.8$	0	0
$S4.10$	0	0	$S5.9$	0	0
$S4.11$	0	0	$S5.10$	0	0
$S4.12$	1	0	$S5.11$	0	0
$S4.13$	0	0	$S5.12$	0	0
$S4.14$	0	0	$S5.13$	0	0
$S4.15$	3	0	$S5.14$	0	0

Tablica 4: Skoro-klase paralelizma i skoro-rezolucije u $S(k, 2k^2 - 2k + 1)$.

našli sve (skoro) klase paralelizma tražimo klike u grafu čiji su vrhovi pravci, a bridovi parovi paralelnih pravaca. Drugi put tražimo klike u grafu čiji su vrhovi (skoro) klase paralelizma. Bridom su spojene klase koje su međusobno disjunktne.

Definicija 2.21 *Neka su* $\mathcal{R} = \{P_1, \ldots, P_n\}$ *i* $\mathcal{R}' = \{P'_1, \ldots, P'_n\}$ *(skoro) rezolucije incidencijske strukture* S*, pri čemu su* P_i*,* P'_j *(skoro) klase paralelizma. Kažemo da su* $\mathcal{R}$ *i* $\mathcal{R}'$ **ortogonalne** *ako vrijedi* $|P_i \cap P'_j| \leq 1$*, za sve* $i, j = 1, \ldots, n$*.*

Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$ s dovoljnim brojem međusobno ortogonalnih skoro-rezolucija u vezi su s vrlo zanimljivim konačnim strukturama, tzv. eliptičkim poluravninama.

Definicija 2.22 Eliptička (v, k) **poluravnina** *je incidencijska struktura koja zadovoljava aksiome:*

(1) *Ukupni broj točaka je* v*.*

(2) *Na svakom pravcu leži* k *točaka i kroz svaku točku prolazi* k *pravaca.*

(3) *Svake dvije točke spojene su najviše jednim pravcem.*

(4) *Za svaku točku T i pravac ℓ koji nisu incidentni najviše jedan pravac kroz T paralelan je s ℓ i najviše jedna točka na ℓ paralelna je s T.*

Napomena 2.23 Prebrojavanjem incidentnih parova vidimo da je ukupni broj pravaca također v. Očito vrijedi i dual aksioma (3) (svaka dva pravca sijeku se najviše u jednoj točki). Prema tome, dualna struktura je također eliptička (v, k) poluravnina. Eliptičke poluravnine mogli smo kraće definirati kao simetrične v_k konfiguracije koje zadovoljavaju samodualni aksiom (4). Primjeri eliptičkih poluravnina su konačne projektivne ravnine i strukture koje od njih dobivamo izbacivanjem Baerovih (gustih) zatvorenih podstruktura.

Napomena 2.24 U incidencijskoj strukturi pod *stupnjem* točke (pravca) podrazumijevamo broj s njom incidentnih pravaca (točaka). *Red* strukture je maksimalni stupanj umanjen za jedan. P.Dembowski je u knjizi [5] definirao *poluravninu* kao incidencijsku strukturu koja zadovoljava aksiome (3) i (4) i u kojoj je svaki element stupnja bar tri. Pokazao je da u konačnoj poluravnini reda n skup stupnjeva svih elemenata može biti samo $\{n-1, n, n+1\}$, $\{n, n+1\}$ ili $\{n+1\}$. U prvom slučaju poluravnine je nazvao *hiperboličkim*, u drugom *paraboličkim*, a u trećem *eliptičkim*. Red eliptičke (v, k) poluravnine je $n = k - 1$.

Važnu ulogu pri rasvjetljavanju veze eliptičkih poluravnina i $S(k,\, 2k^2 - 2k + 1)$ dizajna igra vrlo općenita klasa incidencijskih struktura, koje se na engleskom zovu "group divisible designs". U hrvatskom se još nije ustalio naziv, pa ćemo koristiti samo njihove parametre $GDD_\lambda(k, g, v)$. Nažalost način zapisivanja parametara nije kod svih autora isti. Koristimo oblik iz knjige [2].

Definicija 2.25 *Za incidencijsku strukturu kažemo da je $GDD_\lambda(k, g, v)$ ako vrijedi:*

(1) *Ukupni broj točaka je v.*

(2) *Svaki pravac sadrži k točaka.*

(3) *Postoji particija skupa točaka na blokove duljine g takva da su parovi točaka iz različitih blokova spojeni s λ pravaca, a parovi točaka iz istog bloka nisu spojeni pravcem.*

Blokove particije iz (3) *zovemo* **grupe**. *Ako je* $\lambda = 1$, *parametre bilježimo* $GDD(k, g, v)$. *Ako je ukupni broj pravaca također* v, *govorimo o* **simetričnom** $GDD_\lambda(k, g, v)$.

Primjer 2.26 Promotrimo incidencijsku strukturu dobivenu punktiranjem Steinerovog 2-dizajna, tj. uklanjanjem jedne točke i svih pravaca koji kroz nju prolaze. Ukupni broj točaka smanjen je na $v - 1$, ali broj točaka na svakom od preostalih pravaca i dalje je k. Uklonjeni pravci particioniraju preostale točke na r grupa duljine $k - 1$, tako da je zadovoljeno svojstvo (3) za $\lambda = 1$. Prema tome, radi se o $GDD(k, k - 1, v - 1)$.

Obrnuto, ako krenemo od strukture $GDD(k, k-1, v-1)$, nadodamo jednu novu točku, te grupe proširimo novom točkom i proglasimo novim pravcima, dobit ćemo Steinerov 2-dizajn $S(k, v)$. Klasama paralelizma i rezolucijama strukture $GDD(k, k - 1, v - 1)$ odgovaraju skoro-klase paralelizma i skoro-rezolucije dizajna $S(k, v)$ obzirom na uklonjenu/nadodanu točku.

Teorem 2.27 *Incidencijska struktura je eliptička* (v, k) *poluravnina ako i samo ako je simetrični* $GDD(k, g, v)$. *Pritom je* $g = v - k(k - 1)$.

Dokaz. Prvo dokazujemo da je eliptička (v, k) poluravnina simetrični $GDD(k, g, v)$. Treba samo provjeriti svojstvo (3), postojanje particije skupa točaka na grupe. Zbog aksioma (4) iz definicije eliptičke poluravnine paralelizam je relacija ekvivalencije. Za grupe uzmimo klase ekvivalencije na točkama. Kroz bilo koju točku T prolazi k pravaca, a na svakom leži još $k - 1$ točaka. Znači, $k(k - 1)$ točaka nije paralelno s T, tj. proizvoljna grupa sadrži $g = v - k(k - 1)$ točaka. Točke iz iste grupe nisu spojene pravcima (jer su paralelne), a točke iz različitih grupa u parovima su spojene po jednim pravcem (jer nisu paralelne). Dakle, imamo simetrični $GDD(k, g, v)$.

Dokazujemo obrat, da je simetrični $GDD(k, g, v)$ eliptička (v, k) poluravnina. Očito su ispunjeni aksiomi (1) i (3). Za aksiom (2) treba vidjeti da kroz svaku točku prolazi k pravaca. Proizvoljna točka T spojena je pravcem sa svim točkama koje nisu u istoj grupi, njih $v - g$. Na svakom pravcu kroz T leži osim T još $k - 1$ točaka. Dakle, kroz T prolazi $\frac{v-g}{k-1}$ pravaca. Prebrojavanjem incidentnih parova slijedi $v \cdot \frac{v-g}{k-1} = v \cdot k \implies \frac{v-g}{k-1} = k$. Usput smo dobili $g = v - k(k - 1)$.

Još treba provjeriti aksiom (4). Neka je zadana točka T i pravac ℓ koji nisu incidentni. Dvije točke koje nisu spojene pravcem s T leže u istoj grupi, pa ni međusobno nisu spojene pravcem. Zato najviše jedna od njih može ležati na ℓ. Dakle, najviše jedna točka na ℓ paralelna je s T, pa je najmanje

$k-1$ točaka na ℓ spojeno s T. Drugačije rečeno, bar $k-1$ pravaca kroz T siječe ℓ, a to opet znači da je najviše jedan pravac kroz T paralelan s ℓ. Dakle, struktura je eliptička (v,k) poluravnina.

■

Teorem 2.28 (Lamken, Vanstone) *Eliptička (v,k) poluravnina s $g < k-1$ postoji ako i samo ako postoji $GDD(k-g,g,(k-1)(k-g))$ s g međusobno ortogonalnih rezolucija, za $g = v-k(k-1)$.*

Dokaz. Neka je S eliptička (v,k) poluravnina i $g < k-1$. Primjenom prethodnog teorema na dualnu strukturu (koja je također eliptička (v,k) poluravnina) slijedi da pravce možemo podijeliti na grupe duljine g unutar kojih su međusobno paralelni pravci. Odaberimo jednu grupu $\{\ell_1,\ldots,\ell_g\}$. Neka je S' podstruktura od S dobivena brisanjem odabranih pravaca i točaka koje na njima leže. Tvrdimo da je S' $GDD(k-g,g,(k-1)(k-g))$.

Izbrisali smo kg točaka, pa je u S' ostalo $v-kg = k(k-1)+g-kg = (k-1)(k-g)$ točaka. Pravci iz S' sijeku svaki od izbrisanih pravaca, jer ne pripadaju odabranoj grupi. Slijedi da na svakom pravcu iz S' leži $k-g$ točaka iz S'. Nadalje, točka podstrukture spojena je sa svim izbrisanim točkama, pa grupa kojoj pripada leži cijela u S'. Dakle, S' je $GDD(k-g,g,(k-1)(k-g))$.

Pramen pravaca kroz svaku od izbrisanih točaka (bez pripadnog izbrisanog pravca) je klasa paralelizma u S'. Klase paralelizma koje odgovaraju izbrisanim točkama na istom izbrisanom pravcu međusobno su disjunktne. Slijedi da svaki izbrisani pravac određuje rezoluciju podstrukture S'. Tako dobivenih g rezolucija u parovima je ortogonalno. Dvije točke s dva različita izbrisana pravca spojene su najviše jednim pravcem, pa pripadne klase paralelizma imaju najviše jedan zajednički pravac.

Obrnuto, neka je S $GDD(k-g,g,(k-1)(k-g))$ i neka su $\mathcal{R}^{(i)} = \{P_1^{(i)},\ldots,P_k^{(i)}\}$, $i=1,\ldots,g$ međusobno ortogonalne rezolucije ($P_j^{(i)}$ su klase paralelizma). Proširimo S točkama $P_j^{(i)}$, uz definiciju $P_j^{(i)}\ I\ \ell \iff \ell \in P_j^{(i)}$. Nadodajmo još $\mathcal{R}^{(1)},\ldots,\mathcal{R}^{(g)}$ kao nove pravce, uz "$\in$" kao relaciju incidencije. Pokazuje se da je proširena struktura simetrični $GDD(k,g,v)$, odnosno eliptička (v,k) poluravnina.

■

Prethodni teorem dokazan je u [11]. Jedan smjer dokazali su još prije R.D.Baker i G.L.Ebert.

Korolar 2.29 *Steinerov 2-dizajn $S(k,2k^2-2k+1)$ s $k-1$ međusobno ortogonalnih skoro-rezolucija (obzirom na istu točku) postoji ako i samo ako postoji eliptička $((4k-1)(k-1),2k-1)$ poluravnina.*

Dokaz. Prema teoremu 2.28 postojanje eliptičke $((4k-1)(k-1), 2k-1)$ poluravnine ekvivalentno je postojanju $GDD(k, k-1, 2k^2-2k)$ s $k-1$ međusobno ortogonalnih rezolucija. U primjeru 2.26 vidjeli smo da je to ekvivalentno postojanju $S(k, 2k^2-2k+1)$ dizajna s $k-1$ međusobno ortogonalnih skoro-rezolucija.

■

Primjer 2.30 Dizajn $S4.1$ posjeduje 11 skoro-rezolucija, među njima 3 ortogonalne. Punktiranjem u specijalnoj točki dobivamo $GDD(4, 3, 24)$ s 3 međusobno ortogonalne rezolucije. Prema teoremu 2.28, iz njega možemo konstruirati eliptičku $(45, 7)$ poluravninu s $g = 3$. Poluravnina je samodualna i ima $A_7.\mathbb{Z}_3$ kao punu grupu automorfizama (reda 7560). Ta grupa djeluje tranzitivno na točke i pravce.

Napomena 2.31 Glavno pitanje o poluravninama kojim se bavio Dembowski u [5] tiče se njihovog ulaganja u projektivne ravnine. Za hiperboličke i paraboličke poluravnine Dembowski je dokazao da se uvijek ulažu u odgovarajuću projektivnu ravninu. Za eliptičke (v, k) poluravnine dokazao je da vrijedi $g = k$, $g = k-1$ ili $g \leq k - \sqrt{k}$. U prva dva slučaja i ako se u trećem slučaju dostiže jednakost uspio je dokazati da se poluravnina ulaže u projektivnu ravninu reda k. Dembowski je postavio hipotezu da eliptičke poluravnine s $1 < g < k - \sqrt{k}$ ne postoje.

R.D.Baker [1] je 1977. godine konstruirao protuprimjer, eliptičku $(45, 7)$ poluravninu. Njegova poluravnina izomorfna je poluravnini iz primjera 2.30, iako nije dobivena na isti način. Osim Bakerovog primjera poznata je samo još jedna eliptička poluravnina s $1 < g < k - \sqrt{k}$. Radi se o eliptičkoj $(135, 12)$ poluravnini, a konstruirao ju je R.Mathon.

3 Klasifikacija

U ovom poglavlju dokazujemo pomoću računala da Steinerovih 2-dizajna $S(k, 2k^2-2k+1)$ ima točno dva za $k=3$ i točno osamnaest za $k=4$. Algoritam za klasifikaciju je objašnjen u općenitom kontekstu jer na analogan način u petom poglavlju konstruiramo orbitne strukture. Prvi dio poglavlja posvećen je kanonskom preslikavanju, koje igra ključnu ulogu u algoritmu. Opisani su alati za računanje kanonskih predstavnika i pune grupe automorfizama. U drugom dijelu opisan je algoritam za klasifikaciju i njegova primjena na Steinerove 2-dizajne i orbitne strukture.

3.1 Kanonsko preslikavanje

Na početku uvodimo nazive i oznake koje ćemo koristiti u cijelom poglavlju. Neka je X skup *objekata* na kojem djeluje grupa G. Za objekte $A, B \in X$ kažemo da su *izomorfni* i pišemo $A \cong B$ ako postoji $g \in G$ takav da je $B = gA$, tj. ako pripadaju istoj stazi. Stabilizator $G_A = \{g \in G \mid gA = A\}$ zovemo *puna grupa automorfizama* objekta A i označavamo $\mathrm{Aut}(A)$.

Primjer 3.1 Neka je X skup svih incidencijskih struktura sa skupom točaka $\mathcal{P} = \{1, \ldots, v\}$ i skupom pravaca $\mathcal{L} = \{1, \ldots, b\}$. Na njemu djeluje direktni produkt simetričnih grupa $G = S_v \times S_b$, tako da relaciju incidencije $I \subseteq \mathcal{P} \times \mathcal{L}$ preslika u $(\pi, \sigma)I = \{(\pi(i), \sigma(j)) \mid (i,j) \in I\}$, za $(\pi, \sigma) \in G$. Izomorfnost i puna grupa automorfizama obzirom na ovo djelovanje podudaraju se s pojmovima definiranim u uvodu (1.21). Umjesto X možemo uzeti G-invarijantan podskup $X' \subseteq X$, na primjer Steinerove 2-dizajne $S(k, v)$.

Primjer 3.2 Neka je $X = M_{mn}(\mathbb{N}_0)$ skup svih $m \times n$ matrica nad $\mathbb{N}_0$. Grupa $G = S_m \times S_n$ na njemu djeluje permutiranjem redaka i stupaca. Za $(\pi, \sigma) \in G$ i $A = [a_{ij}] \in X$ slika $(\pi, \sigma)A = B = [b_{ij}]$ definirana je s $b_{\pi(i)\sigma(j)} = a_{ij}$. Umjesto X možemo uzeti manji, G-invarijantan skup matrica, na primjer incidencijske matrice Steinerovih 2-dizajna $S(k, v)$.

Primjer 3.3 *Obojani graf* sastoji se od konačnog skupa V, familije dvočlanih podskupova $B \subseteq \mathcal{P}_2(V)$ i funkcije $b : V \to \mathbb{N}$. Elemente iz V zovemo *vrhovi*, elemente iz B *bridovi*, a b *bojanje*. Neka je X skup svih obojanih grafova sa skupom vrhova $V = \{1, \ldots, n\}$, a G simetrična grupa S_n. Djelovanje G na X definiramo formulom $\pi(B, b) = (\pi B, b \circ \pi^{-1})$, gdje je $\pi B = \{\{\pi(i), \pi(j)\} \mid \{i,j\} \in B\}$. Tako dobivamo uobičajene pojmove izomorfnosti i pune grupe automorfizama za grafove, uz uvjet da se samo vrhovi iste boje smiju preslikati jedni na druge.

Definicija 3.4 **Kanonsko preslikavanje** *je svaka funkcija* $c : X \to X$ *koja ima svojstva*

(1) $c(A) \cong A$, *za svaki* $A \in X$

(2) $c(gA) = c(A)$, *za svaki* $g \in G$, $A \in X$

Fiksne točke kanonskog preslikavanja zovemo **kanonski objekti** *ili* **kanonski predstavnici** *obzirom na* c.

Propozicija 3.5 *Ako je* $c : X \to X$ *kanonsko preslikavanje, vrijedi*

$$A \cong B \iff c(A) = c(B)$$

Dokaz. ($\Longrightarrow$) Ako je A izomorfan s B, postoji $g \in G$ takav da je $B = gA$. Slijedi $c(A) = c(gA) = c(B)$.
($\Longleftarrow$) Ako je $c(A) = c(B)$, vrijedi $A \cong c(A) = c(B) \cong B$.
■

Propozicija 3.6 *Neka je zadan totalni uređaj na skupu objekata* X *na kojem djeluje konačna grupa* G. *Tada je funkcija* $c : X \to X$, $c(A) = \max\{gA \mid g \in G\}$ *kanonsko preslikavanje.*

Dokaz. Funkcija je dobro definirana jer su staze $\{gA \mid g \in G\}$ konačni skupovi, pa maksimumi postoje. Očito c zadovoljava svojstva (1) i (2) iz definicije 3.4.
■

Cilj ove točke je razviti algoritam za računanje kanonskog preslikavanja iz prethodne propozicije. Najjednostavniji algoritam je petlja koja prelazi po svim $g \in G$ i pamti najveći među objektima gA. U praksi to nije provedivo jer grupa G ima previše elemenata. Razvit ćemo brži algoritam u specijalnom slučaju matrica nad $\mathbb{N}_0$ (primjer 3.2). Treba nam totalni uređaj na skupu matrica $X = M_{mn}(\mathbb{N}_0)$.

Definicija 3.7 *Neka su* $A = [a_{ij}]$, $B = [b_{ij}] \in M_{mn}(\mathbb{N}_0)$. *Kažemo da je matrica* A **manja** *od matrice* B *i pišemo* $A < B$ *ako postoji par indeksa* $(i_0, j_0) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$ *takav da vrijedi* $a_{i_0 j_0} < b_{i_0 j_0}$ *i* $a_{ij} = b_{ij}$, *za* $i = 1, \ldots, i_0 - 1$, $j = 1, \ldots, n$ *i za* $i = i_0$, $j = 1, \ldots, j_0 - 1$. *Ako je* $A < B$ *ili* $A = B$ *kažemo da je* A **manja ili jednaka** *od* B *i pišemo* $A \leq B$.

Drugim riječima, uspoređujemo obzirom na leksikografski uređaj vektore dobivene spajanjem redaka matrice. Nije teško provjeriti da je definirana relacija totalni uređaj na skupu $X = M_{mn}(\mathbb{N}_0)$.

Da bismo opisali algoritam i dokazali njegovu valjanost trebaju nam neke oznake i činjenice. Neka je V_i skup svih injekcija sa skupa $\{1, \ldots, i\}$ u skup $\{1, \ldots, m\}$. Elemente iz V_i bilježimo kao uređene i-torke; $(\pi_1, \ldots, \pi_i)$ je injekcija koja pridružuje $k \mapsto \pi_k$, $k = 1, \ldots, i$. Elementi iz V_m su permutacije stupnja m, tj. $V_m = S_m$. Definiramo preslikavanje $(A, \pi) \mapsto A\pi \in M_{in}(\mathbb{N}_0)$,

$$A\pi = \begin{bmatrix} a_{\pi(1)} \\ \vdots \\ a_{\pi(i)} \end{bmatrix}, \quad \text{za } \pi \in V_i, \quad A = \begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} \in M_{mn}(\mathbb{N}_0)$$

Pritom su $a_1, \ldots, a_m$ reci matrice A. Pomoću uvedenih oznaka i-ti redak matrice A zapisujemo kao $A(i)$, a matricu sastavljenu od prvih i redaka kao $A(1, \ldots, i)$.

Propozicija 3.8 *Neka su $A, B \in M_{mn}(\mathbb{N}_0)$. Ako je $A \leq B$, onda je $A(1, \ldots, i) \leq B(1, \ldots, i)$, za svaki $i = 1, \ldots, m$.*

Dokaz. Slijedi iz definicije uređaja među matricama 3.7. ■

Propozicija 3.9 *Kad god je za $\pi \in V_i$, $\sigma \in V_j$ definirana kompozicija $\pi \circ \sigma$, vrijedi $A(\pi \circ \sigma) = (A\pi)\sigma$.*

Dokaz. Označimo $A\pi = B = \begin{bmatrix} b_1 \\ \vdots \\ b_i \end{bmatrix} \in M_{in}(\mathbb{N}_0)$, tj. $b_k = a_{\pi(k)}$ za $k = 1, \ldots, i$. Budući da je kompozicija definirana vrijedi $i \geq j$, pa na matricu B možemo primijeniti σ:

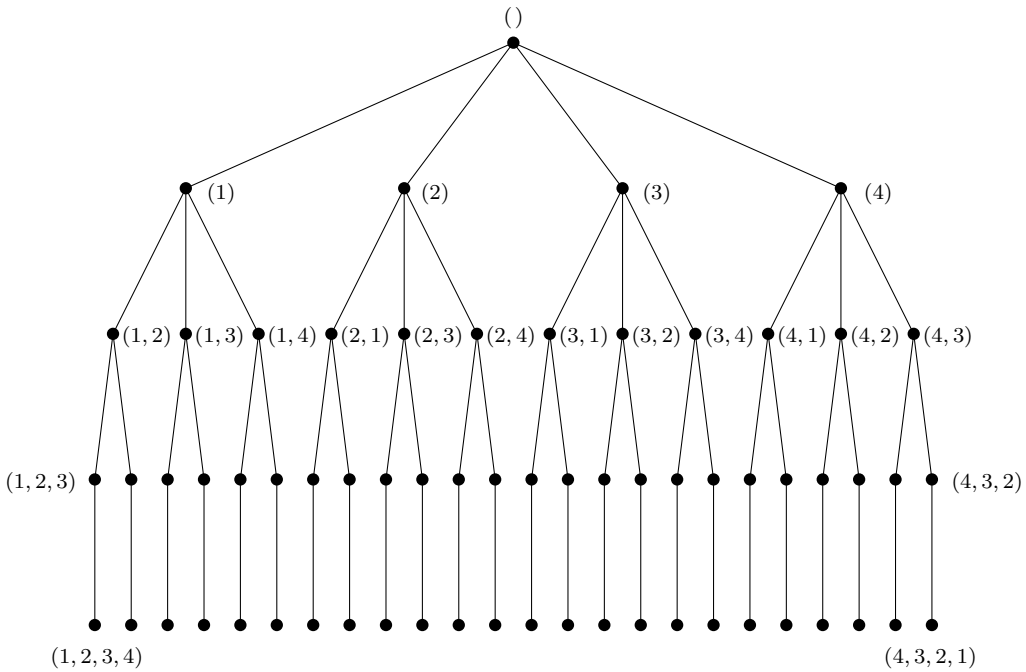
$$(A\pi)\sigma = B\sigma = \begin{bmatrix} b_{\sigma(1)} \\ \vdots \\ b_{\sigma(j)} \end{bmatrix} = \begin{bmatrix} a_{\pi(\sigma(1))} \\ \vdots \\ a_{\pi(\sigma(j))} \end{bmatrix} = A(\pi \circ \sigma)$$

■

Iz propozicije 3.9 slijedi da je $(A, \pi) \mapsto A\pi$ djelovanje grupe $V_m = S_m$ na skup $X = M_{mn}(\mathbb{N}_0)$ zdesna. Veza s djelovanjem grupe $G = S_m \times S_n$ definiranim u 3.2 je $A\pi = (\pi^{-1}, id)A$.

Skup $V = \bigcup_{i=0}^{m} V_i$ organiziramo u stablo. Na i-tom nivou stabla nalaze se elementi iz V_i. Element $() \in V_0$ je korijen stabla. Vrhovi stabla $\pi \in V_i$, $\sigma \in V_{i+1}$ spojeni su bridom ako i samo ako je π restrikcija od σ. Stablo je

zapravo Hasseov dijagram skupa V parcijalno uređenog obzirom na restrikciju. Na slici 4 vidimo prikaz stabla za $m = 4$.



Slika 4: Stablo kojeg pretražuje algoritam 3.10 za $m = 4$.

Algoritam za računanje kanonskog predstavnika matrice pretražuje dio tog stabla po širini (breadth-first search). Da bismo formulirali algoritam trebaju nam oznake za roditelja i djecu vrhova stabla.

Neka je $r : V \setminus V_0 \to V$ funkcija definirana s $r(\pi) = \pi|_{\{1,\dots,i-1\}}$, za $\pi \in V_i$. Funkcija pridružuje vrhu π njegovog roditelja u stablu. Neka je $d : \mathcal{P}(V) \to \mathcal{P}(V)$, $d(W) = r^{-1}(W)$. Funkcija d skupu $W \subseteq V$ pridružuje skup djece vrhova iz W. Nadalje, neka je $\mathbf{sort}(A)$ najveća matrica dobivena permutiranjem stupaca matrice A, tj. $\mathbf{sort}(A) = \max\{(id, \sigma)A \mid \sigma \in S_n\}$. Do nje dolazimo silaznim sortiranjem stupaca od A obzirom na leksikografski uređaj.

Algoritam 3.10 (kanonsko preslikavanje)

učitaj A;
$K_0 := \{\ ()\ \}$;
za $i = 1, \ldots, m$ **radi**
$C_i := \mathbf{sort}(A(1, \ldots, i))$;
$K_i := \emptyset$;
za sve $\pi \in d(K_{i-1})$ **radi**
ako je $\mathbf{sort}(A\pi) = C_i$ **onda** $K_i := K_i \bigcup \{\pi\}$;
ako je $\mathbf{sort}(A\pi) > C_i$ **onda**
$C_i := \mathbf{sort}(A\pi)$;
$K_i := \{\pi\}$;
ispiši C_m;

Tvrdimo da je C_m koji se ispisuje na kraju algoritma jednak kanonskom predstavniku $c(A)$. Označimo $\widetilde{C}_i = \max\{\mathbf{sort}(A\pi) \mid \pi \in V_i\}$, $\widetilde{K}_i = \left\{\pi \in V_i \mid \mathbf{sort}(A\pi) = \widetilde{C}_i\right\}$.

Lema 3.11 *Matrica $\widetilde{C}_i$ sastoji se od prvih i redaka kanonske matrice $c(A)$,*

$$\widetilde{C}_i = c(A)(1, \ldots, i).$$

Dokaz. Primijetimo najprije da je

$$\begin{aligned}\widetilde{C}_i \ &= \ \max\{\max\{(id, \sigma)A\pi \mid \sigma \in S_n\} \mid \pi \in V_i\} \ = \\ &= \ \max\{(id, \sigma)A\pi \mid \pi \in V_i,\ \sigma \in S_n\}.\end{aligned}$$

Dakle, $\widetilde{C}_i$ je najveća matrica oblika $(id, \sigma)A\pi$, za $\pi \in V_i$, $\sigma \in S_n$. Matrica $c(A)(1, \ldots, i)$ jest tog oblika: ako je $c(A) = (\pi, \sigma)A$, onda je $c(A)(1, \ldots, i) = (id, \sigma)A\ \pi^{-1} \circ (1, \ldots, i)$, a $\pi^{-1} \circ (1, \ldots, i) \in V_i$. Slijedi $\widetilde{C}_i \geq c(A)(1, \ldots, i)$.

Da bi dokazali obratnu nejednakost neka je $\pi \in \widetilde{K}_i$, tj. $\widetilde{C}_i = \mathbf{sort}(A\pi)$. Postoje $\sigma \in S_n$ i $\rho \in S_m$ takvi da je $\mathbf{sort}(A\pi) = (id, \sigma)A\pi$ i $\pi = \rho|_{\{1,\ldots,i\}}$. Znamo da je $c(A) \geq (\rho^{-1}, \sigma)A$, iz čega zbog propozicije 3.8 slijedi

$$c(A)(1, \ldots, i) \geq (\rho^{-1}, \sigma)A(1, \ldots, i) = (id, \sigma)A\ \rho \circ (1, \ldots, i) = (id, \sigma)A\pi = \widetilde{C}_i$$

Dakle, $\widetilde{C}_i = c(A)(1, \ldots, i)$.

■

Lema 3.12 *Ako je* $\pi \in \widetilde{K}_i$*, onda je* $r(\pi) \in \widetilde{K}_{i-1}$*.*

Dokaz. Označimo $\rho = r(\pi) = \pi \circ (1, \ldots, i-1)$. Vrijedi:

$$\mathbf{sort}(A\rho) = \mathbf{sort}(A\ \pi\circ(1,\ldots,i-1)) = \mathbf{sort}(A\pi)(1,\ldots,i-1) = \widetilde{C}_i(1,\ldots,i-1)$$

$$= \ (c(A)(1,\ldots,i))(1,\ldots,i-1) \ = \ c(A)(1,\ldots,i-1) \ = \ \widetilde{C}_{i-1}$$

Dakle, $\rho \in \widetilde{K}_{i-1}$.

■

Lema 3.13 *Nakon izvođenja algoritma 3.10 vrijedi* $C_i = \widetilde{C}_i$ *i* $K_i = \widetilde{K}_i$*, za svaki* $i = 1, \ldots, m$*.*

Dokaz. Indukcijom po i. Za $i = 1$ algoritam prelazi po svim $\pi \in d(\,(\,)\,) = V_1$ i pamti najveću matricu oblika $\mathbf{sort}(A\pi)$. Zato je $C_1 = \widetilde{C}_1$ i $K_1 = \widetilde{K}_1$.

Pretpostavimo da tvrdnja vrijedi za $i-1$, tj. $C_{i-1} = \widetilde{C}_{i-1}$ i $K_{i-1} = \widetilde{K}_{i-1}$. Algoritam u i-tom koraku pamti najveću od matrica $\mathbf{sort}(A\pi)$ za $\pi \in d(K_{i-1}) = d(\widetilde{K}_{i-1})$. Za preostale $\pi \in V_i$ matrice $\mathbf{sort}(A\pi)$ su prema lemi 3.12 manje od $\widetilde{C}_i$. Vidimo da se u C_i sprema najveća matrica oblika $\mathbf{sort}(A\pi)$, pa je $C_i = \widetilde{C}_i$ i $K_i = \widetilde{K}_i$.

■

Teorem 3.14 *Matrica* C_m *koju ispisuje algoritam 3.10 jednaka je kanonskom predstavniku matrice* A*.*

Dokaz. $C_m = (\text{lema } 3.13) = \widetilde{C}_m = (\text{lema } 3.11) = c(A)(1,\ldots,m) = c(A)$.

■

Algoritam 3.10 realiziran je u programu `canonmat`, pisanom u programskom jeziku C. Osim za računanje kanonskog predstavnika možemo ga upotrijebiti za određivanje pune grupe automorfizama matrice.

Propozicija 3.15 *Neka su stupci matrice* A *međusobno različiti. Tada je skup* $K_m = \{\pi \in S_m \mid \mathbf{sort}(A\pi) = c(A)\}$ *definiran algoritmom 3.10 u bijektivnom odnosu s punom grupom automorfizama* $\mathrm{Aut}(A)$*.*

Dokaz. Za matricu A postoji jedinstveni $\sigma \in S_n$ takav da je $\mathbf{sort}(A) = (id, \sigma)A$. Ista tvrdnja vrijedi za matrice $A\pi$, $\pi \in S_m$, jer su i njihovi stupci međusobno različiti. Definiramo bijekciju između K_m i skupa $K = \{(\pi, \sigma) \in S_m \times S_n \mid (\pi, \sigma)A = c(A)\}$. Elementu $\pi \in K_m$ pridružujemo par (π^{-1}, σ), gdje je $\sigma \in S_n$ jedinstvena permutacija za koju je $\mathbf{sort}(A\pi) = (id, \sigma)A\pi$. Skup K je lijeva klasa pune grupe automorfizama $\mathrm{Aut}(A)$ (vrijedi

$K = (\pi_0, \sigma_0)\,\mathrm{Aut}(A)$, za bilo koji $(\pi_0, \sigma_0) \in K$). Vidimo da je K_m bijektivan s lijevom klasom K, koja je bijektivna s $\mathrm{Aut}(A)$. ■

Glavni nedostatak algoritma 3.10 je što stablo pretražuje po širini. Zato je potrebno pamtiti skupove $K_1, \ldots, K_m$, koji za pravilne matrice (kao što su incidencijske matrice dizajna) vrlo brzo postaju preveliki za memoriju računala. Postoje algoritmi koji stablo pretražuju po dubini (depth-first search, backtracking), na primjer [12] i [13]. Na taj način ne moraju se pamtiti veliki skupovi vrhova. Osim toga automorfizmi se pronalaze u ranijoj fazi potrage, pa ih se može upotrijebiti za smanjivanje dijela stabla kojeg treba pretražiti. Takvi algoritmi pamte skup generatora pune grupe automorfizama, a ne sve njezine elemente.

Jedan od najbržih programa tog tipa je `nauty` B.D.McKay-a [14]. Program računa kanonskog predstavnika i punu grupu automorfizama obojanog grafa (primjer 3.3). Možemo ga primijeniti na incidencijske strukture (primjer 3.1) i matrice (primjer 3.2) tako da im pridružimo grafove koji imaju izomorfne pune grupe automorfizama.

Incidencijskoj strukturi $S = (\mathcal{P}, \mathcal{L}, I)$ pridružujemo bipartitni graf $\mathcal{G}(S)$ sa skupom vrhova $V = \mathcal{P} \dot{\cup} \mathcal{L}$ (disjunktna unija). Točke su obojane bojom 1, a pravci bojom 2. Bridovi su $\{\{P, \ell\} \mid P \in \mathcal{P},\ \ell \in \mathcal{L},\ PI\ell\}$. Pokazuje se da je $\mathrm{Aut}(S) \cong \mathrm{Aut}(\mathcal{G}(S))$. Slično postupamo za matrice.

Međutim, u sklopu algoritma za klasifikaciju kojeg opisujemo u idućoj točki ipak ćemo koristiti algoritam 3.10. Treba nam kanonsko preslikavanje s nekim dodatnim svojstvima, koje za `nauty` ne možemo provjeriti. Za naše potrebe program `canonmat` je dovoljno brz.

Na kraju ovog odjeljka opisujemo jednu primjenu za koju možemo upotrijebiti bilo koje kanonsko preslikavanje, dakle i `nauty`. Radi se o problemu "filtriranja". Neka je $S \subseteq X$ skup objekata. Treba naći skup predstavnika za S, tj. $P \subseteq S$ sa svojstvima:

(1) Svaki objekt iz S izomorfan je nekom iz P.

(2) Objekti iz P međusobno su neizomorfni.

Problem se, na primjer javlja kod konstrukcije dizajna pomoću grupa automorfizama, kojom se bavimo u petom poglavlju. Dobivaju se skupovi dizajna među kojima može biti izomorfnih. Treba odrediti koliko ih ima do na izomorfizam i naći po jednog predstavnika iz svake klase.

Algoritam 3.16 (filter)

Na ulazu se nalaze objekti iz S. Objekti iz P ispisuju se na izlaz.

$T := \emptyset$;
sve dok ⟨ima objekata na ulazu⟩ **radi**
  učitaj A;
  $C := c(A)$;
  ako $C \notin T$ **onda**
    ispiši A;
    $T := T \cup \{C\}$;

Prethodni algoritam realiziran je u programu `incfilter`. Program "filtrira" skupove 0-1 matrica. Za kanonsko preslikavanje koristi `nauty`. Skup T implementiran je kao stablo, da bi se upit $C \notin T$ izvodio što brže.

3.2 Algoritam za klasifikaciju

Kao i dosad, X označava skup objekata na kojem djeluje grupa G. Pod *klasifikacijom* podrazumijevamo određivanje broja staza pri tom djelovanju i pronalaženje po jednog predstavnika iz svake staze.

Naivan pristup problemu klasifikacije bio bi generiranje pomoću računala svih objekata iz X i njihovo filtriranje algoritmom 3.16. To nije provedivo jer u praksi skup X ima previše elemenata. Na primjer, neka je X skup svih Steinerovih 2-dizajna $S(3, 13)$ na kojem djeluje grupa $G = S_{13} \times S_{26}$. Do na izomorfizam postoje dva takva dizajna, $S3.1$ i $S3.2$. Korištenjem propozicije 1.18 možemo izračunati ukupan broj objekata u X:

$$|X| = \frac{|G|}{|\operatorname{Aut}(S3.1)|} + \frac{|G|}{|\operatorname{Aut}(S3.2)|} = 13!\,26!\left(\frac{1}{39} + \frac{1}{6}\right) \approx 4.8 \cdot 10^{35}$$

Pomoću implementacije algoritma 3.16 na današnjim brzim računalima možemo obraditi na milijune objekata, ali filtriranje ovako velikog skupa ne dolazi u obzir. Glavni cilj algoritma za klasifikaciju upravo je smanjiti broj objekata na koje primjenjujemo kanonsko preslikavanje. Za to nam treba više strukture na skupu X nego dosad.

Neka je zadana funkcija $ord : X \to \mathbb{N}$. Kažemo da je objekt A *reda* $ord(A)$. Skup svih objekata reda l označavamo $X^{(l)} = \{\, A \in X \mid ord(A) = l \,\}$.

Algoritmom klasificiramo objekte reda m tako da prvo klasificiramo objekte manjeg reda $l = 1, 2, 3, \ldots$

Neka na svakom nepraznom $X^{(l)}$ djeluje grupa $G^{(l)}$. Direktni produkt $G = G^{(1)} \times G^{(2)} \times \ldots$ na prirodan način djeluje na X, $(g_1, g_2, \ldots)A = g_{ord(A)}A$ za $A \in X$ i $(g_1, g_2, \ldots) \in G$. U ovoj situaciji prirodno je definirati punu grupu automorfizama objekta $A \in X^{(l)}$ kao njegov $G^{(l)}$-stabilizator, jer grupa $G^{(1)} \times \ldots \times G^{(l-1)} \times G^{(l+1)} \times \ldots$ stabilizira sve objekte reda l.

Neka je $c : X \to X$ kanonsko preslikavanje. Budući da izomorfni objekti imaju isti red, c čuva red objekata. Skup svih kanonskih objekata reda l označavamo $C^{(l)} = \left\{ A \in X^{(l)} \mid c(A) = A \right\}$. Algoritmom konstruiramo $C^{(m)}$, skup predstavnika za $X^{(m)}$.

Najvažnija dodatna struktura na skupu X je veza između objekata različitog reda. Formalno, zahtjevamo postojanje funkcije $p : X \setminus X^{(1)} \to X$ sa svojstvima:

(1) $p(X^{(l+1)}) \subseteq X^{(l)}$, za svaki l (p smanjuje red objekata za jedan)

(2) $p(C^{(l+1)}) \subseteq C^{(l)}$, za svaki l (p čuva kanonske objekte)

Primjer 3.17 Klasificiramo Steinerove 2-dizajne s parametrima v, b, r, k. *Parcijalna incidencijska matrica* je svaka matrica $A = [a_{ij}] \in M_{lb}(\{0, 1\})$ $(1 \leq l \leq v)$ koja zadovoljava:

(1) $A \cdot A^\tau = (r - 1)I_l + J_l$

(2) $\displaystyle\sum_{i=1}^{l} a_{ij} \leq k, \quad \text{za } j = 1, \ldots, b$

Neka je $X^{(l)}$ skup svih parcijalnih incidencijskih $l \times b$ matrica. Ako je $l = v$ svojstva (1) i (2) povlače jednakost u (2), pa prema 1.9 skup $X^{(v)}$ sadrži incidencijske matrice $S(k, v)$ dizajna.

Neka je $X = X^{(1)} \cup \cdots \cup X^{(v)}$ i $ord(A) =$ broj redaka matrice A. Na $X^{(l)}$ djeluje grupa $G^{(l)} = S_l \times S_b$ kao u primjeru 3.2. Za kanonsko preslikavanje uzmimo funkciju $c(A) = \max\{gA \mid g \in G\}$, pri čemu je G direktni produkt $G^{(1)} \times \cdots \times G^{(b)}$. Računamo ga pomoću algoritma 3.10, odnosno programa `canonmat`. Funkcija p neka je brisanje zadnjeg retka matrice,

$$p\left(\begin{bmatrix} a_1 \\ \vdots \\ a_l \end{bmatrix}\right) = \begin{bmatrix} a_1 \\ \vdots \\ a_{l-1} \end{bmatrix}$$

Očito p smanjuje red (tj. broj redaka) matrice za jedan, a zbog sljedeće propozicije kanonske matrice preslikava u kanonske.

Propozicija 3.18 *Neka je* $A \in M_{mn}(\mathbb{N}_0)$ *kanonska matrica obzirom na funkciju* c *iz propozicije 3.6, tj.* $c(A) = A$. *Tada su i matrice* $A(1, \ldots, i)$, $i = 1, \ldots, m$ *kanonske, tj.* $c(A(1, \ldots, i)) = A(1, \ldots, i)$.

Dokaz. $A(1, \ldots, i) = c(A)(1, \ldots, i) =$ (lema 3.11) $=$

$$= \max\{(id, \sigma)A\pi \mid \pi \in V_i,\ \sigma \in S_n\} \geq \max\{(id, \sigma)A\pi \mid \pi \in S_i,\ \sigma \in S_n\} =$$

$$= \max\{(\pi^{-1}, \sigma)A(1, \ldots, i) \mid \pi \in S_i,\ \sigma \in S_n\} = c(A(1, \ldots, i))$$

Očito vrijedi i drugi smjer nejednakosti, pa je $c(A(1, \ldots, i)) = A(1, \ldots, i)$. ■

Algoritam 3.19

$R_1 := C^{(1)}$;
za $l := 2, \ldots, m$ **radi**
⌈ $R_l := \emptyset$;
| **za sve** $A \in p^{-1}(R_{l-1})$ **radi**
⌊ [**ako je** $c(A) = A$ **onda** $R_l := R_l \cup \{A\}$;
ispiši R_m;

Propozicija 3.20 *Nakon izvođenja algoritma 3.19 vrijedi* $R_l = C^{(l)}$, *za* $l = 1, \ldots, m$.

Dokaz. Indukcijom po l. Za $l = 1$ tvrdnja vrijedi zbog inicijalizacije na početku algoritma. Pretpostavimo da je $R_{l-1} = C^{(l-1)}$. Nakon izvođenja l-tog koraka petlje očito je $R_l = p^{-1}(R_{l-1}) \cap C^{(l)} = p^{-1}(C^{(l-1)}) \cap C^{(l)}$. Zbog svojstva (2) funkcije p vrijedi $p^{-1}(C^{(l-1)}) \supseteq C^{(l)}$, pa je presjek jednak $C^{(l)}$. Dakle, $R_l = C^{(l)}$. ■

Algoritam realiziramo tako da se skupovi $R_1, \ldots, R_m$ pamte na vanjskoj memoriji računala (disku). Treba nam program za računanje praslike $p^{-1}(R_{l-1})$. U slučaju klasifikacije Steinerovih 2-dizajna proširujemo parcijalne incidencijske $(l-1) \times b$ matrice jednim retkom, do parcijalnih incidencijskih $l \times b$ matrica. Problem rješava program `p-1`, za proizvoljne parametre $S(k, v)$. Treba nam još program koji iz niza objekata izbacuje one koji nisu kanonski. Za matrice nad $\mathbb{N}_0$ koristimo program `canonfilter`, napisan na osnovu algoritma 3.10. Prilikom klasifikacije $S(k, v)$ dizajna primjenjujemo ga na parcijalne incidencijske matrice.

Primjer 3.21 Klasificiramo Steinerove 2-dizajne $S(3,13)$ algoritmom 3.19. Krećemo od jedinstvene parcijalne incidencijske 1×26 matrice u kanonskom obliku:

```
11111100000000000000000000
```

Programom `p-1` proširujemo je do parcijalnih incidencijskih 2×26 matrica i pomoću `canonfilter`-a izbacujemo nekanonske. Tako dobivamo skup $R_2 = C^{(2)}$, a analogno konstruiramo skupove $R_3, \ldots, R_{13}$. Točan redoslijed pozivanja programa vidljiv je iz shell-skripte `klas1`. Rezultati su sabrani u tablici 5. Skup R_{13} sadrži dvije incidencijske matrice, koje pripadaju dizajnima $S3.1$ i $S3.2$. Zaključujemo da do na izomorfizam postoje točno dva $S(3,13)$ dizajna.

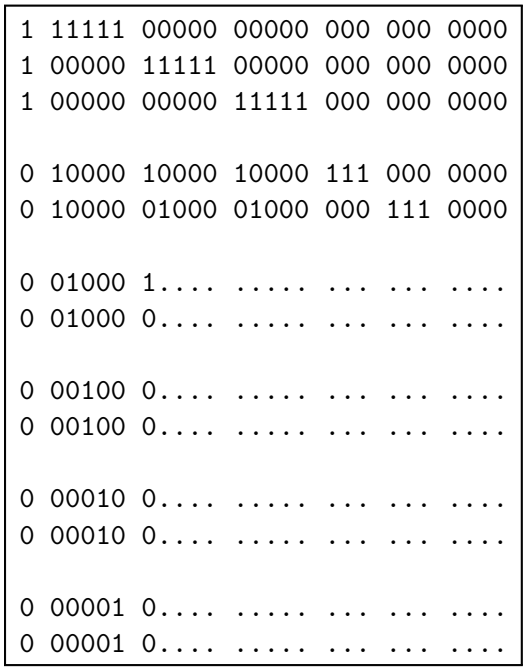
l	$\lvert R_l\rvert = \lvert C^{(l)}\rvert$	$\lvert p^{-1}(R_l)\rvert$
1	1	93024
2	1	37128
3	2	29520
4	2	11214
5	3	6254
6	6	4611
7	12	2869
8	14	1135
9	33	723
10	44	276
11	23	38
12	5	5
13	**2**	—

Tablica 5: Klasifikacija $S(3,13)$ pomoću algoritma 3.19.

U primjeru vidimo glavni nedostatak algoritma 3.19. Skup R_1 proširivali smo do ukupno 93024 parcijalnih incidencijskih 2×26 matrica i zatim izbacivali nekanonske, a sasvim je jasno da je među njima samo jedna kanonska:

```
11111100000000000000000000
10000011111000000000000000
```

Štoviše, kanonske incidencijske matrice $S(3,13)$ dizajna očito su oblika prikazanog na slici 5. Matrice koje nisu tog oblika ne treba ni razmatrati.



Slika 5: Oblik kanonskih incidencijskih matrica za $S(3, 13)$.

Općenito, neka je $Y^{(m)}$ skup objekata reda m koji sadrži sve kanonske objekte ($C^{(m)} \subseteq Y^{(m)} \subseteq X^{(m)}$). Definiramo $Y^{(l)} = p(Y^{(l+1)})$ za $l = m - 1, m-2, \ldots, 1$, $Y = \bigcup_{l=1}^{m} Y^{(l)}$ i $q = p|_{Y \setminus Y^{(1)}} : Y \setminus Y^{(1)} \to Y$. Pretpostavimo da je za neki l_0 skup $Y^{(l_0)}$ poznat.

Algoritam 3.22

$P_{l_0} := Y^{(l_0)}$;
za $l := l_0 + 1, \ldots, m$ **radi**
$\lceil$ $P_l := \emptyset$;
za sve $A \in q^{-1}(P_{l-1})$ **radi**
$\lceil$ **ako je** $c(A) = A$ **onda** $P_l := P_l \cup \{A\}$;
ispiši P_m;

Propozicija 3.23 *Nakon izvođenja algoritma 3.22 vrijedi* $P_m = C^{(m)}$.

Dokaz. Označimo $Z^{(m)} = C^{(m)}$ i neka je $Z^{(l)} = p(Z^{(l+1)})$, za $l = m - 1$, $m - 2, \ldots, 1$. Silaznom indukcijom lako se pokazuje da za svaki l vrijedi

$C^{(l)} \supseteq Z^{(l)}$ i $Y^{(l)} \supseteq Z^{(l)}$. Dokazujemo uzlaznom indukcijom da ista tvrdnja vrijedi za skupove definirane algoritmom, $P_l \supseteq Z^{(l)}$ za $l = l_0, \ldots, m$.

Zbog inicijalizacije na početku algoritma je $P_{l_0} = Y^{(l_0)}$, pa tvrdnja vrijedi za $l = l_0$. Pretpostavimo $P_{l-1} \supseteq Z^{(l-1)}$. Iz toga slijedi $p^{-1}(P_{l-1}) \supseteq p^{-1}(Z^{(l-1)}) \supseteq Z^{(l)}$. Algoritam definira skup P_l kao presjek

$$P_l = q^{-1}(P_{l-1}) \cap C^{(l)} = p^{-1}(P_{l-1}) \cap Y^{(l)} \cap C^{(l)}$$

Sva tri skupa u presjeku su nadskupovi od $Z^{(l)}$, pa je i P_l nadskup od $Z^{(l)}$. Posebno, za $l = m$ slijedi

$$C^{(m)} \supseteq q^{-1}(P_{m-1}) \cap C^{(m)} = P_m \supseteq Z^{(m)} = C^{(m)}$$

Dakle, $P_m = C^{(m)}$.

■

Primjer 3.24 Klasificiramo Steinerove 2-dizajne $S(3, 13)$ algoritmom 3.22. Neka je $Y^{(m)}$ skup incidencijskih matrica za $S(3, 13)$ koje su oblika kao na slici 5. Među njima su sve kanonske incidencijske matrice. Skup $Y^{(l)}$ sadrži parcijalne incidencijske matrice dobivene odbacivanjem $v - l$ redaka matrica iz $Y^{(m)}$. One su oblika kao prvih l redaka sa slike 5. Klasifikaciju započinjemo od jednočlanog skupa $Y^{(5)}$, koji sadrži matricu:

```
1111110000000000000000000
1000001111100000000000000
1000000000011111000000000
0100001000010000111000000
0100000100001000000111000
```

Kod provedbe algoritma 3.22 jedina razlika u odnosu na algoritam 3.19 je što treba računati praslike $q^{-1}(P_{l-1})$ umjesto $p^{-1}(R_{l-1})$. Konkretno, to znači da $(l-1) \times b$ matrice proširujemo samo do $l \times b$ matrica iz skupa $Y^{(l)}$, tj. do parcijalnih incidencijskih matrica oblika kao prvih l redaka sa slike 5. Koristimo program `q-1` umjesto programa `p-1`. Točan redoslijed u kojem pozivamo programe vidljiv je iz shell-skripte `klas2`, a rezultati su sabrani u tablici 6.

Osnovni zahtjev koji postavljamo na algoritam za klasifikaciju je što manji broj objekata na koje primjenjujemo kanonsko preslikavanje. Vidimo da po tom kriteriju možemo spretnim odabirom skupa $Y^{(m)}$ postići znatno poboljšanje algoritma 3.22 u odnosu na algoritam 3.19. U primjeru 3.21 "filtrirali" smo ukupno $\sum_{l=1}^{12} |p^{-1}(R_l)| = 186797$ matrica, a u primjeru 3.24 samo $\sum_{l=5}^{12} |q^{-1}(P_l)| = 859$.

l	$\lvert P_l\rvert$	$\lvert q^{-1}(P_l)\rvert$
5	1	58
6	2	174
7	3	306
8	6	100
9	10	139
10	31	65
11	9	12
12	5	5
13	**2**	—

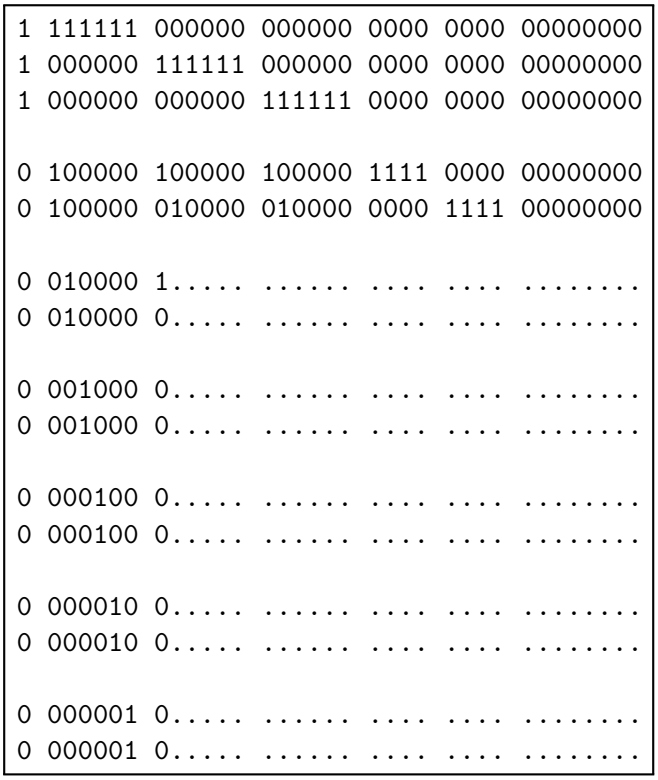
Tablica 6: Klasifikacija $S(3,13)$ pomoću algoritma 3.22.

Drugi problem koji se javlja prilikom klasifikacije je pohranjivanje međurezultata. U tipičnoj situaciji parcijalnih objekata ima znatno više nego potpunih, što je vidljivo i iz tablice 5. Kod klasifikacije $S(3,13)$ dizajna skupovi R_l i P_l su zanemarivo mali i pohranjivanje ne predstavlja problem. Za veće dizajne skupovi mogu doseći kapacitet današnjih diskova čak i kad potpunih objekata nema puno. Vidimo da je i u tom pogledu algoritam 3.22 bolji od algoritma 3.19, jer ne pohranjuje sve parcijalne objekte. Na primjer, skup P_9 sadrži samo 10 od ukupno 33 parcijalnih incidencijskih 9×26 matrica.

Spomenimo da je B.D.McKay [15] razvio algoritam za klasifikaciju kod kojeg se ne pojavljuje taj problem. Ideja je klase ekvivalencije objekata organizirati u stablo, s potpunim objektima na posljednjem nivou. Stablo se pretražuje po dubini, za što je potrebno pamtiti samo po jedan objekt sa svakog nivoa. McKayev algoritam zahtjeva više strukture na skupu objekata X.

Primjer 3.25 Steinerove 2-dizajne $S(3,15)$ klasificirali su 1983. godine R.Mathon, K.T.Phelps i A.Rosa (prema [4]). Dobili su ukupno 80 neizomorfnih dizajna. Ponavljamo klasifikaciju korištenjem algoritma 3.22 primjenjenog na incidencijske matrice oblika sa slike 6. Klasifikaciju započinjemo od skupa P_5 i programima `q-1` i `canonfilter` konstruiramo skupove $P_6,\ldots,P_{15}$. Kao što je vidljivo iz tablice 7, također dobivamo 80 dizajna $S(3,15)$.

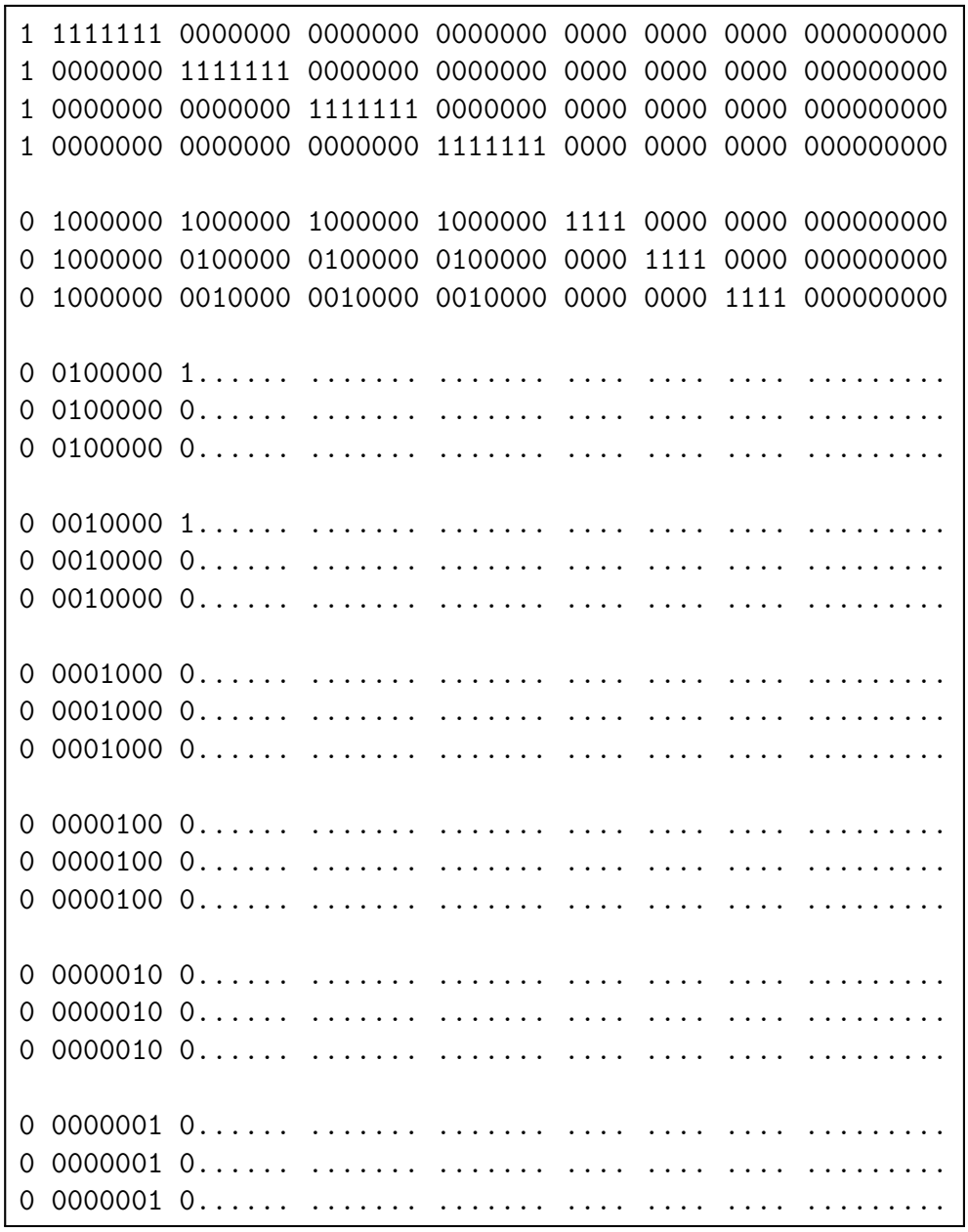
Primjer 3.26 Steinerove 2-dizajne $S(4,25)$ klasificirao je E.Spence [18] 1996. godine. Spence je algoritmom 3.22 konstruirao parcijalne incidencijske 13×50 matrice oblika sa slike 7. Dobio je 120014 kanonskih matrica. U nastavku klasifikacije više se ne isplati izbacivati nekanonske matrice nakon



Slika 6: Oblik kanonskih incidencijskih matrica za $S(3, 15)$.

l	$\lvert P_l \rvert$	$\lvert q^{-1}(P_l) \rvert$
5	1	966
6	2	3510
7	5	11714
8	14	4851
9	25	5934
10	326	10317
11	704	16310
12	4495	12366
13	1717	3170
14	626	626
15	**80**	—

Tablica 7: Klasifikacija $S(3, 15)$ pomoću algoritma 3.22.



Slika 7: Oblik kanonskih incidencijskih matrica za $S(4, 25)$.

proširivanja jednim retkom, nego tek kad ih proširimo do potpunih incidencijskih matrica. Za konstrukciju skupa P_{14} trebalo bi filtrirati znatno više matrica nego što ih dobivamo proširivanjem matrica iz P_{13} do kraja. Spence je na taj način dobio 18 neizomorfnih $S(4, 25)$ dizajna.

Ovdje klasifikaciju ponavljamo samo djelomično. Pomoću programa `q-1` i `canonfilter` konstruiramo skupove $P_7, \ldots, P_{11}$ (tablica 8). Spence je za računanje kanonskih predstavnika koristio program F.Bussemakera, koji je osjetno brži od programa `canonmat`. Postupak proširivanja matrica iz P_{13} do potpunih incidencijskih matrica također je vrlo dugotrajan. Spenceovi programi trebali su više mjeseci procesorskog vremena.

l	$\lvert P_l\rvert$	$\lvert q^{-1}(P_l)\rvert$
7	1	14844
8	3	110019
9	16	92472
10	32	14717
11	126	311603
12		
13	120014	
25	**18**	—

Tablica 8: Klasifikacija $S(4, 25)$.

Vidimo da su algoritmom 3.22 klasificirani dizajni $S(3, 13)$, $S(3, 15)$ i $S(4, 25)$. Izuzevši projektivne i afine ravnine, to su jedini parametri za koje je poznat točan broj Steinerovih 2-dizajna. Projektivne i afine ravnine, $S(n + 1, n^2 + n + 1)$ i $S(n, n^2)$ klasificirane su pomoću računala sve do $n = 10$. Korišene su veze s latinskim kvadratima (za $n \leq 9$) i binarnim kodovima (za $n = 10$). Više o tome može se pročitati u diplomskom radu [10].

Primjer 3.27 Na kraju objašnjavamo primjenu algoritma za klasifikaciju na orbitne strukture. Neka su zadani vektori $\nu = (\nu_1, \ldots, \nu_m) \in \mathbb{N}^m$ i $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ (zovemo ih *marginalni vektori*). Označimo $v = \sum_{i=1}^{m} \nu_i$, $b = \sum_{j=1}^{n} \beta_j$ i neka su $r, k, \lambda \in \mathbb{N}$. *Orbitna struktura* je svaka matrica $A = [a_{ij}] \in M_{mn}(\mathbb{N}_0)$ koja zadovoljava:

(1) $0 \leq a_{ij} \leq \beta_j$, za $1 \leq i \leq m$, $1 \leq j \leq n$

$$(2)\quad \sum_{j=1}^{n} a_{ij} = r, \quad \text{za } 1 \le i \le m$$

$$(3)\quad \sum_{i=1}^{m} \frac{\nu_i}{\beta_j}\, a_{ij} = k, \quad \text{za } 1 \le j \le n$$

$$(4)\quad \sum_{j=1}^{n} \frac{\nu_i}{\beta_j}\, a_{ij}a_{i'j} = \begin{cases} \lambda\nu_i, & \text{ako je } i \ne i' \\ \lambda(\nu_i - 1) + r, & \text{ako je } i = i' \end{cases}, \quad \text{za } 1 \le i, i' \le m$$

Takve matrice javljaju se prilikom konstrukcije (v, k, λ) blok dizajna sa zadanom grupom automorfizama (vidi poglavlje 5.1). Pretpostavljamo da su parametri v, b, r, k, λ dopustivi.

Parcijalna orbitna struktura je matrica $A = [a_{ij}] \in M_{ln}(\mathbb{N}_0)$, $1 \le l \le m$, koja ima svojstva (1), (2), (4) i

$$(3')\quad \sum_{i=1}^{l} \frac{\nu_i}{\beta_j}\, a_{ij} \le k, \quad \text{za } 1 \le j \le n$$

Neka je X skup svih parcijalnih orbitnih struktura. Red $ord(A)$ je broj redaka matrice A, pa je $X^{(l)}$ skup parcijalnih $l \times n$ orbitnih struktura. Matrice u $X^{(m)}$ su orbitne strukture, jer uvjeti (2) i (3′) zajedno s $l = m$ impliciraju uvjet (3). Računamo:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \nu_i a_{ij} \;=\; \sum_{i=1}^{m} \nu_i \sum_{j=1}^{n} a_{ij} \;=\; \sum_{i=1}^{m} \nu_i r \;=\; vr$$

S druge strane, ako je u (3′) nejednakost stroga bar za jedan j, slijedi

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \nu_i a_{ij} \;=\; \sum_{j=1}^{n}\sum_{i=1}^{m} \nu_i a_{ij} \;<\; \sum_{j=1}^{n} \beta_j k \;=\; bk$$

Dobili smo $vr < bk$, a za dopustive parametre mora vrijediti jednakost. Dakle, $X^{(m)}$ je skup potpunih orbitnih struktura, koje želimo klasificirati.

Pri definiciji izomorfizma (parcijalnih) orbitnih stuktura treba paziti da svojstva (1) - (4) ostanu sačuvana. Dopuštamo samo permutacije redaka i stupaca koje ostavljaju marginalne vektore invarijantnim:

$$H^{(l)} = \left\{ \pi \in S_l \mid \nu_{\pi(i)} = \nu_i,\ i = 1, \ldots, l \right\}$$

$$K = \left\{ \sigma \in S_n \mid \beta_{\sigma(j)} = \beta_j,\ j = 1, \ldots, n \right\}$$

Grupa $G^{(l)} = H^{(l)} \times K$ djeluje na skup $X^{(l)}$ parcijalnih $l \times n$ orbitnih struktura kao u primjeru 3.2. Za $A \in X^{(l)}$ i $(\pi, \sigma) \in G^{(l)}$ vrijedi $(\pi, \sigma)A \in X^{(l)}$, pa je djelovanje dobro definirano (čuvaju se svojstva (1) - (4)).

Kao i prije, definiramo $G = G^{(1)} \times \cdots \times G^{(m)}$. Za kanonsko preslikavanje uzimamo funkciju $c(A) = \max\{(\pi, \sigma)A \mid (\pi, \sigma) \in G\}$, obzirom na uređaj među matricama definiran u 3.7. Uz male modifikacije funkciju c možemo računati algoritmom 3.10, odnosno programom `canonmat`.

Veza među matricama različitog reda neka je brisanje zadnjeg retka:

$$p : X \setminus X^{(1)} \to X, \qquad p(\begin{bmatrix} a_1 \\ \vdots \\ a_l \end{bmatrix}) = \begin{bmatrix} a_1 \\ \vdots \\ a_{l-1} \end{bmatrix}$$

Očito p smanjuje red objekata za jedan. Slično kao u propoziciji 3.18 pokazuje se da p preslikava kanonske matrice u kanonske. Time smo došli u situaciju u kojoj možemo primijeniti algoritam 3.19.

Ako imamo informaciju o obliku kanonskih orbitnih struktura možemo dodatno ubrzati klasifikaciju korištenjem algoritma 3.22. Računanje praslike $q^{-1}(P_{l-1})$ je proširivanje parcijalnih orbitnih struktura jednim retkom, na sve dozvoljene načine. Treba poštivati zadani oblik, a proširene matrice također trebaju biti parcijalne orbitne strukture. Zadatak rješava program `t-1`.

Proširene matrice nisu sve u kanonskom obliku, pa ih treba "filtrirati". To radimo programom `canonfilter` s opcijom `-t`. Navođenjem opcije razmatraju se samo permutacije redaka i stupaca koje ostavljaju marginalne vektore invarijantnim. Klasifikacija orbitnih struktura bit će ilustrirana nizom konkretnih primjera u petom poglavlju.

4 Konstrukcija pomoću diferencijskih familija

4.1 Diferencijske familije

U ovom poglavlju G označava konačnu grupu reda v. Binarnu operaciju zapisujemo aditivno, iako G ne mora biti Abelova.

Definicija 4.1 *Neka grupa $(G,+)$ djeluje na skup X. Kažemo da je djelovanje* **regularno** *ako za bilo koje $x,y \in X$ postoji jedinstveni $g \in G$ takav da je $g+x=y$.*

Regularno djelovanje omogućuje identifikaciju elemenata skupa X s elementima grupe G. Odaberemo čvrsti $x_0 \in X$ i definiramo funkciju $\varphi : X \to G$, $\varphi(x) =$ jedinstveni $g \in G$ sa svojstvom $g + x_0 = x$. Zbog regularnosti φ je dobro definirana bijekcija. Uz identifikaciju $x \equiv \varphi(x)$ djelovanje se podudara s lijevim translacijama u grupi G. Obrnuto, djelovanje bilo koje grupe na samu sebe lijevim translacijama je regularno.

Definicija 4.2 *Neka je $\mathcal{F} = \{D_1, \ldots, D_n\}$ familija k-članih podskupova od G.* **Razvoj** *familije $\mathcal{F}$ je incidencijska struktura* $\operatorname{dev}\mathcal{F} = (G, G+\mathcal{F}, \in)$*, pri čemu je $G+\mathcal{F} = \{g + D_i \mid g \in G,\ i = 1, \ldots, n\}$, $g + D_i = \{g+x \mid x \in D_i\}$. Elemente iz $\mathcal{F}$ zovemo* **temeljni blokovi** *razvoja* $\operatorname{dev}\mathcal{F}$*.*

Razvoj familije $\mathcal{F}$ je uniformna incidencijska struktura, tj. svaki blok sadrži točno k točaka. Ukoliko $\mathcal{F}$ sadrži dva bloka koji pripadaju istoj G-orbiti, recimo $D_1 = g + D_2$ za neki $g \in G$, tada je $\operatorname{dev}\{D_1, D_2, \ldots, D_n\} = \operatorname{dev}\{D_2, \ldots, D_n\}$. Stoga možemo pretpostaviti da temeljni blokovi pripadaju različitim stazama pri djelovanju G na $\mathcal{P}_k(G)$.

Propozicija 4.3 *G je grupa automorfizama incidencijske strukture* $\operatorname{dev}\mathcal{F}$*, koja djeluje regularno na točke.*

Dokaz. G djeluje na točke i pravce od $\operatorname{dev}\mathcal{F}$ lijevim translacijama. Očito vrijedi $x \in y + D_i \iff g + x \in g + y + D_i$, pa je G grupa automorfizama. Djelovanje na točke je regularno jer se radi o lijevim translacijama u G. ■

Definicija 4.4 **Multiskup** *m na G je funkcija $m : G \to \mathbb{N}_0$. Kažemo da je element $g \in G$ sadržan $m(g)$ puta u m.* **Lista** *u G je funkcija $\ell : S \to G$, pri čemu je S konačan skup.*

Poseban slučaj liste je uređena n-torka (konačan niz) s elementima iz G. $(g_1, \ldots, g_n)$ je funkcija $g : \{1, \ldots, n\} \to G$, $g(i) = g_i$. Svaka lista na prirodan način definira multiskup: $m(g) = |\ell^{-1}(g)|$, za $g \in G$. Svaki multiskup možemo definirati listom, ali ne jedinstvenom.

Definicija 4.5 *Neka je $D \subseteq G$ podskup grupe G.* **Lista razlika** *skupa D je funkcija*

$$\Delta D : \{(x, y) \mid x, y \in D,\ x \neq y\} \to G, \qquad \Delta D(x, y) = (-x) + y$$

Multiskup definiran listom razlika također označavamo ΔD.

Da bi definirali listu i multiskup razlika za familiju podskupova od G treba nam pojam unije lista, odnosno multiskupova.

Definicija 4.6 Unija multiskupova *je njihov zbroj, $m_1 \cup \cdots \cup m_n = m_1 + \ldots + m_n$.* **Disjunktna unija** *skupova $S_1, \ldots, S_n$ je skup $\dot{\bigcup}_i S_i = \bigcup_i S_i \times \{i\}$.* **Unija lista** *$\ell_1 : S_1 \to G, \ldots, \ell_n : S_n \to G$ je lista*

$$\ell \ = \ \ell_1 \cup \cdots \cup \ell_n \ : \ \dot{\bigcup_i} S_i \ \to \ G, \qquad \ell(x, i) = \ell_i(x).$$

Iz definicije slijedi da je multiskup pridružen uniji lista jednak uniji multiskupova pridruženih tim listama.

Definicija 4.7 Lista razlika *familije $\mathcal{F} = \{D_1, \ldots, D_n\}$ podskupova od G je unija njihovih lista razlika, $\Delta\mathcal{F} = \Delta D_1 \cup \cdots \cup \Delta D_n$. Pripadni multiskup također označavamo $\Delta\mathcal{F}$.*

Teorem 4.8 *Neka je $\mathcal{F} = \{D_1, \ldots, D_n\}$ familija k-članih podskupova grupe G koji imaju trivijalne stabilizatore i pripadaju različitim stazama pri djelovanju G na $\mathcal{P}_k(G)$. Tada je ekvivalentno:*

(1) *Multiskup razlika $\Delta\mathcal{F}$ sadrži svaki element iz $G \setminus \{0\}$ točno λ puta.*

(2) *Razvoj* $\operatorname{dev}\mathcal{F}$ *je (v, k, λ) blok dizajn.*

Dokaz. Neka je zadan dvočlani podskup $\{a, b\} \subseteq G$. Dokazat ćemo da je broj blokova od $\operatorname{dev}\mathcal{F}$ koji ga sadrže jednak broju pojavljivanja elementa $(-a) + b$ u multiskupu $\Delta\mathcal{F}$. Iz toga će slijediti tvrdnja teorema.

Blokove razvoja dev $\mathcal{F}$ možemo identificirati sa skupom

$$T \;=\; G \times \{1, \ldots, n\} \;=\; \{(g, i) \mid g \in G,\ i = 1, \ldots, n\}\,.$$

Preslikavanje $(g, i) \mapsto g + D_i$ koje elementima iz T pridružuje blokove je bijekcija, zbog pretpostavke da temeljni blokovi $D_1, \ldots, D_n$ imaju trivijalne stablizatore i pripadaju različitim G-orbitama. Broj blokova koji sadrže $\{a, b\}$ jednak je broju elemenata skupa

$$T_1 \;=\; \{(g, i) \in T \mid \{a, b\} \subseteq g + D_i\}\,.$$

S druge strane, domena liste razlika $\Delta\mathcal{F}$ je skup

$$S \;=\; \{(x, y, i) \mid x, y \in D_i,\ x \neq y,\ i = 1, \ldots, n\}\,.$$

Pripadni multiskup sadrži $(-a) + b$ onoliko puta koliko ima elemenata u

$$S_1 \;=\; \Delta\mathcal{F}^{-1}((-a) + b) \;=\; \{(x, y, i) \in S \mid (-x) + y = (-a) + b\}\,.$$

Treba dokazati jednakobrojnost skupova S_1 i T_1. Funkcije

$$\varphi : S_1 \to T_1, \quad \varphi(x, y, i) = (a - x, i) = (b - y, i)$$

$$\psi : T_1 \to S_1, \quad \psi(g, i) = ((-g) + a, (-g) + b, i)$$

su dobro definirane i jedna drugoj inverzne. Slijedi $|S_1| = |T_1|$, čime je teorem dokazan.

■

Definicija 4.9 *Neka $\mathcal{F}$ zadovoljava pretpostavke teorema 4.8 i bilo koju od ekvivalentnih tvrdnji (1), (2). Tada $\mathcal{F}$ zovemo (v, k, λ)* **diferencijska familija**.

Propozicija 4.10 *Ako postoji (v, k, λ) diferencijska familija, onda je $\lambda(v - 1) \equiv 0 \pmod{k(k-1)}$.*

Dokaz. Neka je $\mathcal{F} = \{D_1, \ldots, D_n\}$ (v, k, λ) diferencijska familija. Domena liste razlika $\Delta\mathcal{F}$ ima $nk(k-1)$ elemenata. Razlike pokrivaju skup $G \setminus \{0\}$ točno λ puta, pa je taj broj jednak $\lambda \cdot |G \setminus \{0\}| = \lambda(v - 1)$.

■

Korolar 4.11 *Ako je $\mathcal{F} = \{D_1, \ldots, D_n\}$ $(v, k, 1)$ diferencijska familija, onda je $v = nk^2 - nk + 1$.*

Vidimo da Steinerovi 2-dizajni konstruirani pomoću $(v, k, 1)$ diferencijskih familija imaju parametre oblika $S(k, nk^2 - nk + 1)$ i dopuštaju grupu automorfizama regularnu na točkama. Sljedeći cilj je dokazati obrat: ako Steinerov 2-dizajn $S(k, nk^2 - nk + 1)$ ima grupu automorfizama regularnu na točkama, može se konstruirati pomoću diferencijske familije.

Lema 4.12 *Neka Steinerov 2-dizajn $S(k, nk^2 - nk + 1)$ ima grupu automorfizama G regularnu na točkama. Tada su G-stabilizatori pravaca trivijalni.*

Dokaz. Pretpostavimo suprotno, da postoji pravac $\ell = \{T_1, \ldots, T_k\}$ invarijantan obzirom na netrivijalni automorfizam $\alpha \in G$. Možemo pretpostaviti da je α prostog reda p. U suprotnom, ako je α reda $p \cdot r$ za $r > 1$, zamijenimo ga s α^r. Zbog regularnosti α nema fiksnih točaka, pa iz $\alpha(\{T_1, \ldots, T_k\}) = \{T_1, \ldots, T_k\}$ slijedi $p \mid k$. No p dijeli i $v = |G|$, što je kontradikcija jer su k i $v = nk^2 - nk + 1$ relativno prosti. ■

Propozicija 4.13 *Neka Steinerov 2-dizajn S s parametrima $S(k, nk^2 - nk + 1)$ ima grupu automorfizama G regularnu na točkama. Tada postoji diferencijska familija $\mathcal{F}$ u G takva da je* $\operatorname{dev}\mathcal{F} \cong S$.

Dokaz. Zbog regularnosti možemo identificirati točke s automorfizmima. To znači da je G skup točaka od S, a pravci su neki k-člani podskupovi od G. Broj pravaca je $b = \frac{v(v-1)}{k(k-1)} = vn$. Zbog leme 4.12 orbite na pravcima su duljine v, pa je broj orbita n. Odaberemo po jedan pravac iz svake od orbita: $\ell_1, \ldots, \ell_n$. Temeljni blokovi neka su ti pravci. Ako prihvatimo aditivnu notaciju u G, orbite na pravcima su $G + \ell_1, \ldots, G + \ell_n$. Slijedi $\operatorname{dev}\{\ell_1, \ldots, \ell_n\} = S$. ■

Napomena 4.14 Uvjet da su parametri oblika $S(k, nk^2 - nk + 1)$ je nuždan, kao što pokazuje sljedeći primjer. Neka je $G = \mathbb{Z}_{15}$ i $\mathcal{F} = \{\{0, 1, 4\}, \{0, 2, 9\}, \{0, 5, 10\}\}$. Razvoj $\operatorname{dev}\mathcal{F}$ je Steinerov 2-dizajn $S(3, 15)$. On prema propoziciji 4.3 ima $\mathbb{Z}_{15}$ kao grupu automorfizama koja djeluje regularno na točke. Međutim, $v = 15$ nije oblika $nk^2 - nk + 1 = 6n + 1$, pa se $\operatorname{dev}\mathcal{F}$ ne može konstruirati pomoću diferencijske familije (korolar 4.11). Zaista, temeljni blok $\{0, 5, 10\}$ ima netrivijalni stabilizator, a 5 i 10 mogu se na više načina prikazati kao razlike ($\Delta\mathcal{F}$ sadrži svakog po tri puta). Stoga $\mathcal{F}$ nije diferencijska familija, prema definiciji 4.9. Ponekad se u definiciji diferencijske familije dozvoljavaju blokovi s netrivijalnim stabilizatorom, koji se nazivaju *kratki blokovi*.

Steinerovi 2-dizajni koje proučavamo u ovom radu imaju parametre oblika $S(k, 2k^2 - 2k + 1)$, prikladne za konstrukciju pomoću diferencijskih familija s dva temeljna bloka ($n = 2$).

Teorem 4.15 *Steinerovi 2-dizajni $S(k, 2k^2-2k+1)$ s grupom automorfizama regularnom na točkama postoje i jedinstveni su za $k = 3, 4, 5$, a ne postoje za $k = 6, 7, 8$.*

Dokaz. Za $k = 3$ postoje dva dizajna $S(3, 13)$. Dizajn $S3.1$ ima $\mathbb{Z}_{13}$ kao regularnu grupu automorfizama. Puna grupa automorfizama dizajna $S3.2$ ne djeluje tranzitivno, pa ne može imati regularnu podgrupu (vidi tablicu 1).

Za $k = 4$ postoji osamnaest dizajna $S(4, 25)$. Od toga jedino dizajn $S4.2$ ima punu grupu automorfizama tranzitivnu na točkama. Ona ima podgrupu koja djeluje regularno, izomorfnu sa $\mathbb{Z}_5 \times \mathbb{Z}_5$. Ostali $S(4, 25)$ dizajni ne mogu se konstruirati pomoću diferencijske familije.

Za $k = 5$ dizajni $S(5, 41)$ nisu potpuno klasificirani. Od poznatih primjera jedino $S5.1$ dopušta grupu automorfizama regularnu na točkama. To dokazuje samo egzistenciju, pa treba još dokazati jedinstvenost za $k = 5$ i nepostojanje za $k = 6, 7, 8$.

Primijetimo najprije da su grupe reda 41, 61, 85 i 113 jedinstvene. Radi se naravno o cikličkim grupama. Problem rješavamo računalom, pomoću programa `dfsearch` koji sustavno traži diferencijske familije u cikličkim grupama. U grupi $\mathbb{Z}_{41}$ dobivamo nekoliko diferencijskih familija s $n = 2$, čiji su razvoji izomorfni dizajnu $S5.1$. Zaključujemo da je to jedini $S(5, 41)$ dizajn s regularnom grupom automorfizama. U grupama $\mathbb{Z}_{61}$, $\mathbb{Z}_{85}$ i $\mathbb{Z}_{113}$ program ne nalazi diferencijske familije s $n = 2$. Prema tome, ne postoje dizajni $S(6, 61)$, $S(7, 85)$ i $S(8, 113)$ s regularnim grupama automorfizama. ■

Napomena 4.16 Potraga za $(113, 8, 1)$ diferencijskim familijama trajala je na računalima koja su mi bila dostupna oko tjedan dana. Njihovo nepostojanje je nov rezultat.

4.2 Wilsonov teorem

Vidjeli smo da su poznata tri Steinerova 2-dizajna $S(k, 2k^2 - 2k + 1)$ koje je moguće konstruirati pomoću diferencijske familije. Egzistencija pripadnih diferencijskih familija slijedi iz teorema R.M.Wilsona [21]. U tom teoremu ulogu grupe G igra zbrajanje u konačnom polju. Osnovna svojstva konačnih polja sabrana su u sljedećem teoremu.

Teorem 4.17 (1) *Konačno polje s q elemenata postoji ako i samo ako je q prim potencija. Ako postoji, jedinstveno je do na izomorfizam i označavamo ga s $GF(q)$.*

(2) *Aditivna grupa polja $GF(q)$ je elementarno Abelova, reda q. Multiplikativna grupa je ciklička, reda $q-1$. Svaki generator multiplikativne grupe nazivamo* **primitivni element** *polja $GF(q)$.*

(3) *Ako je $q-1 = m \cdot n$, multiplikativna grupa ima jedinstvenu podgrupu reda n i indeksa m, koju označavamo H^m. Radi se o n-tim korijenima jedinice, odnosno m-tim potencijama ne-nul elemenata:*

$$H^m \;=\; \{\xi \in GF(q) \mid \xi^n = 1\} \;=\; \{\xi^m \mid \xi \in GF(q) \setminus \{0\}\}.$$

(4) *Ako je q paran, $-1 = 1$ pa sve podgrupe H^m sadrže -1. Ako je q neparan, $-1 \in H^m$ ako i samo ako je $n = \frac{q-1}{m}$ paran.*

Definicija 4.18 *Ako liste $\ell_1 : S \to G$ i $\ell_2 : T \to G$ definiraju isti multiskup na G kažemo da su* **ekvivalentne** *i pišemo $\ell_1 \approx \ell_2$.*

Lema 4.19 *Liste $\ell_1 : S \to G$, $\ell_2 : T \to G$ su ekvivalentne ako i samo ako postoji bijekcija $\varphi : T \to S$ sa svojstvom $\ell_2 = \ell_1 \circ \varphi$.*

Dokaz. ($\Rightarrow$) Za svaki $g \in G$ skupovi $S_g = \ell_1^{-1}(g)$ i $T_g = \ell_2^{-1}(g)$ su jednakobrojni, pa postoji bijekcija $\varphi_g : T_g \to S_g$. Traženu bijekciju $\varphi : T \to S$ dobivamo proširivanjem, $\varphi(x) = \varphi_{\ell_2(x)}(x)$.

($\Leftarrow$) Iz $\ell_2 = \ell_1 \circ \varphi$ slijedi $\ell_2^{-1}(g) = (\ell_1 \circ \varphi)^{-1}(g) = \varphi^{-1}(\ell_1^{-1}(g))$. Zbog bijektivnosti od φ to povlači $|\ell_2^{-1}(g)| = |\ell_1^{-1}(g)|$, za svaki $g \in G$. ■

Definicija 4.20 Produkt lista *$\ell_1 : S \to GF(q)$ i $\ell_2 : T \to GF(q)$ je lista $\ell_1 \cdot \ell_2 : S \times T \to GF(q)$, $(\ell_1 \cdot \ell_2)(x, y) = \ell_1(x) \cdot \ell_2(y)$.*

Lema 4.21 *Množenje lista u $GF(q)$ je do na ekvivalenciju distributivno obzirom na uniju, $(\ell_1 \cup \ell_2) \cdot \ell_3 \approx (\ell_1 \cdot \ell_3) \cup (\ell_2 \cdot \ell_3)$.*

Dokaz. Ako domenu od ℓ_i označimo sa S_i, domena liste $(\ell_1 \cup \ell_2) \cdot \ell_3$ je

$$S \;=\; (S_1 \dot{\cup} S_2) \times S_3 \;=\; \{\,(x,i,y) \mid x \in S_i,\ i \in \{1,2\},\ y \in S_3\,\}\,.$$

S druge strane, domena od $(\ell_1 \cdot \ell_3) \cup (\ell_2 \cdot \ell_3)$ je skup

$$T \;=\; (S_1 \times S_3) \dot{\cup} (S_2 \times S_3) \;=\; \{\,(x,y,i) \mid x \in S_i,\ y \in S_3,\ i \in \{1,2\}\,\}\,.$$

Funkcija $\varphi : T \to S,\ \ \varphi(x,y,i) = (x,i,y)$ očito je bijekcija i vrijedi $(\ell_1 \cdot \ell_3) \cup (\ell_2 \cdot \ell_3) = [(\ell_1 \cup \ell_2) \cdot \ell_3] \circ \varphi$.

■

Teorem 4.22 (Wilson, 1972.) *Neka je $q = nk^2 - nk + 1$ prim potencija, a ω primitivni element konačnog polja $GF(q)$.*

(1) *Ukoliko je $k = 2m+1$ neparan, neka je $\varepsilon = \omega^{2mn}$ i $D = \{1, \varepsilon, \ldots, \varepsilon^{k-1}\}$. Ako elementi $\varepsilon - 1, \varepsilon^2 - 1, \ldots, \varepsilon^m - 1$ pripadaju različitim klasama modulo H^m, onda je $\mathcal{F} = \{D, \omega^m D, \ldots, \omega^{(n-1)m} D\}$ $(q,k,1)$ diferencijska familija.*

(2) *Ukoliko je $k = 2m$ paran, neka je $\varepsilon = \omega^{2mn}$ i $D = \{0, 1, \varepsilon, \ldots, \varepsilon^{k-2}\}$. Ako elementi $1, \varepsilon - 1, \ldots, \varepsilon^{m-1} - 1$ pripadaju različitim klasama modulo H^m, onda je $\mathcal{F} = \{D, \omega^m D, \ldots, \omega^{(n-1)m} D\}$ $(q,k,1)$ diferencijska familija.*

Dokaz. (1) Prvo dokazujemo teorem za neparni k. U tom slučaju ε je primitivni k-ti korijen jedinice, tj. generator podgrupe $D = H^{2mn}$. Vidjet ćemo da multiskup $\Delta\mathcal{F}$ sadrži svaki ne-nul element točno jednom. Iz toga slijedi da temeljni blokovi leže u različitim stazama i imaju trivijalne stabilizatore obzirom na djelovanje aditivne grupe. Kad bi dva temeljna bloka pripadala istoj orbiti, pripadne liste razlika bile bi jednake pa bi $\Delta\mathcal{F}$ neke elemente sadržao bar dva puta. Nadalje, kad bi za neki $\alpha \neq 0$ vrijedilo $\alpha + \omega^{im} D = \omega^{im} D$, taj bi se α na više načina mogao prikazati kao razlika elemenata iz $\omega^{im} D$.

Preostaje dokazati da $\Delta\mathcal{F}$ pokriva $GF(q) \setminus \{0\}$ točno jednom. Dokaz se sastoji od tri koraka.

Korak 1. $\quad \Delta D \approx \pm D \cdot (\varepsilon - 1, \varepsilon^2 - 1, \ldots, \varepsilon^m - 1)$

Na lijevoj strani je lista razlika skupa D. To je funkcija

$$\ell_1 : S = \{\,(x,y) \mid x,y \in D,\ x \neq y\} \to GF(q), \qquad \ell_1(x,y) = y - x.$$

Skup $\pm D$ definiran je s $\pm D = D \cup -D$. Skupovi D i $-D$ su disjunktni, jer je $\frac{q-1}{2mn} = k$ neparan, pa po teoremu 4.17 (4) D ne sadrži -1. Podskupove

od $GF(q)$ možemo također shvatiti kao liste, identificirajući ih s pripadnim inkluzijama. Na desnoj strani je produkt lista $\pm D$ i $(\varepsilon - 1, \ldots, \varepsilon^m - 1)$:

$$\ell_2 : T = \pm D \times \{1, \ldots, m\} \to GF(q), \qquad \ell_2(x, i) = x \cdot (\varepsilon^i - 1).$$

Želimo dokazati da su liste ℓ_1 i ℓ_2 ekvivalentne. Definiramo funkciju

$$\varphi : T \to S, \qquad \varphi(x, i) = \begin{cases} (x, \varepsilon^i x), & \text{ako je } x \in D \\ (-\varepsilon^i x, -x), & \text{ako je } x \in -D \end{cases}$$

φ je dobro definirana i vrijedi $\ell_2 = \ell_1 \circ \varphi$. Osim toga, φ je injekcija. Pretpostavimo $\varphi(x, i) = \varphi(y, j)$. Ako x i y nisu u istom skupu D ili $-D$, recimo $x \in D$, $y \in -D$, slijedi

$$(x, \varepsilon^i x) = (-\varepsilon^j y, -y) \quad \Rightarrow \quad x = -\varepsilon^j y,\ \varepsilon^i x = -y \quad \Rightarrow \quad -\varepsilon^{i+j} y = -y \quad \Rightarrow$$
$$\Rightarrow \quad \varepsilon^{i+j} = 1 \quad \Rightarrow \quad i + j \equiv 0 \pmod{k}.$$

Ova kongruencija nije moguća, jer je $1 \leq i, j \leq m$, $k = 2m + 1$. Zato x i y oba pripadaju jednom od skupova D ili $-D$, iz čega slijedi $(x, i) = (y, j)$. Injektivnost i jednakobrojnost domene i kodomene ($|T| = 2km = k(k-1) = |S|$) povlače bijektivnost od φ. Prema 4.19 liste ℓ_1 i ℓ_2 su ekvivalentne, čime je prvi korak dokazan.

Korak 2. $\quad \pm D = H^{mn}$

Znamo da je $D = H^{2mn}$ podgrupa reda k. Skup $\pm D$ je zatvoren obzirom na množenje i invertiranje, pa je i to podgrupa. Ona je reda $2k$, jer su D i $-D$ disjunktni. Zbog jedinstvenosti u teoremu 4.17 (3) $\pm D$ se podudara s H^{mn}.

Korak 3. $\quad \Delta\mathcal{F} \approx H^m \cdot (\varepsilon - 1, \varepsilon^2 - 1, \ldots, \varepsilon^m - 1)$

U prva dva koraka dokazali smo $\Delta D \approx H^{mn} \cdot (\varepsilon - 1, \ldots, \varepsilon^m - 1)$. Lako se provjeri $\Delta(\omega^{im} D) \approx \omega^{im} \Delta D$, pa slijedi

$$\Delta\mathcal{F} \;=\; \bigcup_{i=0}^{n-1} \Delta(\omega^{im} D) \;\approx\; \bigcup_{i=0}^{n-1} \omega^{im} \Delta D \;\approx\; \bigcup_{i=0}^{n-1} \left[\omega^{im} H^{mn} \cdot (\varepsilon - 1, \ldots, \varepsilon^m - 1)\right]$$
$$\approx (\text{lema } 4.21) \approx \left[\bigcup_{i=0}^{n-1} \omega^{im} H^{mn}\right] \cdot (\varepsilon - 1, \ldots, \varepsilon^m - 1)$$

Nadalje,

$$\bigcup_{i=0}^{n-1} \omega^{im} H^{mn} \;=\; \bigcup_{i=0}^{n-1} \omega^{im} \left\{\omega^{jmn} \mid j = 0, \ldots, 2k-1\right\} \;=$$

$$= \bigcup_{i=0}^{n-1} \{\omega^{(i+jn)m} \mid j = 0, \ldots, 2k-1\} = \{\omega^{rm} \mid r = 0, \ldots, 2nk-1\} = H^m$$

Time je i treći korak dokazan. Ako $\varepsilon - 1, \ldots, \varepsilon^m - 1$ pripadaju različitim klasama modulo H^m, skupovi $H^m(\varepsilon - 1), \ldots, H^m(\varepsilon^m - 1)$ su međusobno disjunktni. Zajedno s tvrdnjom trećeg koraka to povlači $\Delta\mathcal{F} \approx GF(q) \setminus \{0\}$.

(2) Za parni k dokaz je sličan. ε je primitivni $(k-1)$-vi korijen jedinice (generator od H^{2mn}), a $D = \{0\} \cup H^{2mn}$. Temeljni blokovi pripadaju različitim stazama i imaju trivijalne stabilizatore. To slijedi iz $\Delta\mathcal{F} \approx GF(q) \setminus \{0\}$, što ponovo dokazujemo u tri koraka.

Korak 1. $\Delta D \approx \pm H^{2mn} \cdot (1, \varepsilon - 1, \ldots, \varepsilon^{m-1} - 1)$

Korak 2. $\pm H^{2mn} = H^{mn}$

Korak 3. $\Delta\mathcal{F} \approx H^m \cdot (1, \varepsilon - 1, \ldots, \varepsilon^{m-1} - 1)$

Dokazi ovih triju tvrdnji analogni su dokazima iz slučaja (1), pa ih nećemo ponavljati.

■

Propozicija 4.23 *Steinerov 2-dizajn konstruiran pomoću teorema 4.22 ima kao grupu automorfizama semidirektan produkt grupe H^{2mn} s aditivnom grupom od $GF(q)$, pri čemu H^{2mn} djeluje množenjem na $GF(q)$.*

Dokaz. Neka je $G = H^{2mn} \times GF(q)$. Operaciju u G definiramo s

$$(h_1, g_1)(h_2, g_2) = (h_1h_2, g_1 + h_1g_2).$$

Pokazuje se da je G grupa, semidirektan produkt od H^{2mn} i $GF(q)$. Djelovanje na točke i pravce od dev $\mathcal{F}$ zadano je formulama

$$(h, g)x = hx + g, \quad (h, g)(y + \omega^{im}D) = hy + g + \omega^{im}D.$$

Budući da su temeljni blokovi invarijantni obzirom na množenje elementima iz H^{2mn}, vrijedi $x \in y + \omega^{im}D \iff hx + g \in hy + g + \omega^{im}D$. Zato je G grupa automorfizama od dev $\mathcal{F}$.

■

Primjer 4.24 Nas prvenstveno zanima primjena teorema za $n = 2$, jer tako dobivamo Steinerove 2-dizajne $S(k, 2k^2 - 2k + 1)$. Pogledajmo najprije slučaj $k = 3$, u kojem je $q = 13$ primbroj. Konačno polje $GF(13)$ čine cijeli

brojevi sa zbrajanjem i množenjem modulo 13, $(\mathbb{Z}_{13}, +_{13}, \cdot_{13})$. Za primitivni element možemo uzeti $\omega = 2$. k je neparan, $m = 1$, $\varepsilon = \omega^{2mn} = 3$ i $D = \{1, 3, 9\}$. Skup elemenata za koje treba provjeriti da leže u različitim klasama modulo H^m je jednočlan, pa je uvjet ispunjen. Prema teoremu 4.22 $\mathcal{F}_3 = \{D, \omega D\} = \{\{1, 3, 9\}, \{2, 6, 5\}\}$ je $(13, 3, 1)$ diferencijska familija. Razvoj dev $\mathcal{F}_3$ izomorfan je sa $S3.1$ i prema 4.23 ima grupu automorfizama $\mathbb{Z}_3 \,.\, \mathbb{Z}_{13}$. To je ujedno puna grupa automorfizama.

Primjer 4.25 Za $n = 2$, $k = 4$ dobivamo prim potenciju $q = 25$. Konačno polje $GF(25)$ konstruiramo kao kvocijent $\mathbb{Z}_5[x]/(x^2 + 2)$ prstena polinoma nad $\mathbb{Z}_5$. Polinom $x^2 + 2$ je ireducibilan, pa je ideal $(x^2 + 2)$ maksimalan. To znači da je kvocijentni prsten polje, koje očito ima 25 elemenata. Kao primitivni element ω uzmimo polinom $x + 1$. U ovom slučaju k je paran, $m = 2$, $\varepsilon = \omega^{2mn} = (x+1)^8 \equiv x+2 \pmod{x^2+2}$ i $D = \{0, 1, x+2, 4x+2\}$. Treba provjeriti da 1 i $\varepsilon - 1 = x + 1$ leže u različitim klasama modulo $H^2 = \langle \omega^2 \rangle$. To vrijedi jer je $1 \in H^2$, a $\varepsilon - 1 = \omega \notin H^2$. Wilsonov teorem nam daje $(25, 4, 1)$ diferencijsku familiju $\mathcal{F}_4 = \{D, \omega^2 D\} = \{\{0, 1, x+2, 4x+2\}, \{0, 2x+4, 3x+4, 2\}\}$. Razvoj dev $\mathcal{F}_4$ izomorfan je sa $S4.2$. Na njemu prema 4.23 djeluje $G = \mathbb{Z}_3 \,.\, (\mathbb{Z}_5 \times \mathbb{Z}_5)$, ali to nije puna grupa automorfizama. Involucija $\alpha x + \beta \mapsto -\alpha x + \beta$ ostavlja temeljne blokove invarijantnim. Zato je ona također automorfizam, koji s G tvori semidirektan produkt. Tako dobivamo punu grupu automorfizama od dev $\mathcal{F}_4$, $\mathbb{Z}_2 \,.\, G$.

Primjer 4.26 Za $n = 2$ i $k = 5$ dobivamo primbroj $q = 41$. $\omega = 6$ je primitivni element polja $GF(41) = (\mathbb{Z}_{41}, +_{41}, \cdot_{41})$. k je neparan, $m = 2$, $\varepsilon = 10$ i $D = \{1, 10, 18, 16, 37\}$. Brojevi $\varepsilon - 1 = 9$ i $\varepsilon^2 - 1 = 17$ leže u različitim klasama modulo H^2 jer 9 jest, a 17 nije dvadeseti korijen jedinice (tj. $9 \in H^2$, $17 \notin H^2$). Zato je $\mathcal{F}_5 = \{D, \omega^2 D\} = \{\{1, 10, 18, 16, 37\}, \{36, 32, 33, 2, 20\}\}$ $(41, 5, 1)$ diferencijska familija u $\mathbb{Z}_{41}$. Razvoj dev $\mathcal{F}_5$ je izomorfan sa $S5.1$, a propozicija 4.23 ponovo daje punu grupu automorfizama $\mathbb{Z}_5 \,.\, \mathbb{Z}_{41}$.

Definicija 4.27 *Neka je $q = nk^2 - nk + 1$ prim potencija. Za $(q, k, 1)$ diferencijsku familiju u $GF(q)$ kažemo da je* **radikalna** *ako:*

– *za neparni k, temeljni blokovi su klase modulo $H^{(k-1)n}$*

– *za parni k, temeljni blokovi su unije klasa modulo H^{kn} s nulom.*

'Radikalna diferencijska familija' kratko pišemo RDF.

Teorem 4.22 daje dovoljan uvjet za postojanje radikalne diferencijske familije. Ako za neparni k elementi $\varepsilon-1,\ldots,\varepsilon^m-1$, a za parni $1,\varepsilon-1,\ldots,\varepsilon^{m-1}-1$ pripadaju različitim klasama modulo H^m, onda je $\mathcal{F}=\{\omega^{im}D \mid i=0,\ldots,n-1\}$ RDF.

Uvjet teorema nije nuždan. Neka je $k=2m=4$, $n=16$, $q=193$. Primitivni element polja $GF(193)$ je $\omega=5$. Označimo $\varepsilon=\omega^{2mn}=84$, $D=\{0\}\bigcup H^{kn}=\{0,1,84,108\}$. Budući da 1 i $\varepsilon-1=83$ oba leže u H^m, familija $\mathcal{F}=\{\omega^{2i}D \mid i=0,\ldots,15\}$ iz 4.22 nije diferencijska. Međutim, u $GF(193)$ ipak postoji RDF: $\mathcal{F}'=\{\omega^{i+4j}D \mid i=0,1,\ j=0,\ldots,7\}$.

M. Buratti je u [3] dao slabiji uvjet za postojanje radikalne diferencijske familije. Uz oznake teorema 4.22, kvocijente iz skupa $A\subseteq GF(q)\setminus\{0\}$ označimo $\Phi(A)=\{xy^{-1} \mid x,y\in A\}$. Neka postoji niz djelitelja $d_0=1\,|\,d_2\,|\,d_3\,|\cdots|\,d_{2s+1}=mn$ takav da:

(1) $n=\displaystyle\prod_{i=0}^{s}\frac{d_{2i+1}}{d_{2i}}$

(2) Za neparni k skup $\Phi(\varepsilon-1,\ldots,\varepsilon^m-1)$, a za parni $\Phi(1,\varepsilon-1,\ldots,\varepsilon^{m-1}-1)$ sadržan je u $\displaystyle\bigcup_{i=1}^{s}\left(H^{d_{2i+1}}\setminus H^{d_{2i}}\right)\bigcup\{1\}$.

Tada je $\mathcal{F}'=\{\omega^iD \mid i\in I\}$, $I=\left\{\sum_{i=0}^{s}k_id_{2i} \mid 0\le k_i<\frac{d_{2i+1}}{d_{2i}},\ i=0,\ldots,s\right\}$ radikalna diferencijska familija.

Wilsonov uvjet implicira Burattijev, a ako su m i n relativno prosti s njim je ekvivalentan. Burattijev uvjet je i nuždan za $k\le 7$. Radikalna diferencijska familija u $GF(193)$ dobivena je pomoću niza djelitelja $1\,|\,2\,|\,4\,|\,8\,|\,8\,|\,16\,|\,16\,|\,32$.

U sljedećoj propoziciji dan je jedan nuždan uvjet za postojanje RDF.

Propozicija 4.28 *Neka je $q=nk^2-nk+1$ prim potencija, ω primitivni element u $GF(q)$, $m=\left\lfloor\frac{k}{2}\right\rfloor$, $\varepsilon=\omega^{2mn}$. Ako postoji radikalna $(q,k,1)$ diferencijska familija, onda za neparni k elementi $\varepsilon-1,\ldots,\varepsilon^m-1$, a za parni $1,\varepsilon-1,\ldots,\varepsilon^{m-1}-1$ leže u različitim klasama modulo H^{mn}.*

Dokaz. Neka je $k=2m+1$ neparan. Uvjet da $\varepsilon-1,\ldots,\varepsilon^m-1$ pripadaju različitim klasama modulo H^{mn} ne ovisi o izboru primitivnog elementa ω, iako je $\varepsilon=\omega^{2mn}$ definiran pomoću njega. Naime, vrijedi

$$\varepsilon^{k-i}-1 \;=\; \varepsilon^{k-i}-\varepsilon^k \;=\; -\varepsilon^{k-i}(\varepsilon^i-1).$$

Elementi $\varepsilon^{k-i}-1$ i ε^i-1 pripadaju istoj klasi modulo H^{mn}, jer je $-\varepsilon^{k-i}\in H^{mn}$ (zbog $(-\varepsilon^{k-i})^{2k}=1$). Vidimo da je uvjet ekvivalentan s uvjetom da skup

$\{\varepsilon-1,\ldots,\varepsilon^m-1,\varepsilon^{m+1}-1,\ldots,\varepsilon^{2m}-1\}=(H^{2mn}-1)\setminus\{0\}$ siječe svaku klasu modulo H^{mn} najviše u dva elementa. To očito ne ovisi o izboru ω.

U dokazu teorema 4.22 vidjeli smo da je $\Delta(\alpha H^{2mn})\approx\alpha H^{mn}\cdot(\varepsilon-1,\ldots,\varepsilon^m-1)$. Ako dva elementa među $\varepsilon-1,\ldots,\varepsilon^m-1$ pripadaju istoj klasi modulo H^{mn}, multiskupovi razlika klasa αH^{2mn} sadrže neke elemente dva ili više puta. Tada klase ne mogu biti temeljni blokovi diferencijske familije.

Dokaz je za parni k sličan.

■

Pomoću propozicije 4.28 možemo ustanoviti nepostojanje radikalnih diferencijskih familija. Zanima nas slučaj $n=2$; promotrimo u kojim je od polja $GF(q)$, $q=2k^2-2k+1$ ispunjen nužni uvjet. Za $k=3,4,5,6,8,10$ elementi $\varepsilon-1,\ldots,\varepsilon^m-1$, odnosno $1,\varepsilon-1,\ldots,\varepsilon^{m-1}-1$ pripadaju različitim klasama modulo H^{mn}. Znamo da RDF postoje za $k=3,4,5$. Za $k=6,8,10$ liste razlika skupova oblika $\{0\}\cup\alpha H^{2mn}$ imaju u parovima neprazne presjeke, pa ne mogu tvoriti diferencijske familije. Nužni uvjet nije zadovoljen za $11\le k\le 2000$, kad god je $q=2k^2-2k+1$ prim potencija. To sam provjerio pomoću sustava za računalnu algebru *Mathematica* (`Wilson.nb`). Time je dokazan sljedeći rezultat.

Propozicija 4.29 *Radikalne* $(2k^2-2k+1,k,1)$ *diferencijske familije postoje za* $k=3,4,5$, *a ne postoje za* $6\le k\le 2000$.

5 Konstrukcija pomoću grupa automorfizama

5.1 Metoda konstrukcije

U ovom poglavlju koristimo poznatu metodu za konstrukciju blok dizajna sa zadanim parametrima i grupom automorfizama. Metodu je među prvima uspješno upotrebljavao hrvatski matematičar Z.Janko, pa je kod nas poznata kao "Jankova metoda". Centralnu ulogu igra pojam taktičke dekompozicije.

Definicija 5.1 *Neka je* $(\mathcal{P}, \mathcal{L}, I)$ *incidencijska struktura.* **Taktička dekompozicija** *sastoji se od particije skupa točaka* $\mathcal{P} = \mathcal{P}_1 \dot\cup \cdots \dot\cup \mathcal{P}_m$ *i particije skupa pravaca* $\mathcal{L} = \mathcal{L}_1 \dot\cup \cdots \dot\cup \mathcal{L}_n$ *takvih da za svake* $1 \le i \le m$, $1 \le j \le n$ *vrijedi:*

(1) *Broj točaka iz* $\mathcal{P}_i$ *incidentnih s pravcem* $\ell \in \mathcal{L}_j$ *ne ovisi o izboru tog pravca.*

(2) *Broj pravaca iz* $\mathcal{L}_j$ *incidentnih s točkom* $T \in \mathcal{P}_i$ *ne ovisi o izboru te točke.*

Propozicija 5.2 *Neka je* G *grupa automorfizama incidencijske strukture. Particija skupa točaka i pravaca na* G*-orbite čini taktičku dekompoziciju.*

Dokaz. Neka su ℓ, ℓ' pravci iz iste G-orbite $\mathcal{L}_j$, tj. $\ell' = g\ell$ za neki $g \in G$. Neka je $\mathcal{P}_i$ orbita na točkama. Djelovanje grupe G na točke i pravce čuva incidenciju. Stoga je $T \mapsto gT$ bijekcija između skupa točaka iz $\mathcal{P}_i$ incidentnih s ℓ, odnosno ℓ'. Svojstvo (2) dokazuje se analogno. ■

Taktička dekompozicija dizajna ima dodatne pravilnosti. Neka je $(\mathcal{P}, \mathcal{L}, I)$ blok dizajn s parametrima v, b, r, k, λ, a $\mathcal{P} = \mathcal{P}_1 \dot\cup \cdots \dot\cup \mathcal{P}_m$, $\mathcal{L} = \mathcal{L}_1 \dot\cup \cdots \dot\cup \mathcal{L}_n$ taktička dekompozicija. Označimo duljine blokova sa $\nu_i = |\mathcal{P}_i|$ i $\beta_j = |\mathcal{L}_j|$. Vektore $\nu = (\nu_1, \ldots, \nu_m)$ i $\beta = (\beta_1, \ldots, \beta_n)$ zovemo *marginalni vektori*. Očito vrijedi $\sum_{i=1}^{m} \nu_i = v$ i $\sum_{j=1}^{n} \beta_j = b$.

Označimo nadalje

$$a_{ij} = |\{\ell \in \mathcal{L}_j \mid T\, I\, \ell\}|, \quad \text{za bilo koju točku } T \in P_i$$

$$b_{ij} = |\{T \in \mathcal{P}_i \mid T\, I\, \ell\}|, \quad \text{za bilo koji pravac } \ell \in \mathcal{L}_j$$

Brojevi su dobro definirani zbog definicijskih svojstava taktičke dekompozicije. Proučimo pobliže matrice $A = [a_{ij}]$ i $B = [b_{ij}] \in M_{mn}(\mathbb{N}_0)$.

Lema 5.3

$$\sum_{j=1}^{n} a_{ij} = r, \quad \textit{za svaki } 1 \leq i \leq m.$$

$$\sum_{i=1}^{m} b_{ij} = k, \quad \textit{za svaki } 1 \leq j \leq n.$$

Dokaz. $\sum\limits_{j=1}^{n} a_{ij} = \sum\limits_{j=1}^{n} |\{\ell \in \mathcal{L}_j \mid T\, I\, \ell\}| = |\{\ell \in \mathcal{L} \mid T\, I\, \ell\}| = r.$ Druga tvrdnja dokazuje se analogno.

■

Lema 5.4 *Za svaki* $1 \leq i \leq m$, $1 \leq j \leq n$ *vrijedi* $\nu_i\, a_{ij} = \beta_j\, b_{ij}$.

Dokaz. Dvostrukim prebrojavanjem incidentnih parova iz $\mathcal{P}_i \times \mathcal{L}_j$.

■

Lema 5.5 *Za sve* $1 \leq i, i' \leq m$ *vrijedi*

$$\sum_{j=1}^{n} a_{i'j} b_{ij} = \begin{cases} \lambda\nu_i, & \textit{ako je } i \neq i' \\ \lambda(\nu_i - 1) + r, & \textit{ako je } i = i' \end{cases}$$

Dokaz. Neka je $T \in \mathcal{P}_{i'}$ bilo koja točka. Skup svih pravaca koji prolaze kroz T označavamo (T). Računamo:

$$\sum_{j=1}^{n} a_{i'j} b_{ij} \;=\; \sum_{j=1}^{n} |\{\ell \in \mathcal{L}_j \mid T\, I\, \ell\}| \cdot b_{ij} \;=\; \sum_{j=1}^{n} b_{ij} \cdot \sum_{\ell \in (T) \cap \mathcal{L}_j} 1 \;=$$

$$= \sum_{j=1}^{n} \sum_{\ell \in (T) \cap \mathcal{L}_j} b_{ij} \;=\; \sum_{j=1}^{n} \sum_{\ell \in (T) \cap \mathcal{L}_j} |\{P \in \mathcal{P}_i \mid P\, I\, \ell\}| \;=$$

$$= \sum_{j=1}^{n} |\{(P, \ell) \mid P \in \mathcal{P}_i,\ \ell \in (T) \cap \mathcal{L}_j,\ P\, I\, \ell\}| \;=$$

$$= \sum_{j=1}^{n} \sum_{P \in \mathcal{P}_i} |\{\ell \in (T) \cap \mathcal{L}_j \mid P\, I\, \ell\}| \;=\; \sum_{P \in \mathcal{P}_i} |(T) \cap (P)|$$

Ako je $i \neq i'$ točke P i T pripadaju različitim blokovima particije, pa su različite. Tada ih spaja točno λ pravaca, tj. $|(T) \cap (P)| = \lambda$. Vidimo da je u ovom slučaju $\sum\limits_{j=1}^{n} a_{i'j} b_{ij} = \sum\limits_{P \in \mathcal{P}_i} \lambda = \lambda\nu_i$.

Ako je $i = i'$ točke P i T mogu biti jednake. Vrijedi

$$|(T) \cap (P)| \;=\; \begin{cases} r, & \text{ako je } T = P \\ \lambda, & \text{ako je } T \neq P \end{cases}$$

Iz toga slijedi $\sum_{j=1}^{n} a_{i'j} b_{ij} = r + \sum_{P \in \mathcal{P}_i \setminus \{T\}} \lambda = \lambda(\nu_i - 1) + r.$ ■

Propozicija 5.6 *Matrica $A = [a_{ij}]$ ima svojstva:*

(1) $0 \leq a_{ij} \leq \beta_j, \quad za\ 1 \leq i \leq m,\ 1 \leq j \leq n$

(2) $\displaystyle\sum_{j=1}^{n} a_{ij} = r, \quad za\ 1 \leq i \leq m$

(3) $\displaystyle\sum_{i=1}^{m} \frac{\nu_i}{\beta_j}\, a_{ij} = k, \quad za\ 1 \leq j \leq n$

(4) $\displaystyle\sum_{j=1}^{n} \frac{\nu_i}{\beta_j}\, a_{ij} a_{i'j} = \begin{cases} \lambda\nu_i, & ako\ je\ i \neq i' \\ \lambda(\nu_i - 1) + r, & ako\ je\ i = i' \end{cases}, \quad za\ 1 \leq i, i' \leq m$

Dokaz. Svojstvo (1) slijedi direktno iz definicije brojeva a_{ij}, a svojstvo (2) dokazali smo u lemi 5.3. Svojstvo (3) slijedi iz lema 5.3 i 5.4, a svojstvo (4) iz lema 5.4 i 5.5. ■

Slično dokazujemo svojstva matrice B.

Propozicija 5.7 *Matrica $B = [b_{ij}]$ ima svojstva:*

(1) $0 \leq b_{ij} \leq \nu_i, \quad za\ 1 \leq i \leq m,\ 1 \leq j \leq n$

(2) $\displaystyle\sum_{i=1}^{m} b_{ij} = k, \quad za\ 1 \leq j \leq n$

(3) $\displaystyle\sum_{j=1}^{n} \frac{\beta_j}{\nu_i}\, b_{ij} = r, \quad za\ 1 \leq i \leq m$

(4) $\displaystyle\sum_{j=1}^{n} \frac{\beta_j}{\nu_{i'}}\, b_{ij} b_{i'j} = \begin{cases} \lambda\nu_i, & ako\ je\ i \neq i' \\ \lambda(\nu_i - 1) + r, & ako\ je\ i = i' \end{cases}, \quad za\ 1 \leq i, i' \leq m$

Definicija 5.8 *Svaku matricu* $A = [a_{ij}] \in M_{mn}(\mathbb{N}_0)$ *koja ima svojstva iz propozicije 5.6 zovemo* **orbitna struktura** (*ili* **matrica taktičke dekompozicije**) (v, k, λ) *dizajna obzirom na marginalne vektore* ν, β.

Napomena 5.9 Točnije bi bilo matricu A zvati *točkovna orbitna struktura*, a matricu B *pravčasta orbitna struktura*. U ovom radu za konstrukciju dizajna koristimo isključivo točkovne orbitne strukture.

Postupak za konstrukciju (v, k, λ) dizajna s grupom automorfizama G sastoji se od dva koraka.

1. Pronalaženje svih orbitnih struktura, do na izomorfizam. Izomorfizam orbitnih struktura je permutacija redaka i stupaca koja čuva marginalne vektore. Koristimo algoritam za klasifikaciju, kao što je opisano u 3.27.

2. Indeksiranje orbitnih struktura. Unose u orbitnoj strukturi zamjenjujemo na sve moguće načine odgovarajućim $0-1$ matricama, tako da dobijemo incidencijsku matricu (v, k, λ) dizajna. Unos a_{ij} zamjenjujemo $0-1$ matricom dimenzije $\nu_i \times \beta_j$. Matrica ima a_{ij} jedinica u svakom retku i invarijantna je obzirom na djelovanje grupe G.

Ako postupak indeksiranja primjenimo na sve orbitne strukture dobit ćemo incidencijske matrice svih (v, k, λ) dizajna s grupom automorfizama G.

Treba naglasiti da osim strukture grupe G moramo znati način na koji ona djeluje na točke i pravce dizajna. Najteži dio posla upravo je odabir prikladne grupe i konzistentnog djelovanja. U ovom radu bavimo se isključivo konstrukcijom $S(k, 2k^2-2k+1)$ dizajna s cikličkim grupama prostog reda $\mathbb{Z}_p$. U tom slučaju orbite su duljine 1 ili p, jer $\mathbb{Z}_p$ nema pravih podgrupa. Stoga su marginalni vektori jedinstveno određeni brojem fiksnih točaka i pravaca. U idućem odjeljku bavimo se fiksnim strukturama automorfizma prostog reda.

Problem indeksiranja rješavamo programom `index1`. Program radi za sve $(v, k, 1)$ dizajne, uz ograničenje da je grupa G ciklička, a duljine orbita (unosi u marginalnim vektorima) samo 1 i p. Incidencijske matrice dobivene indeksiranjem mogu biti izomorfne. Na kraju konstrukcije koristimo algoritam 3.16, odnosno program `incfilter` za prebrojavanje neizomorfnih dizajna.

5.2 Automorfizmi prostog reda

Lema 5.10 *Neka je* α *automorfizam Steinerovog 2-dizajna. Ako* α *fiksira dvije točke, njihova je spojnica fiksni pravac. Ako* α *fiksira dva pravca koji se sijeku, njihov je presjek fiksna točka.*

Dokaz. Neka su T_1 i T_2 fiksne točke, a ℓ njihova spojnica. Pravac $\alpha\,\ell$ prolazi kroz točke $\alpha\,T_1 = T_1$ i $\alpha\,T_2 = T_2$, pa se podudara s ℓ. Dakle, $\ell = \alpha\,\ell$ je fiksni pravac. Druga tvrdnja dokazuje se analogno. ■

Lema 5.11 *Neka je α automorfizam prostog reda $p \geq k-1$ Steinerovog 2-dizajna $S(k,v)$. Ako α fiksira dvije točke, sve točke na njihovoj spojnici su fiksne.*

Dokaz. Budući da je p prost broj, duljine α-orbita mogu biti samo 1 i p. Prema lemi 5.10 spojnica ℓ dvije fiksne točke je fiksni pravac. Skup točaka koje leže na ℓ podijeljen je na α-orbite, među kojima su dvije duljine 1. Preostalih $k-2$ točaka ne mogu tvoriti orbitu duljine p, pa su i one fiksne. ■

Propozicija 5.12 *Neka Steinerov 2-dizajn $S(k,v)$ ima automorfizam α prostog reda $p \geq k-1$. Skup fiksnih točaka od α može biti:*

(a) *prazan skup*

(b) *jednočlan skup*

(c) *skup od k kolinearnih točaka*

(d) *skup točaka pravog poddizajna $S(k,v')$*

Dokaz. Pretpostavimo da postoje bar dvije fiksne točke, tj. da ne nastupaju slučajevi (a) i (b). Prema lemi 5.11 sve točke na njihovoj spojnici su fiksne. Ako su to jedine fiksne točke nastupa slučaj (c). Ako postoje i fiksne točke izvan tog pravca, skup svih fiksnih točaka i njihovih spojnica tvori poddizajn $S(k,v')$. Tada nastupa slučaj (d). ■

Korolar 5.13 *Neka Steinerov 2-dizajn $S(k, 2k^2-2k+1)$ ima automorfizam α prostog reda $p \geq k-1$. Skup fiksnih točaka od α može biti:*

(a) *prazan skup*

(b) *jednočlan skup*

(c) *skup od k kolinearnih točaka*

Dokaz. Za $v = 2k^2-2k+1$ slučaj (d) iz prethodne propozicije nije moguć, zbog propozicije 2.5.

■

Propozicija 5.14 *Neka Steinerov 2-dizajn $S(k, 2k^2-2k+1)$ ima automorfizam α prostog reda $p > k$. Fiksna struktura od α može biti:*

(a) *Prazan skup.*

(b) *Skup od k kolinearnih točaka i pravac na kojem leže.*

Prvi slučaj nastupa ako i samo ako p dijeli $v = 2k^2 - 2k + 1$, a drugi slučaj ako i samo ako je $p = 2k - 1$.

Dokaz. Za automorfizam reda $p > k$ otpada slučaj (b) iz korolara 5.13. Naime, p ne dijeli $v - 1 = 2k(k - 1)$, jer bi iz toga slijedilo $p \mid k - 1$ ili $p \mid k$. Dakle, α nema fiksnih točaka ili ima k kolinearnih fiksnih točaka. U prvom slučaju nema ni fiksnih pravaca (točke na njima bile bi fiksne). Iz istog razloga u drugom slučaju jedino je pravac na kojem leže sve fiksne točke fiksan.

U slučaju (a) jasno je da p dijeli $v = 2k^2 - 2k + 1$, jer su točke podijeljene na α-orbite duljine p. U slučaju (b) promotrimo pramen pravaca kroz jednu od fiksnih točaka. Jedan od njih je fiksan, a preostalih $r-1 = 2k-1$ pravaca podijeljeni su na orbite duljine p. Zato p dijeli $2k - 1$, a zbog $p > k$ iz toga slijedi $p = 2k - 1$. Obrat vrijedi jer $2k - 1$ ne dijeli $v = (2k - 1)(k - 1) + k$. Ako p dijeli v nastupa slučaj (a), a ako je $p = 2k - 1$ nastupa slučaj (b).

■

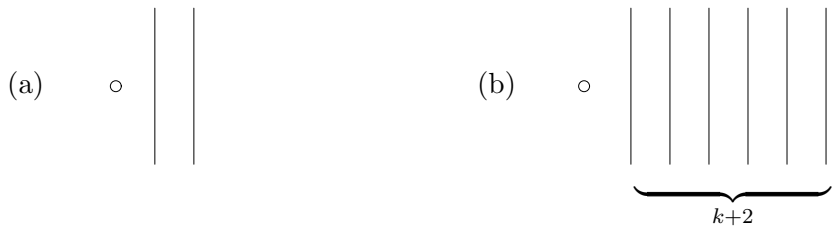
Primjer 5.15 Automorfizmi iz prethodne propozicije zaista su mogući. Na primjer, dizajn $S3.1$ ima automorfizam tipa (a) (reda 13), a dizajn $S4.1$ automorfizam tipa (b) (reda 7).

Korolar 5.16 *Ako Steinerov 2-dizajn $S(k, 2k^2 - 2k + 1)$ ima automorfizam prostog reda $p > k$, onda je $p = 2k - 1$ ili p dijeli $v = 2k^2 - 2k + 1$.*

Propozicija 5.17 *Neka Steinerov 2-dizajn $S(k, 2k^2-2k+1)$ ima automorfizam α prostog reda $p = k$. Fiksna struktura od α može biti:*

(a) *Jedna točka i dva paralelna pravca koja ne prolaze kroz fiksnu točku.*

(b) *Jedna točka i $k+2$ međusobno paralelnih pravaca koji ne prolaze kroz fiksnu točku.*



Slika 8: Fiksne strukture automorfizma reda $p = k$.

Dokaz. Broj $p = k$ ne dijeli $v = 2(k-1)k+1$ i $v-k = (2k-3)k+1$, pa automorfizam α ne može imati 0 ili k fiksnih točaka. Preostaje mogućnost (b) iz korolara 5.13, da α ima jedinstvenu fiksnu točku T. Kad bi na fiksnom pravcu ležala fiksna točka, sve bi točke na tom pravcu bile fiksne. Zato su fiksni pravci međusobno paralelni i ne prolaze kroz T.

Fiksnih pravaca nema više od $\frac{v-1}{k} = 2k-2$. Skup pravaca podijeljen je na α-orbite duljine 1 i p, pa je broj fiksnih pravaca (orbita duljine 1) kongruentan modulo p ukupnom broju pravaca $b = 4(k-1)k+2 \equiv 2 \pmod{p}$. Vidimo da fiksnih pravaca može biti 2 ili $k+2$. ■

Primjer 5.18 Automorfizam tipa (a) javlja se kod dizajna $S3.1$ i kod četiri $S(5, 41)$ dizajna (teorem 5.31). Niti jedan od poznatih $S(k, 2k^2-2k+1)$ dizajna nema automorfizam tipa (b). Najmanji k za koji je takav automorfizam možda moguć je $k = 7$ (vidi 5.40).

Propozicija 5.19 *Neka Steinerov 2-dizajn $S(k, 2k^2-2k+1)$ ima automorfizam α prostog reda $p = k-1$. Fiksna struktura od α može biti:*

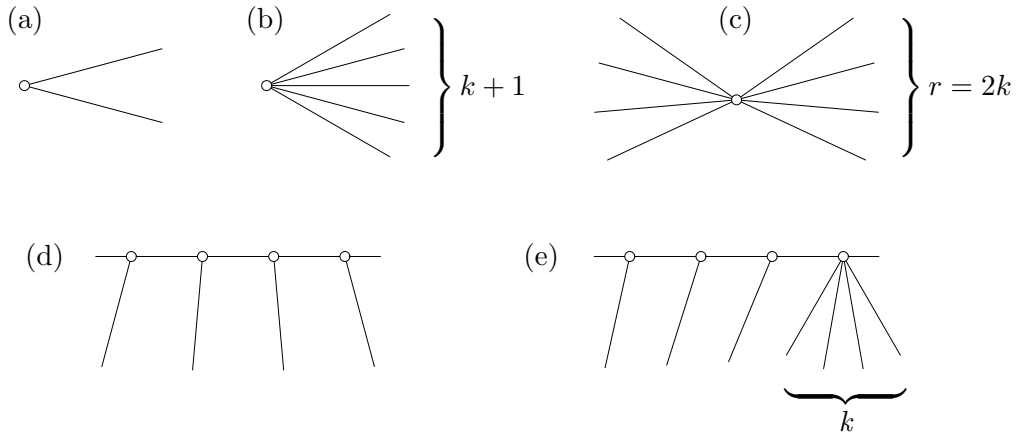
(a) *Jedna točka i dva pravca kroz nju.*

(b) *Jedna točka i $k+1$ pravaca kroz nju.*

(c) *Jedna točka i svi pravci kroz nju.*

(d) *Skup od k točaka jednog pravca, taj pravac i kroz svaku točku još po jedan pravac.*

(e) *Skup od k točaka jednog pravca i taj pravac. Dodatnih k pravaca kroz jednu od točaka, a po jedan dodatni pravac kroz preostale točke.*



Slika 9: Fiksne strukture automorfizma reda $p = k - 1$.

Dokaz. Automorfizam α mora imati bar jednu fiksnu točku, jer $p = k-1$ ne dijeli $v = 2k(k-1)+1$. Prema korolaru 5.13 fiksnih točaka ima 1 ili k.

Pretpostavimo da α fiksira jedinstvenu točku T. Na svakom fiksnom pravcu leži bar jedna fiksna točka, pa svi fiksni pravci prolaze kroz T. Pramen pravaca kroz T podijeljen je na α-orbite duljine 1 i $p = k-1$. Zaključujemo da je broj fiksnih pravaca 2, $k+1$ ili $r = 2k$, tj. fiksna struktura od α je oblika (a), (b) ili (c).

Ako α fiksira k točaka, one leže na nekom pravcu ℓ. Kao i u prvom slučaju, fiksni pravci sadrže bar jednu fiksnu točku, a fiksne točke leže na 2, $k+1$ ili $r = 2k$ fiksnih pravaca. Vidimo da kroz svaku fiksnu točku prolazi osim ℓ bar još jedan fiksni pravac. Dva takva pravca (kroz dvije različite točke na ℓ) moraju biti disjunktni, jer bi njihovo sjecište bila fiksna točka izvan ℓ (lema 5.10). Zato nije moguće da su svi pravci kroz neku od fiksnih točaka fiksni. Iz istog razloga najviše kroz jednu fiksnu točku prolazi $k+1$ fiksnih pravaca. Preostaju dvije mogućnosti: kroz svaku fiksnu točku osim ℓ prolazi još jedan fiksni pravac (slučaj (d)), ili kroz jednu od njih prolazi ℓ i još k fiksnih pravaca, a kroz ostale ℓ i još jedan fiksni pravac (slučaj (e)). Time su opisane sve moguće fiksne strukture od α. ■

Primjer 5.20 Svih pet slučajeva iz prethodne propozicije javljaju se kod Steinerovih 2-dizajna $S(4, 25)$. Dizajn $S4.5$ ima automorfizme reda 3 tipa (a), (b), (d) i (e), a dizajn $S4.1$ automorfizam tipa (c) (teorem 5.25).

Automorfizmi reda $p < k-1$ mogu fiksirati i više od k točaka dizajna $S(k, 2k^2-2k+1)$. Za njih nemamo općenite rezultate o fiksnim strukturama, nego samo za konkretne parametre (propozicije 5.26 i 5.32).

5.3 Konstrukcija $S(4, 25)$ dizajna

Rezultati o grupama automorfizama Steinerovih 2-dizajna $S(4, 25)$ trivijalno slijede iz Spenceove potpune klasifikacije i podataka sabranih u tablici 1. Ovdje ih ipak dokazujemo Jankovom metodom, radi provjere programa kojima vršimo konstrukciju.

Propozicija 5.21 *Ako Steinerov 2-dizajn $S(4, 25)$ ima automorfizam prostog reda p, onda je $p \in \{2, 3, 5, 7\}$.*

Dokaz. Prema korolaru 5.16 jedini kandidati veći od $k = 4$ su $p = 2k-1 = 7$ i prosti faktori od $v = 25$, tj. $p = 5$. Dozvoljeni su i prosti brojevi $p \leq k$, u ovom slučaju 2 i 3. ■

Teorem 5.22 *Postoje točno tri Steinerova 2-dizajna $S(4, 25)$ s automorfizmom reda 7. To su S4.1, S4.3 i S4.4.*

Dokaz. Prema propoziciji 5.14 automorfizam reda 7 fiksira jedan pravac i točke na njemu. Stoga su marginalni vektori $\nu = (1, 1, 1, 1, 7, 7, 7)$ i $\beta = (1, 7, 7, 7, 7, 7, 7, 7)$. Pripadne orbitne strukture konstruiramo algoritmom 3.22, kao što je opisano u 3.27. Dobivamo samo jednu orbitnu strukturu:

	1	7	7	7	7	7	7	7
1	1	7	0	0	0	0	0	0
1	1	0	7	0	0	0	0	0
1	1	0	0	7	0	0	0	0
1	1	0	0	0	7	0	0	0
7	0	1	1	1	1	3	1	0
7	0	1	1	1	1	1	0	3
7	0	1	1	1	1	0	3	1

Indeksiranjem dobivamo niz incidencijskih matrica za $S(4, 25)$. Pomoću programa `incfilter` vidimo da su među njima tri neizomorfne i da pripadaju dizajnima S4.1, S4.3 i S4.4. ■

Prema [8] i [9], prethodni teorem dokazali su 1980. godine A.E.Brouwer i V.D.Tonchev, neovisno jedan o drugom.

Napomena 5.23 Proračuni opisani u dokazu teorema 5.22 realiziraju se pozivanjem odgovarajućih programa (`t-1` i `canonfilter` za klasifikaciju orbitnih struktura, `index1` za indeksiranje i `incfilter` za eliminiranje izomorfnih dizajna). Cijeli je postupak automatiziran shell-skriptom `p7`. I ostali "kompjuterski" dokazi u ovom poglavlju popraćeni su shell-skriptama, pohranjenim na priloženom CD-u. Svi rezultati i međurezultati također su pohranjeni na CD-u. Radi se o velikoj količini podataka koju ne bi bilo praktično u cijelosti reproducirati na papiru.

Teorem 5.24 *Postoji jedinstveni Steinerov* 2*-dizajn* $S(4, 25)$ *s automorfizmom reda* 5*,* $S4.2$*.*

Dokaz. Prema 5.14 automorfizam reda 5 nema fiksnih elemenata. Algoritmom za klasifikaciju dobivamo šest orbitnih struktura, od kojih je dvije moguće indeksirati. Sve dobivene incidencijske matrice izomorfne su incidencijskoj matrici dizajna $S4.2$.

■

Dizajn $S4.2$ konstruirao je R.C.Bose još 1939, pomoću diferencijske familije (vidi primjer 4.25). Brouwer i Tonchev su 1980. dokazali da je to jedini $S(4, 25)$ s automorfizmom reda 5.

Teorem 5.25 *Postoji točno šesnaest Steinerovih* 2*-dizajna* $S(4, 25)$ *s automorfizmom reda* 3*. To su* $S4.1, \ldots, S4.16$*.*

Dokaz. Propozicija 5.19 ostavlja pet mogućnosti za fiksnu strukturu automorfizma reda 3.

(a) Jedna točka i dva pravca kroz nju. Kanonske orbitne strukture su sljedećeg oblika:

```
    1 1 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
  ┌─────────────────────────────────────┐
1 │ 1 1 3 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 │
3 │ 1 0 . . . . . . . . . . . . . . . . │
3 │ 0 1 . . . . . . . . . . . . . . . . │
3 │ 0 0 . . . . . . . . . . . . . . . . │
3 │ 0 0 . . . . . . . . . . . . . . . . │
3 │ 0 0 . . . . . . . . . . . . . . . . │
3 │ 0 0 . . . . . . . . . . . . . . . . │
3 │ 0 0 . . . . . . . . . . . . . . . . │
3 │ 0 0 . . . . . . . . . . . . . . . . │
  └─────────────────────────────────────┘
```

Nepoznati dio nadopunjuje se algoritmom 3.22 na 91 bitno različitih načina. Točan redoslijed pozivanja programa `t-1` i `canonfilter` vidljiv je iz shell-skripte `p3a`. Od ukupno 91 orbitnih struktura moguće je indeksirati njih 10, pri čemu dobivamo 13 neizomorfnih incidencijskih matrica. One pripadaju dizajnima $S4.1$, $S4.2$, $S4.3$, $S4.5$, $S4.6$, $S4.7$, $S4.8$, $S4.9$, $S4.10$, $S4.11$, $S4.12$, $S4.15$ i $S4.16$.

(b) Jedna točka i pet pravaca kroz nju. Kanonske orbitne strukture su oblika:

```
    1 1 1 1 1 3 3 3 3 3 3 3 3 3 3 3 3 3 3
  ┌─────────────────────────────────────────┐
1 │ 1 1 1 1 1 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 │
3 │ 1 0 0 0 0 . . . . . . . . . . . . . . . │
3 │ 0 1 0 0 0 . . . . . . . . . . . . . . . │
3 │ 0 0 1 0 0 . . . . . . . . . . . . . . . │
3 │ 0 0 0 1 0 . . . . . . . . . . . . . . . │
3 │ 0 0 0 0 1 . . . . . . . . . . . . . . . │
3 │ 0 0 0 0 0 . . . . . . . . . . . . . . . │
3 │ 0 0 0 0 0 . . . . . . . . . . . . . . . │
3 │ 0 0 0 0 0 . . . . . . . . . . . . . . . │
  └─────────────────────────────────────────┘
```

Algoritmom za klasifikaciju dobivamo 8 neizomorfnih orbitnih struktura. Indeksiraju se njih 3 i pritom dobivamo dizajne $S4.5$, $S4.6$ i $S4.7$.

(c) Jedna točka i svih osam pravaca kroz nju. U ovom slučaju postoje 4 orbitne strukture, kojima je kanonski oblik:

	1	1	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.
3	0	1	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	1	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.

Dvije orbitne strukture mogu se indeksirati, što daje dizajne $S4.1$ i $S4.3$.

(d) Točke jednog pravca, taj pravac i još po jedan pravac kroz svaku točku. Vidimo da kanonske orbitne strukture imaju oblik:

	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	1	1	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	1	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0
1	1	0	0	0	1	0	0	0	0	0	0	3	3	0	0	0	0	0	0	0
3	0	1	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Dobivamo 9 orbitnih struktura. Četiri je moguće indeksirati, što daje incidencijske matrice dizajna $S4.1$, $S4.3$, $S4.4$, $S4.5$, $S4.6$, $S4.7$, $S4.13$ i $S4.14$.

(e) Uz točke i pravce iz slučaja (d), automorfizam fiksira još 3 pravca kroz jednu od fiksnih točaka. Postoje dvije orbitne strukture, sljedećeg kanonskog oblika:

	1	1	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3
1	1	1	1	1	1	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	1	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	1	0	0	0	0	3	3	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	1	0	0	0	0	0	3	3	0	0	0	0	0	0
3	0	1	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	1	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.

Obje je moguće indeksirati. Dobivamo dizajne $S4.5$, $S4.6$ i $S4.7$.

Vidimo da smo dobili svih 16 dizajna $S(4, 25)$ s netrivijalnom grupom automorfizama.

■

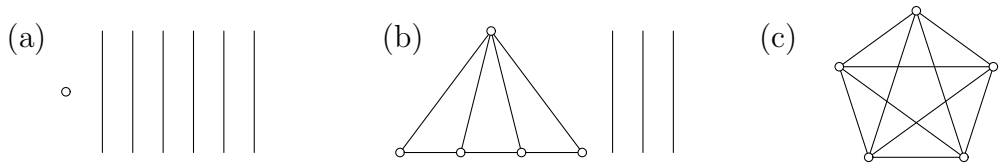
Prethodni teorem dokazali su Kramer, Magliveras i Mathon u [8]. Naš se dokaz u potpunosti slaže s njihovim, uključujući međurezultate (broj orbitnih struktura u pojedinim slučajevima i indeksiranje). U istom članku može se naći dokaz sljedeće tvrdnje.

Propozicija 5.26 *Neka Steinerov 2-dizajn $S(4, 25)$ ima involutorni automorfizam α. Fiksna struktura od α može biti:*

(a) *Jedna točka i šest međusobno paralelnih pravaca koji ne prolaze kroz fiksnu točku.*

(b) *Četiri kolinearne točke i još jedna točka, te njihove spojnice. Dodatna tri međusobno paralelna pravca koji ne sijeku tu konfiguraciju.*

(c) *Pet točaka i deset pravaca koji čine potpuni peterovrh, tj. konfiguraciju $(5_4, 10_2)$.*



Slika 10: Fiksne strukture automorfizma reda 2 za $S(4, 25)$.

Teorem 5.27 *Postoje točno tri Steinerova 2-dizajna $S(4, 25)$ s automorfizmom reda 2. To su S4.1, S4.2 i S4.8.*

Dokaz. Predhodna propozicija ostavlja tri mogućnosti za fiksnu strukturu involutornog automorfizma.

(a) Jedna točka, šest pravaca. Kanonske orbitne strukture su sljedećeg oblika:

	1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
1	0 0 0 0 0 0 2 2 2 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
2	1 0 0 0 0 0 . . . . .
2	1 0 0 0 0 0 . . . . .
2	0 1 0 0 0 0 . . . . .
2	0 1 0 0 0 0 . . . . .
2	0 0 1 0 0 0 . . . . .
2	0 0 1 0 0 0 . . . . .
2	0 0 0 1 0 0 . . . . .
2	0 0 0 1 0 0 . . . . .
2	0 0 0 0 1 0 . . . . .
2	0 0 0 0 1 0 . . . . .
2	0 0 0 0 0 1 . . . . .
2	0 0 0 0 0 1 . . . . .

Algoritmom za klasifikaciju pronalazimo ukupno 65 orbitnih struktura, do na izomorfizam. Samo jednu je moguće indeksirati, pri čemu dobivamo dizajn *S*4.1.

(b) Pet točaka, osam pravaca. Kanonski oblik orbitnih struktura je:

	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	1	0	0	0	0	0	2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	1	0	0	0	0	0	0	0	0	2	2	2	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	2	2	2	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	0	0	0	0	0	0
2	1	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	1	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	1	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	1	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Postoje tri takve orbitne strukture, ali ih nije moguće indeksirati.

(c) Pet točaka, deset pravaca. Kanonske orbitne strukture su oblika:

	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	1	1	1	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	1	0	0	1	1	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0
2	1	0	0	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	1	0	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	1	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	1	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	1	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	1	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	1	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	0	0	0	0	0	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Ima ih 31, od čega je dvije moguće indeksirati. Dobivamo dizajne $S4.2$ i $S4.8$.

Sveukupno smo dobili tri dizajna, $S4.1$, $S4.2$ i $S4.8$. ■

Napomena 5.28 U članku [8] navodi se da orbitnih struktura tipa (c) ima 45. Razlika je u tome što Kramer, Magliveras i Mathon konstruiraju samo nefiksni dio orbitne strukture. U slučaju (c) nefiksni dio ekvivalentan je incidencijskoj matrici parcijalno balansiranog dizajna s parametrima $2-(10, \{3, 4\}, 2)$. Takvih matrica zaista ima 45, ali samo je 31 moguće "obrubiti" do pune orbitne strukture. Ostali detalji dokaza slažu se s člankom [8].

Konstruirali smo sve Steinerove 2-dizajne $S(4, 25)$ s netrivijalnom grupom automorfizama. Prelazimo na dizajne $S(5, 41)$.

5.4 Konstrukcija $S(5, 41)$ dizajna

Propozicija 5.29 *Ako Steinerov 2-dizajn $S(5, 41)$ ima automorfizam prostog reda p, onda je $p \in \{2, 3, 5, 41\}$.*

Dokaz. Prosti brojevi $p \leq 5$ su 2, 3 i 5. Po korolaru 5.16 jedini kandidati $p > 5$ su $2k - 1 = 9$, što nije prost broj i prosti faktori od $v = 41$, dakle $p = 41$. ■

Teorem 5.30 *Postoji jedinstveni Steinerov 2-dizajn $S(5, 41)$ s automorfizmom reda 41, $S5.1$.*

Dokaz. Automorfizam reda 41 djeluje regularno na točke dizajna (propozicija 5.14). U teoremu 4.15 vidjeli smo da postoji točno jedan takav dizajn. ■

Teorem 5.31 *Postoje točno četiri Steinerova 2-dizajna $S(5, 41)$ s automorfizmom reda 5. To su $S5.1$, $S5.2$, $S5.3$ i $S5.6$.*

Dokaz. Prema propoziciji 5.17 imamo dvije mogućnosti za fiksnu strukturu.

(a) Jedna točka i dva pravca. Kanonske orbitne strukture su oblika:

	1	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
1	0	0	5	5	0	0	0	0	0	0	0	0	0	0	0	0	0
5	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Algoritmom 3.22 dobivamo čak 2277 orbitnih struktura, ali samo je dvije moguće indeksirati. Indeksiranjem jedne od njih dobivamo incidencijsku matricu dizajna $S5.1$, a indeksiranjem druge dizajne $S5.2$, $S5.3$ i $S5.6$.

(b) Jedna točka i sedam pravaca. Kanonske orbitne strukture imale bi oblik:

	1	1	1	1	1	1	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5
1	0	0	0	0	0	0	0	5	5	0	0	0	0	0	0	0	0	0	0	0	0
5	1	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	1	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	1	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	0	1	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Pomoću algoritma za klasifikaciju vidimo da ne postoje takve orbitne strukture.

■

Prethodni teorem dokazali su R.Mathon i A.Rosa. Osim spomenuta četiri dizajna konstruirali su dizajn $S5.4$, transformacijom opisanom na stranici 18 ovog rada. U knjizi *The CRC Handbook of Combinatorial Designs* [4] tih pet dizajna navode se kao jedini poznati primjeri za $S(5, 41)$. Prelazimo na klasifikaciju $S(5, 41)$ dizajna s automorfizmom reda 3. Tri od pet poznatih

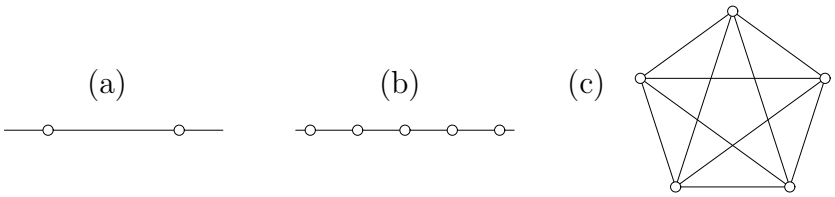
primjera posjeduju automorfizam reda 3. Osim njih dobit ćemo još devet novih $S(5, 41)$ dizajna.

Propozicija 5.32 *Neka Steinerov 2-dizajn $S(5, 41)$ ima automorfizam α reda 3. Fiksna struktura od α može biti:*

(a) *Dvije točke i njihova spojnica.*

(b) *Pet točaka jednog pravca i taj pravac.*

(c) *Pet točaka i deset pravaca koji čine potpuni peterovrh, tj. konfiguraciju $(5_4, 10_2)$.*



Slika 11: Fiksne strukture automorfizma reda 3 za $S(5, 41)$.

Dokaz. Označimo s f broj fiksnih točaka, a s g broj fiksnih pravaca od α. Neka je b_i broj pravaca koji sadrže točno i fiksnih točaka, za $i = 0, \ldots, 5$. Ako pravac sadrži tri fiksne točke, sve točke na njemu su fiksne, pa je $b_3 = b_4 = 0$.

Prema lemi 5.10 pravac koji sadrži dvije fiksne točke je fiksan. U ovom slučaju vrijedi i obrat: svaki fiksni pravac sadrži bar dvije fiksne točke, zbog $k \equiv 2 \pmod 3$. Vidimo da je ukupni broj fiksnih pravaca $g = b_2 + b_5$.

Označimo li broj orbita duljine 3 na točkama s p, a na pravcima s q, slijedi

$$f + 3p = 41 \quad \Longrightarrow \quad f = 41 - 3p \tag{1}$$

$$g + 3q = 82 \quad \Longrightarrow \quad b_2 + b_5 = 82 - 3q \tag{2}$$

Dvostrukim prebrojavanjem dvočlanih skupova fiksnih točaka dobivamo jednadžbu

$$\binom{f}{2} = \binom{2}{2} b_2 + \binom{5}{2} b_5$$

Uvrštavanjem (1) slijedi

$$b_2 + 10b_5 = \frac{(41 - 3p)(40 - 3p)}{2} \tag{3}$$

Rješavanjem jednadžbi (2) i (3) po b_2 i b_5 dobivamo

$$\begin{aligned} b_2 &= \frac{p(27-p)}{2} - \frac{10q}{3} \\ b_5 &= 82 - \frac{p(27-p)}{2} + \frac{q}{3} \end{aligned}$$

Vidimo da q mora biti djeljiv s 3, recimo $q = 3r$. Prebrojavanjem dvočlanih skupova nefiksnih točaka slijedi

$$\binom{41-f}{2} = \binom{5}{2}b_0 + \binom{4}{2}b_1 + \binom{3}{2}b_2$$

Uvrštavanjem (1) to prelazi u

$$10b_0 + 6b_1 + 3b_2 = \frac{3p(3p-1)}{2} \tag{4}$$

Osim toga znamo da je

$$b_0 + b_1 + b_2 + b_5 = 82 \tag{5}$$

Rješavanjem jednadžbi (4) i (5) uz uvažavanje već poznatih rezultata za b_2 i b_5 dobivamo:

$$\begin{aligned} b_0 &= \frac{3p(p-7)}{2} - 6r \\ b_1 &= -\frac{3p(p-7)}{2} + 15r \\ b_2 &= \frac{p(27-p)}{2} - 10r \\ b_5 &= 82 - \frac{p(27-p)}{2} + r \end{aligned} \tag{6}$$

p	r	q	b_0	b_1	b_2	b_5	f	g
13	9	27	63	18	1	0	2	1
12	9	27	36	45	0	1	5	1
12	8	24	42	30	10	0	5	10
11	8	24	18	54	8	2	8	10

Tablica 9: Rješenja sustava (6).

Orbita duljine 3 na točkama nema više od 13, a na pravcima od 27, tj. $1 \leq p \leq 13$, $1 \leq r \leq 9$. Uz te uvjete sustav (6) ima točno 16 rješenja

$b_0, b_1, b_2, b_5 \in \mathbb{N}_0$. Uočimo da na svakom pravcu koji sadrži dvije fiksne točke leži jedna orbita od tri točke. To nam daje dodatni uvjet $b_2 \leq p$, kojeg zadovoljavaju 4 od 16 rješenja (tablica 9).

Četvrto rješenje ($p = 11$, $r = 8$) nije moguće. Naime, $b_5 = 2$ znači da postoje dva pravca na kojima su sve točke fiksne. To je kontradikcija jer fiksnih točaka ima samo $f = 8$. Očito prva tri rješenja odgovaraju redom slučajevima (a), (b) i (c).

■

Teorem 5.33 *Postoji točno dvanaest Steinerovih 2-dizajna $S(5, 41)$ s automorfizmom reda 3. To su S5.2,...,S5.5 i S5.7,...,S5.14.*

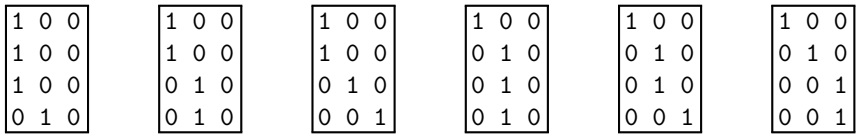
Dokaz. Trebamo ispitati tri slučaja, koji odgovaraju fiksnim strukturama iz prethodne propozicije.

(a) Ako automorfizam fiksira jedan pravac i dvije točke na njemu, kanonske orbitne strukture su oblika:

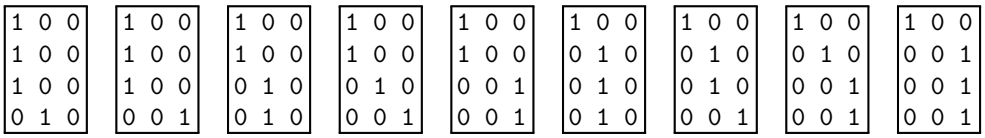
```
    1 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
  ┌─────────────────────────────────────────────────────────┐
1 │ 1 3 3 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 │
1 │ 1 0 0 0 3 3 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 │
1 │ 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 │
3 │ 0 1 0 0 A A A . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 1 0 0 A A A . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 1 0 0 A A A . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 1 0 0 A A A . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 1 0 B B B . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 1 0 B B B . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 1 0 B B B . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 1 0 B B B . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 0 1 C C C . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 0 1 C C C . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 0 1 C C C . . . . . . . . . . . . . . . . . . . . . . │
3 │ 0 0 0 1 C C C . . . . . . . . . . . . . . . . . . . . . . │
  └─────────────────────────────────────────────────────────┘
```

Uzmemo li za $Y^{(m)}$ skup svih orbitnih struktura tog oblika i primijenimo algoritam 3.22, klasifikaciju ne možemo dovesti do kraja jer su skupovi P_l preveliki. Treba nam još informacija o kanonskom obliku.

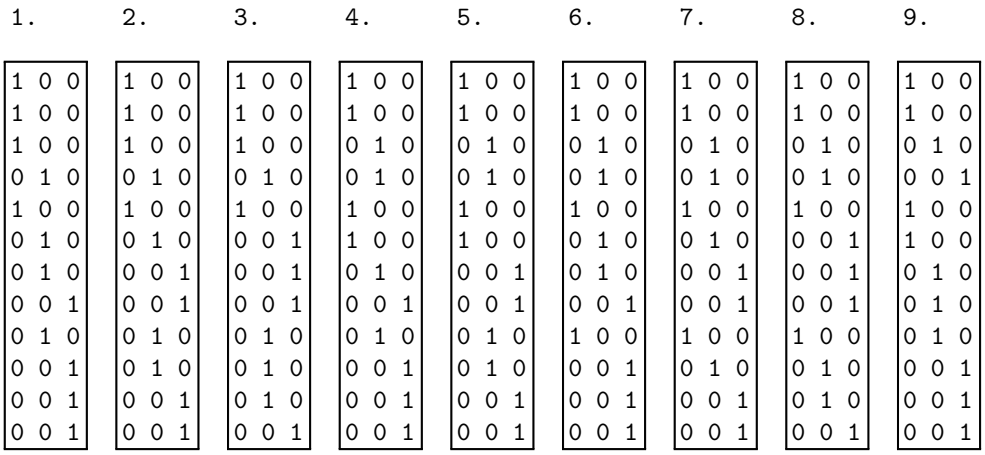
Nepoznati dio matrice u petom, šestom i sedmom stupcu označen je slovima `A`, `B`, `C`. U bloku `A` smijemo permutirati retke, a zatim stupce. Kanonske orbitne strukture imaju na tom mjestu jednu od sljedećih šest matrica:



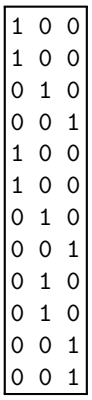
U bloku označenim slovom B smijemo permutirati samo retke. Kandidati za blok A imaju u prvom stupcu jednu, dvije ili tri jedinice. Zato se u prvom stupcu blokova B i C nalazi bar jedna jedinica. Možemo je dovesti u prvi redak bloka B, jer smijemo zamijeniti blokove B i C. Prema tome, u bloku B kanonske orbitne strukture nalazi se jedna od sljedećih devet matrica:



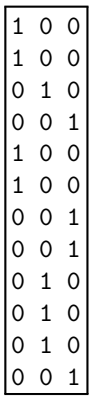
U bloku C smijemo permutirati retke. Ako su poznati blokovi A i B kanonske orbitne strukture, blok C je jednoznačno određen. Kombiniranjem kandidata za blokove A i B dobivamo 36 mogućih blok-stupaca:



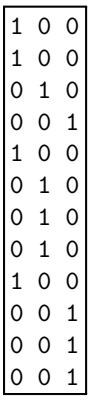
10.



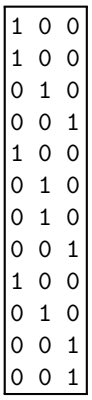
11.



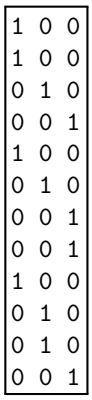
12.



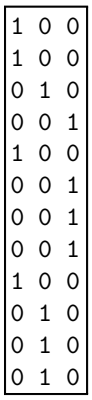
13.



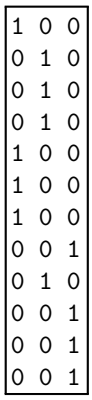
14.



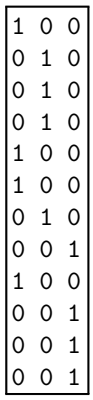
15.



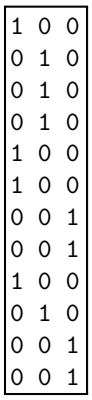
16.



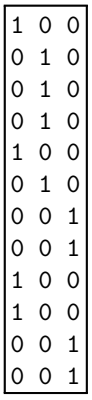
17.



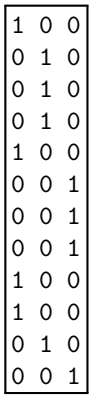
18.



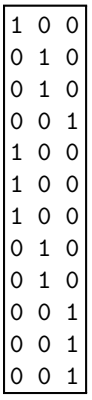
19.



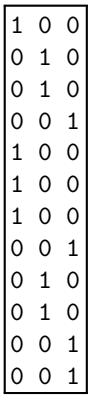
20.



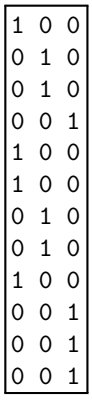
21.



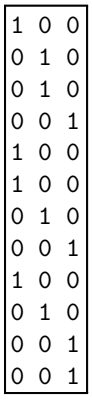
22.



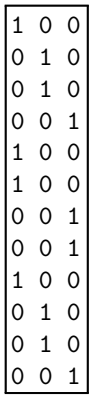
23.



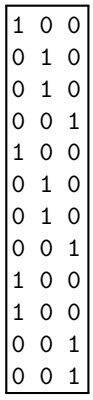
24.



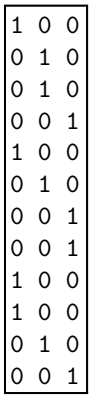
25.



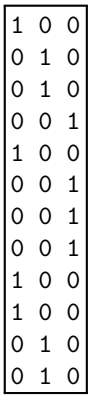
26.



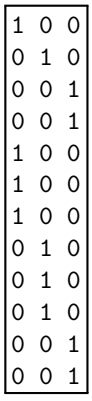
27.



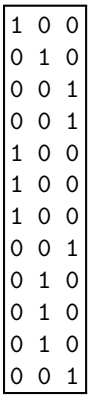
28.



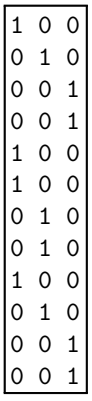
29.



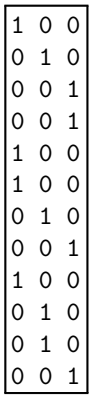
30.



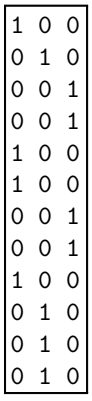
31.



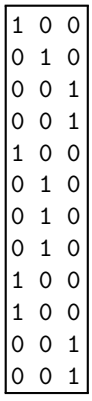
32.



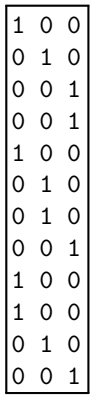
33.



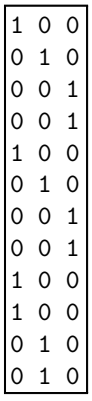
34.



35.



36.



U svakom od 36 slučajeva primjenjujemo algoritam 3.22 do 8. retka. U idućem koraku više se ne isplati izbacivati nekanonske matrice, jer bi za konstrukciju skupa P_9 morali "filtrirati" više matrica nego što ih dobivamo proširivanjem do potpunih orbitnih struktura. Zato parcijalne 8×28 orbitne strukture programom `complete` proširujemo do potpunih orbitnih struktura i tek na kraju izbacujemo nekanonske. Rezultat je sabran u tablici 10. Ukupno dobivamo 47528 neizomorfnih orbitnih struktura, od čega je 12 moguće indeksirati. Dobivamo 10 dizajna: $S5.2$, $S5.3$, $S5.4$, $S5.7$, $S5.8$, $S5.9$, $S5.10$, $S5.11$, $S5.12$ i $S5.14$.

Slučaj	# o.s.	Slučaj	# o.s.	Slučaj	# o.s.	Slučaj	# o.s.
1.	1007	10.	5515	19.	7	28.	5
2.	3695	11.	490	20.	2	29.	2
3.	162	12.	79	21.	3	30.	2
4.	1133	13.	11901	22.	13	31.	38
5.	1153	14.	11963	23.	17	32.	105
6.	615	15.	91	24.	598	33.	5
7.	7179	16.	0	25.	185	34.	9
8.	678	17.	10	26.	52	35.	50
9.	463	18.	8	27.	270	36.	23

Tablica 10: Broj orbitnih struktura za automorfizam tipa (a).

(b) Ako automorfizam fiksira jedan pravac i sve točke na njemu, kanonske orbitne strukture su oblika:

	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	1	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0
3	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	2	1	1	1	0	0	0	0	0	0
3	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Primjenom algoritma 3.22 konstruiramo parcijalne 10×28 orbitne strukture, kojih ima 22956. Proširujemo ih programom `complete` do potpunih i izbacijemo nekanonske (programom `canonfilter`). U ovom slučaju postoji 5 neizomorfnih orbitnih struktura, od kojih je 4 moguće indeksirati. Dobivamo 7 dizajna: $S5.5$, $S5.7$, $S5.8$, $S5.9$, $S5.10$, $S5.12$ i $S5.13$.

(c) Ako automorfizam fiksira potpuni peterovrh, kanonske orbitne strukture su oblika:

	1	1	1	1	1	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	1	1	1	1	0	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	1	1	1	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	1	0	0	1	1	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	1	0	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	1	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	1	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	1	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	1	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	1	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	0	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	0	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	0	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	0	0	0	0	0	0	0	0	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Algoritam 3.22 primjenjujemo do desetog retka. Skup P_{10} sadrži 1907 kanonskih parcijalnih 10×34 orbitnih struktura. Proširujemo ih do kraja i izbacujemo nekanonske. Dobivamo ukupno 1904 orbitnih struktura, ali niti jednu nije moguće indeksirati.

■

Napomena 5.34 U prethodnom dokazu računalno najzahtjevniji dio je klasifikacija orbitnih struktura, pogotovo u slučaju (a). Za obrađivanje tog slučaja bilo je potrebno više mjeseci procesorskog vremena. Postupak indeksiranja je za $p = 3$ brz. Na indeksiranje otpada vrlo mali dio ukupno utrošenog procesorskog vremena, usprkos velikom broju orbitnih struktura koje treba obraditi.

Ostaje otvorena mogućnost postojanja $S(5, 41)$ dizajna čije su pune grupe automorfizama 2-grupe. Involutorni automorfizmi mogu imati sedam različitih fiksnih struktura. U svakom od tih slučajeva orbitne strukture su velike i teško ih je potpuno klasificirati.

5.5 Neki rezultati za $k \geq 6$

Još uvijek je upitno da li dizajni $S(k, 2k^2 - 2k + 1)$ postoje za $k \geq 6$. Na kraju poglavlja sabrali smo niz pokušaja njihove konstrukcije Jankovom metodom. Tvrdnje su formulirane kao rezultati o grupama automorfizama (eventualnih) dizajna $S(6, 61)$, $S(7, 85)$ i $S(8, 113)$.

Propozicija 5.35 *Ako Steinerov 2-dizajn $S(6, 61)$ ima automorfizam prostog reda p, onda je $p \in \{2, 3, 5\}$.*

Dokaz. Korolar 5.16 dopušta još $p = 11$ i $p = 61$. Automorfizam reda 61 djelovao bi regularno na točkama, a vidjeli smo da to nije moguće (teorem 4.15). Automorfizam reda 11 inducirao bi orbitnu strukturu sljedećeg kanonskog oblika:

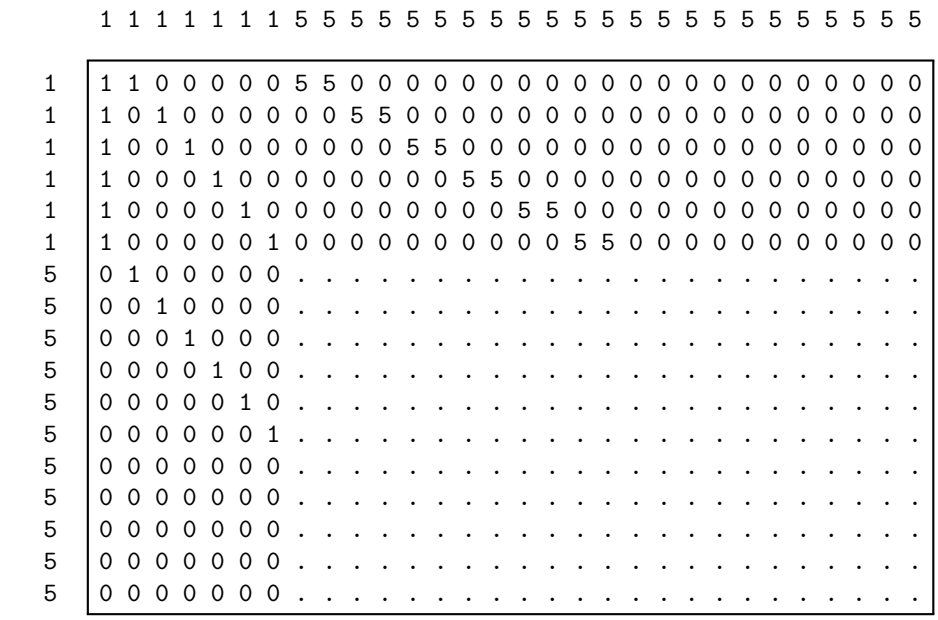
	1	11	11	11	11	11	11	11	11	11	11	11
1	1	11	0	0	0	0	0	0	0	0	0	0
1	1	0	11	0	0	0	0	0	0	0	0	0
1	1	0	0	11	0	0	0	0	0	0	0	0
1	1	0	0	0	11	0	0	0	0	0	0	0
1	1	0	0	0	0	11	0	0	0	0	0	0
1	1	0	0	0	0	0	11	0	0	0	0	0
11	0	.	.	.	.	.	.	.	.	.	.	.
11	0	.	.	.	.	.	.	.	.	.	.	.
11	0	.	.	.	.	.	.	.	.	.	.	.
11	0	.	.	.	.	.	.	.	.	.	.	.
11	0	.	.	.	.	.	.	.	.	.	.	.

Lako se vidi da takve orbitne strukture ne postoje. ■

Propozicija 5.36 *Automorfizam reda 5 Steinerovog 2-dizajna $S(6, 61)$ fiksira jednu točku i dva, sedam ili dvanaest pravaca kroz nju.*

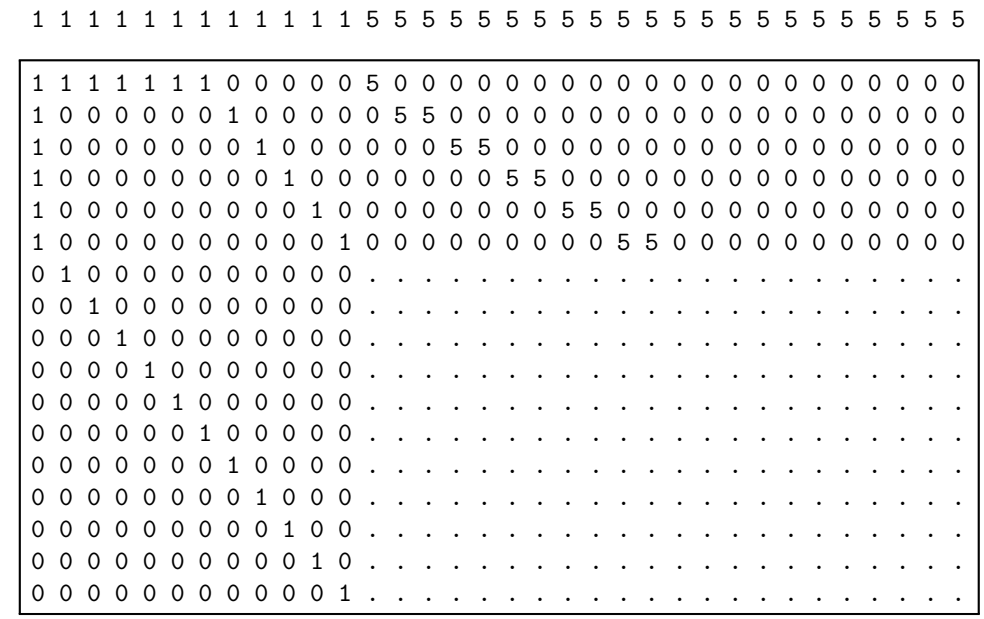
Dokaz. Treba eliminirati slučajeve (d) i (e) iz propozicije 5.19.

(d) Kanonske orbitne strukture su oblika:



Algoritmom 3.22 konstruiramo parcijalne 10×30 orbitne strukture, kojih ima 375. Proširujemo ih do kraja i primjenjujemo `canonfilter`. Postoji 30 potpunih orbitnih struktura. Nije ih moguće indeksirati.

(e) Kanonske orbitne strukture su oblika:



Algoritmom 3.22 dobivamo dvije takve orbitne strukture, koje nije moguće indeksirati.

■

Napomena 5.37 U preostala tri slučaja postoji znatno više orbitnih struktura. Promotrimo slučaj (c) iz propozicije 5.19 (jedna fiksna točka, svi pravci kroz nju fiksni). Nefiksni dio orbitne strukture odgovara incidencijskoj matrici $2-(12,6,5)$ dizajna. Prema *CRC Handbooku* [4] takvih dizajna ima 11603. Indeksiranje jedne orbitne strukture traje nekoliko sati, pa ih ne možemo sve obraditi u razumnom vremenu.

Korolar 5.38 *Ne postoji Steinerov 2-dizajn $S(6,61)$ s grupom automorfizama reda 25.*

Dokaz. Pretpostavimo da postoji $S(6,61)$ s grupom automorfizama G reda 25. Promotrimo djelovanje grupe G na točke dizajna. Ako broj orbita označimo s n, iz Burnsideove leme 1.19 slijedi $25n = \sum_{\alpha\in G} f(\alpha)$. Pritom $f(\alpha)$ označava broj fiksnih točaka automorfizma α. Red elemenata iz G može biti 1 (neutralni element), 5 ili 25. Zbog prethodne propozicije elementi reda 5 fiksiraju jednu točku. Isto vrijedi za automorfizme reda 25, jer su njihove pete potencije reda 5. Slijedi

$$25n \;=\; 61 + \sum_{\alpha\in G\setminus\{id\}} 1 \;=\; 85 \quad\Longrightarrow\quad n = 3.4$$

To je kontradikcija, jer broj orbita mora biti prirodan.

■

Propozicija 5.39 *Ako Steinerov 2-dizajn $S(7,85)$ ima automorfizam prostog reda p, onda je $p \in \{2,3,5,7,17\}$.*

Dokaz. Po korolaru 5.16 dolazi u obzir još jedino $p = 2k-1 = 13$. Orbitna struktura automorfizma reda 13 bila bi oblika:

	1	13	13	13	13	13	13	13	13	13	13	13	13	13
1	1	13	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	13	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	13	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	13	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	13	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	13	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	13	0	0	0	0	0	0
13	0	.	.	.	.	.	.	.	.	.	.	.	.	.
13	0	.	.	.	.	.	.	.	.	.	.	.	.	.
13	0	.	.	.	.	.	.	.	.	.	.	.	.	.
13	0	.	.	.	.	.	.	.	.	.	.	.	.	.
13	0	.	.	.	.	.	.	.	.	.	.	.	.	.
13	0	.	.	.	.	.	.	.	.	.	.	.	.	.

Algoritmom za klasifikaciju brzo vidimo da takve orbitne strukture ne postoje.

■

Napomena 5.40 Automorfizam reda 17 dizajna $S(8, 75)$ djelovao bi bez fiksnih elemenata. Algoritmom 3.22 relativno brzo dobivamo orbitne strukture; ima ih 313. Problem predstavlja njihovo indeksiranje, jer za jednu orbitnu strukturu treba i po nekoliko dana procesorskog vremena. U trenutku predavanja ovog rada obradio sam programom `index1` oko četvrtine od ukupnog broja orbitnih struktura, pri čemu nije dobiven niti jedan dizajn. Najvjerojatnije ne postoje $S(7, 85)$ dizajni s automorfizmom reda 17.

Slučaj $S(7, 85)$ dizajna s automorfizmom reda 7 zaista je preopsežan za potpunu klasifikaciju. Po propoziciji 5.17 takav automorfizam fiksira jednu točku i dva ili devet pravaca. U slučaju (b) postoji više od 100000 neizomorfnih orbitnih struktura, puno više nego što ih možemo indeksirati u prihvatljivom vremenu.

Propozicija 5.41 *Ako Steinerov 2-dizajn $S(8, 113)$ ima automorfizam prostog reda p, onda je $p \in \{2, 3, 5, 7\}$.*

Dokaz. Korolar 5.16 dozvoljava još jedino $p = 113$, ali takav automorfizam nije moguć zbog 4.15.

■

Literatura

[1] R.D.Baker, *An Elliptic Semiplane*, Journal of Combinatorial Theory A, **25** (1978), 193–195

[2] T.Beth, D.Jungnickel, H.Lenz, *Design Theory*, Cambridge University Press, 1993.

[3] M.Buratti, *On Simple Radical Difference Families*, Journal of Combinatorial Designs, **3** (1995), 161–168

[4] C.J.Colbourn, J.H.Dinitz (eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1997.

[5] P.Dembowski, *Finite Geometries*, Springer Verlag, Berlin, 1968.

[6] J.W.DiPaola, *The Structure of the Hyperbolic Planes* $S(2, k, k^2+(k-1)^2)$, Ars Combinatoria, **25** (1988), 77–87

[7] B.W.Kernighan, D.M.Ritchie, *The C Programming Language*, 2nd edition, Prentice Hall, London, 1988.

[8] E.S.Kramer, S.Magliveras, R.Mathon, *The Steiner Systems* $S(2, 4, 25)$ *with Nontrivial Automorphism Group*, Discrete Mathematics, **77** (1989), 137–157

[9] E.S.Kramer, S.Magliveras, V.D.Tonchev, *On the Steiner Systems* $S(2, 4, 25)$ *Invariant under a Group of Order* 9, Annals of Discrete Mathematics, **34** (1987), 307–314

[10] V.Krčadinac, *Klasifikacija konačnih projektivnih ravnina reda* 7 *i* 8, diplomski rad, Matematički odjel, Sveučilište u Zagrebu, 1996.

[11] E.R.Lamken, S.A.Vanstone, *Elliptic Semiplanes and Group Divisible Designs with Orthogonal Resolutions*, Aequationes Mathematicae, **30** (1986), 80–92

[12] J.S.Leon, *Computing Automorphism Groups of Combinatorial Objects*, str. 321–335 u *Computational Group Theory* (ed. M.D.Atkinson), Academic Press, London, 1984.

[13] B.D.McKay, *Computing Automorphisms and Canonical Labellings of Graphs*, str. 223–232 u *Combinatorial Mathematics* (eds. D.A.Holton, J.Seberry), Lecture Notes in Mathematics **686**, Springer–Verlag, Berlin, 1977.

[14] B.D.McKay, `nauty` *User's guide (version 1.5)*, Technical Report TR-CS-90-02, Department of Computer Science, Australian National University, 1990.

[15] B.D.McKay, *Isomorph-free Exhaustive Generation*, Journal of Algorithms, **26** (1998), 306–324

[16] M.O.Pavčević, *Konstrukcija simetričnih blokovnih nacrta s automorfizmima reda pet*, magistarski rad, Matematički odjel, Sveučilište u Zagrebu, 1995.

[17] M.Schönert et al, *GAP – Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, 1995.

[18] E.Spence, *The Complete Classification of Steiner Systems* $S(2, 4, 25)$, Journal of Combinatorial Designs, **4** (1996), 295–300

[19] J.Šiftar, *On the Automorphism Groups of* $2-(46, 6, 1)$ *and* $2-(51, 6, 1)$ *Designs*, Glasnik Matematički, **22** (1987), 3–11

[20] J.Šiftar, B.Shita, *On Rigidity of* $2-(46, 6, 1)$ *Designs*, Glasnik Matematički, **26** (1991), 3–11

[21] R.M.Wilson, *Cyclotomy and Difference Families in Elementary Abelian Groups*, Journal of Number Theory, **4** (1972), 17–47

Sažetak

U ovom radu proučavaju se Steinerovi 2-dizajni s parametrima $S(k, 2k^2 - 2k + 1)$. Rad je podijeljen na pet poglavlja.

Prvo, uvodno poglavlje sadrži osnovne činjenice o dizajnima i djelovanju grupa, korištene kasnije u radu.

U drugom poglavlju analiziraju se svi poznati primjeri $S(k, 2k^2 - 2k + 1)$ dizajna s kombinatoričkog i geometrijskog stanovišta. Promatraju se njihove pune grupe automorfizama, poddizajni i skoro-rezolucije. Objašnjavaju se veze tih dizajna s drugim konačnim strukturama, kao što su simetrične $(2k^2 - 3k + 1)_k$ konfiguracije i eliptičke poluravnine.

U trećem poglavlju razvija se algoritam za klasifikaciju konačnih objekata. Algoritam su E.Spence i drugi koristili u raznim posebnim slučajevima. U radu je algoritam opisan i dokazan na općenit način, te je razvijen niz programa za njegovu provedbu (pisanih u programskom jeziku C). Pomoću algoritma su klasificirani Steinerovi 2-dizajni $S(3, 13)$, $S(3, 15)$ i $S(4, 25)$. Razrađena je primjena algoritma na klasifikaciju orbitnih struktura, često korištena u petom poglavlju.

Četvrto poglavlje posvećeno je konstrukciji dizajna pomoću diferencijskih familija. Tri $S(k, 2k^2 - 2k + 1)$ dizajna dobivaju se na osnovi teorema R.M.Wilsona iz 1972. Pokazano je da se na taj način za $6 \leq k \leq 2000$ ne mogu konstruirati dizajni. Dokazan je jedan nov rezultat, nepostojanje $(113, 8, 1)$ diferencijske familije.

U petom poglavlju primjenjuje se poznata metoda konstrukcije pomoću grupa automorfizama i taktičkih dekompozicija na Steinerove 2-dizajne $S(k, 2k^2 - 2k + 1)$. Algoritam iz trećeg poglavlja omogućuje rješavanje jednog otvorenog slučaja, $S(5, 41)$ s grupom automorfizama $\mathbb{Z}_3$. Dobiveno je devet novih $S(5, 41)$ dizajna. Dokazano je i nekoliko negativnih rezultata, na primjer nepostojanje $S(6, 61)$ dizajna s grupom automorfizama reda 25.

Summary

In this thesis Steiner 2-designs with parameters $S(k, 2k^2 - 2k + 1)$ are studied. The thesis is divided into five chapters.

The first, introductory chapter reviews some facts about designs and group actions needed in the sequel.

In the second chapter all known examples of $S(k, 2k^2 - 2k + 1)$ designs are analysed from a combinatorial and geometric standpoint. Their full automorphism groups, subdesigns and near-resolutions are considered. Connections between the designs and other finite structures, such as symmetric $(2k^2 - 3k + 1)_k$ configurations and elliptic semiplanes are explained.

In the third chapter a classification algorithm for finite objects is developed. The algorithm, used before by E.Spence and other authors in many different cases is described and proved in a general setting. An implementation in the programming language C is presented and the algorithm is applied to Steiner 2-designs $S(3, 13)$, $S(3, 15)$ and $S(4, 25)$. Furthermore, the ground is prepared for an application to tactical decomposition matrices (also called *orbit structures*), repeatedly used in the fifth chapter.

The fourth chapter deals with difference family constructions. Three $S(k, 2k^2 - 2k + 1)$ designs arise from a theorem by R.M.Wilson from 1972. It is shown that for $6 \leq k \leq 2000$ no further examples can be constructed in this fashion. A new result, the non-existence of $(113, 8, 1)$ difference families is proved.

In the fifth and final chapter the well-known construction method using automorphism groups and tactical decompositions is applied to $S(k, 2k^2 - 2k + 1)$ designs. The algorithm from chapter three allows us to cover a previously open case, $S(5, 41)$ with $\mathbb{Z}_3$ as an automorphism group. Nine new $S(5, 41)$ designs are constructed. A number of negative results are also proved, e.g. the non-existence of $S(6, 61)$ designs with automorphism group of order 25.

Životopis

Rođen sam 26. studenog 1973. u Zagrebu. Osnovnu školu sam pohađao u Zagrebu i u Hamburgu (od 2. do 4. razreda). Upisao sam se u Zagrebački MIOC (današnju XV. gimnaziju) i završio ga s odličnim uspjehom.

Školske godine 1992./93. upisao sam studij matematike (profil diplomirani inženjer matematike) na Matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Tokom treće i četvrte godine primao sam stipendiju grada Zagreba. Na četvrtoj godini dodijeljena mi je Rektorova nagrada za rad "Konstrukcija konačnih ravnina u programskom sustavu *Mathematica*". Diplomski rad "Klasifikacija konačnih projektivnih ravnina reda 7 i 8" izradio sam pod vodstvom prof.dr. J.Šiftara. Diplomirao sam s odličnim uspjehom u prosincu 1996.

Školske godine 1996./97. upisao sam poslijediplomski studij matematike na Prirodoslovno-matematičkom fakultetu. Od 1. travnja 1997. zaposlen sam na Matematičkom odjelu kao znanstveni novak. Na ljeto 1998. pohađao sam tečaj kombinatorne geometrije u Cortoni (Italija) u organizaciji *Scuola Matematica Interuniversitaria*. Predavači su bili prof.dr. G.-C.Rota i prof.dr. A.Beutelspacher. Zimski semestar školske godine 1998./99. proveo sam na Sveučilištu u Glasgowu, u studijskom posjetu prof.dr. E.Spenceu. Boravak je stipendirao *The British Scholarship Trust*, a putne troškove snosilo Ministarstvo znanosti i tehnologije.

Oženjen sam od prosinca 1997. Supruga Jelena također je diplomirala na Matematičkom odjelu.