

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODJEL

Vedran Krčadinac

Konstrukcija i klasifikacija konačnih
strukture pomoću računala

Disertacija

Voditelj: prof.dr.sc. Juraj Šiftar

Zagreb, svibanj 2004.

*Mojj djeci,
Emi i Jakovu.*

Ova disertacija predana je na ocjenu Prirodoslovno-matematičkom fakultetu – Matematičkom odjelu Sveučilišta u Zagrebu u svrhu stjecanja znanstvenog stupnja doktora prirodnih znanosti iz područja matematike.

Sadržaj

Predgovor	1
1 Potpuna klasifikacija	3
1.1 Problem klasifikacije	3
1.2 Provjera izomorfности i računanje pune grupe automorfizama	7
1.3 Algoritmi za klasifikaciju	10
1.4 Klasifikacija nekih linearnih prostora	16
1.5 Klasifikacija frekvencijskih kvadrata	21
1.6 Prebrojavanje frekvencijskih kvadrata	27
1.7 Klasifikacija orbitnih matrica	31
2 Klasifikacija uz dodatne pretpostavke	39
2.1 Steinerovi 2-dizajni i njihovi automorfizmi	39
2.2 Dizajni $S(2, 4, 28)$ s netrivialnim automorfizmima	45
2.3 Neki novi $S(2, 4, 37)$ dizajni	50
2.4 Još neki rezultati o Steinerovim 2-dizajnim	57
2.5 TSC prostori	60
3 Nepotpuna potraga	70
3.1 Egzistencija blok dizajna kao optimizacijski problem	70
3.2 Tabu search algoritam za blok dizajne i konfiguracije	72
3.3 Dizajni $S(2, k, 2k^2 - 2k + 1)$ kao TSC prostori	77
4 Dodatak	81
Literatura	107
Sažetak	115
Summary	116
Životopis	117

Predgovor

Tema ove disertacije su algoritamske tehnike konstrukcije i klasifikacije konačnih matematičkih struktura. One omogućuju rješavanje pomoću računala nekih kombinatornih problema za koje danas nisu poznati klasični dokazi i konstrukcije. U sklopu disertacije dobiveni su rezultati o blok dizajnima, konačnim linearnim prostorima, konfiguracijama, latinskim i frekvencijskim kvadratima i orbitnim matricama.

Ne treba posebno naglašavati ulogu koju računala imaju u matematici, kao ni ulogu koju je matematika odigrala u razvoju računala. Usprkos tome često se čuju ozbiljne zamjerke kad se računala koriste za dokazivanje matematičkih tvrdnji. Jedna je od uobičajenih zamjerki da dokazi pomoću računala nisu egzaktni, da su eksperimentalne prirode. Tu zamjerku smatramo samo djelomično opravdanom, jer je vjerojatnost da će se zbog hardverske greške dobiti krivi rezultat obično zanemarivo mala (i uvijek se može učiniti još manjom ponovnim izvođenjem programa). Ozbiljnija je strana zamjerke što je znatno teže provjeriti ispravnost kompjuterskog programa nego ispravnost klasičnog dokaza. U disertaciji posebnu pažnju posvećujemo provjeri rezultata pomoću nekoliko nezavisnih programa, kad god je to moguće. Na primjer, u dodatku su navedene distribucije klasa izotopije frekvencijskih kvadrata reda 7 i 8 obzirom na red pune grupe autotopija. To omogućuje usporedbu rezultata klasifikacije iz cjeline 1.5 s rezultatima prebrojavanja iz cjeline 1.6. Pokazano je da su rezultati dobiveni na vrlo različite načine međusobno usklađeni. Radu je priložen DVD na kojem se, osim elektronske verzije ovog teksta nalaze svi programi korišteni u disertaciji, kao i rezultati i međurezultati dugotrajnih kompjuterskih proračuna. Nadamo se da je na taj način olakšana provjera metoda i rezultata disertacije.

Druga je zamjerka da se pomoću računala ne mogu dobiti općeniti rezultati, nego samo pojedinačni primjeri. Za vrstu računalnih dokaza koja se koristi u disertaciji to je neosporno točno, ali uvjereni smo da i takvi rezultati mogu pridonijeti procesu matematičke spoznaje. Kao posljedica kompjuterskog prebrojavanja frekvencijskih kvadrata reda 8 otkrivena je greška u članku [18] (Teorem 3). Slabija tvrdnja dokazana je u Propoziciji 1.49. Jedan od najvažnijih rezultata disertacije, konstrukcija TSC prostora iz Teorema 2.36, otkriven je generalizacijom primjera konstruiranog pomoću računala.

Spomenut ćemo još jednu zamjerku kompjuterskim dokazima koja je estetske prirode, ali zapravo je smatramo najozbiljnijom. Istinitost nije jedini kriterij kojim se procjenjuju teoremi i njihovi dokazi; matematičari su oduvijek težili jasnoći i eleganciji ideja. Računalni dokazi koji se svode na provjeru milijuna pojedinačnih slučajeva jako su daleko od tog ideala.

Jedino opravdanje takvih dokaza može biti težina problema i stanje teorije koja se njima bavi. Neki od najvažnijih otvorenih problema ove grane kombinatorike (na primjer, postojanje konačnih projektivnih ravnina čiji red nije prim potencija) možda nikad neće biti riješeni elegantnim dokazima. Možda smo zbog kaotične prirode konačnih struktura zauvijek osuđeni na ispitivanje pojedinačnih slučajeva.

Nastanku disertacije doprinijele su mnoge osobe, kojima na ovom mjestu želim izraziti zahvalnost. Prvenstveno zahvaljujem voditelju, prof.dr.sc. Jurju Šiftaru na pozornom praćenju mojeg rada još od studentskih dana. Njegov se doprinos najviše osjeti u dijelovima disertacije koji se bave TSC prostorima, ali i u usmjeravanju mojih interesa ovom graničnom području geometrije i kombinatorike koje obiluje otvorenim problema pogodnim za rješavanje pomoću računala. Zahvaljujem članovima Seminara za geometriju, posebno prof.dr.sc. Mirku Poloniju, prof.dr.sc. Vladimiru Volencu i doc.dr.sc. Mariu Pavčeviću, za korisne sugestije prilikom izlaganja disertacije. Mnogi proračuni iz disertacije ne bi bili mogući bez distribuiranih paralelnih računala [Laboratorija za napredno računanje](#) Matematičkog odjela. Posebnu zahvalu dugujem voditelju LNR-a, prof.dr.sc. Nenadu Antoniću. Također zahvaljujem osoblju Računskog centra i knjižnice Matematičkog odjela na pruženoj podršci. Na kraju, zahvaljujem svim matematičarima iz čijih sam radova učio i čije sam ideje posredno ili neposredno koristio.

1 Potpuna klasifikacija

1.1 Problem klasifikacije

Neka je X konačan skup, a G grupa koja djeluje na X . Bavimo se problemom algoritamskog određivanja *skupa predstavnika* tog djelovanja, tj. skupa koji sadrži točno jedan element iz svake orbite. Elemente skupa X zovemo *objekti*, relaciju ekvivalencije induciranu djelovanjem grupe G zovemo *izomorfizam* i označavamo \cong , a stabilizator objekta $A \in X$ zovemo *puna grupa automorfizama* i označavamo $\text{Aut } A$. Navodimo tri vrste konačnih struktura koje se mogu opisati na taj način.

Definicija 1.1 *Incidencijska struktura* je trojka $(\mathcal{P}, \mathcal{L}, I)$, koja se sastoji od skupa \mathcal{P} čije elemente zovemo **točke**, skupa \mathcal{L} čije elemente zovemo **pravci** ili **blokovi** i relacije $I \subseteq \mathcal{P} \times \mathcal{L}$ koju zovemo **incidencija**.

U prvom slučaju objekti su konačne incidencijske strukture s danim skupom točaka i pravaca. Grupa G je direktan produkt grupa permutacija skupova \mathcal{P} i \mathcal{L} uz prirodno djelovanje na relacije incidencije.

Definicija 1.2 Neka je $\mathbb{N}_n = \{1, 2, \dots, n\}$. **Matrica** dimenzija $m \times n$ nad skupom S je preslikavanje iz $\mathbb{N}_m \times \mathbb{N}_n$ u S .

U drugom slučaju objekti su matrice dimenzija $m \times n$ nad konačnim skupom. Direktan produkt simetričnih grupa $G = S_m \times S_n$ djeluje na matrice permutiranjem redaka i stupaca. Za neke specijalne matrice od interesa su druga djelovanja, o čemu će biti govora [kasnije](#).

Definicija 1.3 **Graf** $\mathcal{G} = (V, B)$ sastoji se od konačnog skupa V čije elemente zovemo **vrhovi** i skupa B koji sadrži dvočlane podskupove od V . Podskupove sadržane u B zovemo **bridovi**.

U trećem slučaju objekti su grafovi s danim skupom vrhova, a G je grupa permutacija od V uz odgovarajuće djelovanje na bridovima.

Pojmovi iz prethodne tri definicije vrlo su općeniti i zapravo nas zanimaju samo specijalne klase takvih objekata. Bez dodatnih zahtjeva stupanj općenitosti je podjednak. Grafovi su specijalan slučaj incidencijskih struktura, ako vrhove identificiramo s točkama, a bridove s pravcima. Incidencijske strukture lako je reprezentirati matricama (Definicija 1.4). Matrice u [idućoj cjelini](#) reprezentiramo grafovima pomoću kojih ispitujemo izomorfnosti i računamo pune grupe automorfizama.

Definicija 1.4 Neka je S konačna incidencijska struktura sa skupom točaka $\mathcal{P} = \{P_1, \dots, P_m\}$ i skupom pravaca $\mathcal{L} = \{\ell_1, \dots, \ell_n\}$. **Incidencijska matrica** strukture S je $m \times n$ matrica $A = [a_{ij}]$ definirana sa

$$a_{ij} = \begin{cases} 1, & \text{ako je } P_i I \ell_j \\ 0, & \text{inače} \end{cases}$$

Slijedi opis konačnih struktura kojima se bavimo u ovoj disertaciji.

Definicija 1.5 Blok dizajn ili 2-dizajn s parametrima (v, k, λ) je incidencijska struktura s v točaka, čiji blokovi sadrže k točaka i u kojoj su svake dvije točke sadržane u λ blokova.

U disertaciji je izloženo nekoliko novih rezultata o egzistenciji 2-dizajna, uglavnom Steinerovih (s parametrom $\lambda = 1$). Kratak pregled poznatih rezultata o Steinerovim 2-dizajnima i njihove povijesti dan je na početku [drugog poglavlja](#), a opsežan pregled rezultata o dizajnima nalazi se u monografijama [5], [6] i [24].

Definicija 1.6 Konfiguracija s parametrima (v_r, b_k) je incidencijska struktura s v točaka i b pravaca, u kojoj svaka točka leži na r pravaca, svaki pravac sadrži k točaka i svake dvije točke su spojene najviše jednim pravcem. Ako je ukupan broj točaka jednak ukupnom broju pravaca, konfiguracija se naziva **simetričnom** i parametri bilježe (v_k) .

Definicija 1.7 Linearni prostor je konačna incidencijska struktura čije su svake dvije točke spojene jedinstvenim pravcem, a svaki pravac sadrži bar dvije točke.

Pregled teorije konačnih linearnih prostora dan je u knjizi [3]. Rezultati izloženi u disertaciji tiču se jedne specijalne klase linearnih prostora, uvedene u radu s J.Šiftarom [61].

Definicija 1.8 Za linearni prostor kažemo da je **TSC prostor** s parametrima (k, l) , ukratko $TSC(k, l)$, ako zadovoljava:

- (1) skup pravaca može se rastaviti na dva disjunktna podskupa tako da pravci iz prvog podskupa sadrže k točaka, a pravci iz drugog podskupa sadrže l točaka;
- (2) kroz svaku točku prolazi k pravaca iz prvog podskupa i l pravaca iz drugog podskupa.

Kratica TSC dolazi od engleskog “twofold symmetric configuration”, jer se zapravo radi o linearnim prostorima sastavljenim od dvije simetrične konfiguracije. U ovom poglavlju potpuno su klasificirani TSC(3, 4) prostori, a niz drugih rezultata o TSC prostorima izložen je u cjelini 2.5.

Važno je naglasiti da su definirane klase incidencijskih struktura invarijantne na izomorfizam, tj. da je svaka incidencijska struktura izomorfna (v, k, λ) blok dizajnu također blok dizajn s istim parametrima, i analogno za linearne prostore, konfiguracije i TSC prostore. To nam omogućuje ograničavanje klasifikacije samo na onu vrstu incidencijskih struktura koje nas zanimaju. Slijedi opis matrica na koje primjenjujemo algoritme za klasifikaciju.

Definicija 1.9 *Latinski kvadrat* reda n je matrica dimenzija $n \times n$ nad \mathbb{N}_n u kojoj se svaki od brojeva $1, 2, \dots, n$ javlja točno jednom u svakom retku i stupcu.

Definicija 1.10 *Frekvencijski kvadrat* reda n s frekvencijskim vektorom $\lambda = (\lambda_1, \dots, \lambda_s)$ je matrica dimenzija $n \times n$ nad \mathbb{N}_s u kojoj se broj i javlja točno λ_i puta u svakom retku i stupcu, za $i = 1, \dots, s$.

Pojam frekvencijskog kvadrata je generalizacija pojma latinskog kvadrata. Monografije o latinskim kvadratima i njihovim generalizacijama su [26] i [27], a elementarniji uvod dan je u knjizi [46]. U disertaciji je izloženo nekoliko novih rezultata o latinskim i frekvencijskim kvadratima reda 7 i 8.

Osim već uvedenog pojma izomorfizma, na skupu svih frekvencijskih kvadrata s danim frekvencijskim vektorom djeluje grupa $G = S_n \times S_n \times K$. Prva dva faktora djeluju permutiranjem redaka i stupaca, a K je podgrupa svih permutacija iz S_s koje ostavljaju frekvencijski vektor invarijantnim i djeluje permutiranjem simbola. Pripadna relacija ekvivalencije naziva se *izotopija*.

Na skupu latinskih kvadrata reda n dodatno djeluje grupa S_3 *konjugiranjem*, tj. zamjenjivanjem uloga redaka, stupaca i simbola. Semidirektan produkt grupe izotopija i grupe konjugacija inducira relaciju ekvivalencije koju zovemo *paratopija*, a klase ekvivalencije *glavne klase*. Osim toga latinski kvadrati predstavljaju tablice množenja algebarskih struktura poznatih kao *kvazigrupe* (uvod u teoriju kvazigrupa dan je u knjizi [100]). Od interesa je relacija ekvivalencije koja odgovara izomorfizmu kvazigrupa (u algebarskom smislu). Radi se o relaciji induciranoj djelovanjem podgrupe svih izotopija oblika $(\varphi, \varphi, \varphi) \in S_n \times S_n \times S_n$. Naglašavamo da se “algebarski izomorfizam” latinskih kvadrata ne podudara s pojmom izomorfizma uvedenim nakon Definicije 1.2. Izomorfizam u tom smislu induciran je djelovanjem podgrupe svih izotopija oblika (φ, ψ, id) , koje se u teoriji kvazigrupa nazivaju *glavne izotopije*.

Frekvencijski, a naročito latinski kvadrati su objekti zanimljivi sami po sebi i imaju brojne kombinatorne i statističke primjene. Iduća vrsta matrica manje je značajna, a treba nam za konstrukciju blok dizajna sa zadanom grupom automorfizama.

Definicija 1.11 *Orbitna matrica* za (v, k, λ) s marginalnim vektorima $\nu = (\nu_1, \dots, \nu_m)$ i $\beta = (\beta_1, \dots, \beta_n)$ je svaka $m \times n$ matrica $A = [a_{ij}]$ nad $\mathbb{N} \cup \{0\}$ koja zadovoljava:

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

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

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

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

Pritom treba vrijediti $\nu_1 + \dots + \nu_m = v$, $\beta_1 + \dots + \beta_n = b$, $r = \frac{\lambda(v-1)}{k-1}$ i $b = \frac{vr}{k}$.

Na skupu svih orbitnih matrica djeluje direktan produkt podgrupa od S_m i S_n koje ostavljaju marginalne vektore invarijantnim. Suženje grupe G u odnosu na grupu uvedenu nakon Definicije 1.2 treba nam da bi svojstva iz definicije orbitnih matrica ostala sačuvana pri izomorfizmu. U poglavlju 5.1 magistarskog rada [55] objašnjena je veza orbitnih matrica i automorfizama blok dizajna.

U disertaciji se ne bavimo direktno klasifikacijom grafova. Oni nam trebaju radi izračunavanja punih grupa automorfizama i provjere izomorfnosti, za što je također potrebna dodatna struktura.

Definicija 1.12 *Bojanje* grafa $\mathcal{G} = (V, B)$ je svaka funkcija $b : V \rightarrow \mathbb{N}$ sa skupa vrhova u skup prirodnih brojeva. **Obojani graf** sastoji se od grafa i jednog njegovog bojanja. **Izomorfizam** obojanih grafova $\mathcal{G} = (V, B, b)$ i $\mathcal{G}' = (V', B', b')$ je bijekcija $\varphi : V \rightarrow V'$ koja čuva bridove i bojanje, tj. ima svojstva $\varphi(B) = B'$ i $b = b' \circ \varphi$.

1.2 Provjera izomorfности i računanje pune grupe automorfizama

U ovoj cjelini bavimo se problemom provjere izomorfnosti danih objekata A , B i određivanja pune grupe automorfizama $\text{Aut } A$. To nije tema disertacije, ali se provjera izomorfnosti javlja kao osnovni korak u algoritmima za klasifikaciju i moramo je riješiti u sklopu njihove implementacije. Koristimo dva gotova rješenja, zasnovana na pojmu kanonskog preslikavanja.

Definicija 1.13 *Kanonsko preslikavanje je svaka funkcija $c : X \rightarrow X$ sa svojstvima $c(A) \cong A$ i $c(gA) = c(A)$, za sve $A \in X$ i $g \in G$.*

Provjera izomorfnosti objekata A , B svodi se na uspoređivanje njihovih kanonskih slika $c(A)$, $c(B)$ [55, Propozicija 3.5]. Programi koje koristimo izračunavaju sliku danog objekta $A \in X$ pod određenim kanonskim preslikavanjem i određuju punu grupu automorfizama $\text{Aut } A$.

Prvi program, razvijen u sklopu magistarskog rada [55], radi s matricama nad $\mathbb{N}_k \cup \{0\}$. Realizira kanonsko preslikavanje koje matrici $A \in X$ pridružuje maksimalni element pripadne orbite $\{gA \mid g \in G\}$, u smislu leksikografskog uređaja [55, Definicija 3.7]. Algoritam je opisan u poglavlju 3.1 magistarskog rada i dokazana je njegova valjanost. Program također izračunava red pune grupe automorfizama i pamti sve njezine elemente, što mu je glavni nedostatak. Za matrice s velikim grupama automorfizama i za jako pravilne matrice (kao što su incidencijske matrice dizajna) program je relativno spor i treba puno memorije. Koristimo ga za klasifikaciju orbitnih matrica, u obliku prilagođenom djelovanju odgovarajuće grupe G (permutacije redaka i stupaca koje čuvaju marginalne vektore). Uz neke preinake koristimo ga i za klasifikaciju frekvencijskih kvadrata obzirom na izotopiju.

Drugi program je `nauty` B.D.McKay-a [70]. Radi se o izuzetno efikasnom programu za računanje kanonskih predstavnika i punih grupa automorfizama obojanih grafova. Prednost je u tome što ne pamti cijelu grupu $\text{Aut } A$, nego samo jedan skup generatora. Program može obraditi vrlo pravilne grafove s velikim brojem vrhova i ogromnim grupama automorfizama. Nedostatak programa `nauty` je što nije jasno koje kanonsko preslikavanje realizira (ono ovisi o računalu i kompajleru koji se koristi).

Da bismo mogli primjenjivati `nauty` na incidencijske strukture i matrice, treba ih reprezentirati grafovima. Točnije, incidencijskim strukturama i matricama pridružujemo obojane grafove tako da ostanu sačuvani pojmovi izomorfnosti i pune grupe automorfizama. U istom su odnosu incidencijska struktura i njezina incidencijska matrica: dvije incidencijske strukture su izomorfne ako i samo ako su im incidencijske matrice izomorfne, a puna

grupa automorfizama incidencijske strukture izomorfna je punoj grupi automorfizama njezine incidencijske matrice. Incidencijske strukture mogu se na sljedeći način reprezentirati obojanim grafovima.

Definicija 1.14 *Neka je $S = (\mathcal{P}, \mathcal{L}, I)$ incidencijska struktura. Definiramo obojani graf $\mathcal{G}(S)$ sa skupom vrhova $V = \mathcal{P} \uplus \mathcal{L}$ (disjunktna unija), skupom bridova $B = \{P\ell \mid P \in \mathcal{P}, \ell \in \mathcal{L}, P I \ell\}$ i bojanjem $b(\mathcal{P}) = 1, b(\mathcal{L}) = 2$.*

Propozicija 1.15 *Skup svih izomorfizama s incidencijske strukture S na incidencijsku strukturu S' je u bijektivnom odnosu sa skupom svih izomorfizama s grafa $\mathcal{G}(S)$ na graf $\mathcal{G}(S')$.*

Dokaz. Izomorfizam sa S u S' je par (α, β) , pri čemu su $\alpha : \mathcal{P} \rightarrow \mathcal{P}$ i $\beta : \mathcal{L} \rightarrow \mathcal{L}$ bijekcije koje čuvaju incidenciju. Definiramo funkciju $\phi : V \rightarrow V$,

$$\phi(v) = \begin{cases} \alpha(v), & \text{za } v \in \mathcal{P} \\ \beta(v), & \text{za } v \in \mathcal{L} \end{cases}$$

Lako se provjeri da je ϕ izomorfizam obojanih grafova $\mathcal{G}(S)$ i $\mathcal{G}(S')$. Pridruživanje $(\alpha, \beta) \mapsto \phi$ je bijekcija jer ima inverznu funkciju. Izomorfizam obojanih grafova ϕ preslikava \mathcal{P} i \mathcal{L} na sebe (jer čuva bojanje), pa možemo definirati restrikcije $\alpha = \phi|_{\mathcal{P}}$ i $\beta = \phi|_{\mathcal{L}}$. □

Korolar 1.16 *Incidencijske strukture S i S' su izomorfne ako i samo ako su pridruženi grafovi $\mathcal{G}(S)$ i $\mathcal{G}(S')$ izomorfni.*

Korolar 1.17 *Puna grupa automorfizama incidencijske strukture S izomorfna je punoj grupi automorfizama pridruženog grafa $\mathcal{G}(S)$.*

Dokaz. U slučaju $S = S'$ pridruživanje $(\alpha, \beta) \mapsto \phi$ je izomorfizam grupa, jer kompoziciji automorfizama pridružuje kompoziciju njihovih slika. □

Graf iz Definicije 1.14 koristimo u programima `incfilter.c` i `aut.c` za ispitivanje izomorfne i računanje pune grupe automorfizama incidencijskih struktura (točnije, njihovih incidencijskih matrica). Program `nauty` također primjenjujemo na frekvencijske kvadrate s relacijom izotopije. Reprezentiramo ih obojanim grafovima na sljedeći način.

Definicija 1.18 *Neka je $A = [a_{ij}]$ frekvencijski kvadrat reda n s frekvencijskim vektorom $\lambda = (\lambda_1, \dots, \lambda_s)$. Neka su $R = \{r_1, \dots, r_n\}$, $C = \{c_1, \dots, c_n\}$, $S = \{1, \dots, s\}$ i $M = \{m_{ij} \mid i, j = 1, \dots, n\}$ međusobno disjunktni skupovi. Definiramo graf $\mathcal{G}(A)$ sa skupom vrhova $V = R \cup C \cup S \cup M$, skupom bridova $B = \cup_{i,j=1}^n \{r_i m_{ij}, c_j m_{ij}, a_{ij} m_{ij}\}$ i bojanjem $b(R) = 1, b(C) = 2, b(S) = 3, b(M) = 4$.*

Propozicija 1.19 *Skup svih izotopija s frekvencijskog kvadrata A na frekvencijski kvadrat B je u bijektivnom odnosu sa skupom svih izomorfizama s grafa $\mathcal{G}(A)$ na graf $\mathcal{G}(B)$.*

Dokaz. Neka je $(\varphi, \psi, \sigma) \in S_n \times S_n \times K$ izotopija kvadrata $A = [a_{ij}]$ na kvadrat $B = [b_{ij}]$. To znači da je $\sigma(a_{\varphi^{-1}(i)\psi^{-1}(j)}) = b_{ij}$, za $i, j = 1, \dots, n$. Definiramo funkciju $\phi : V \rightarrow V$ sa $\phi(r_i) = r_{\varphi(i)}$, $\phi(c_j) = c_{\psi(j)}$, $\phi(k) = \sigma(k)$ i $\phi(m_{ij}) = m_{\varphi(i)\psi(j)}$, za $i, j = 1, \dots, n$, $k = 1, \dots, s$. Ona je očito bijekcija i čuva bojanje. Skupove bridova $\{r_i m_{ij} \mid i, j = 1, \dots, n\}$ i $\{c_i m_{ij} \mid i, j = 1, \dots, n\}$ funkcija ϕ preslikava na same sebe, a skup $\{a_{ij} m_{ij} \mid i, j = 1, \dots, n\}$ preslikava na $\{\sigma(a_{ij})m_{\varphi(i)\psi(j)} \mid i, j = 1, \dots, n\} = \{\sigma(a_{\varphi^{-1}(i)\psi^{-1}(j)})m_{ij} \mid i, j = 1, \dots, n\} = \{b_{ij} m_{ij} \mid i, j = 1, \dots, n\}$. Dakle, ϕ je izomorfizam obojanih grafova $\mathcal{G}(A)$ i $\mathcal{G}(B)$.

Pokazat ćemo da je pridruživanje $(\varphi, \psi, \sigma) \mapsto \phi$ bijekcija tako da definiramo inverznu funkciju. Svaki izomorfizam obojanih grafova ϕ ima svojstva $\phi(R) = R$, $\phi(C) = C$, $\phi(S) = S$ i $\phi(M) = M$. Neka su $\varphi, \psi \in S_n$ i $\sigma \in S_s$ permutacije za koje je $\phi(r_i) = r_{\varphi(i)}$, $\phi(c_j) = c_{\psi(j)}$ i $\phi(k) = \sigma(k)$. Izomorfizam ϕ preslikava bridove $r_i m_{ij}$, $c_j m_{ij}$ na bridove $r_{\varphi(i)}\phi(m_{ij})$, $c_{\psi(j)}\phi(m_{ij})$. Zaključujemo da je $\phi(m_{ij}) = m_{\varphi(i)\psi(j)}$. Skup bridova $\{a_{ij} m_{ij} \mid i, j = 1, \dots, n\}$ preslikava se na $\{\sigma(a_{ij})m_{\varphi(i)\psi(j)} \mid i, j = 1, \dots, n\} = \{\sigma(a_{\varphi^{-1}(i)\psi^{-1}(j)})m_{ij} \mid i, j = 1, \dots, n\}$. Taj skup je jednak $\{b_{ij} m_{ij} \mid i, j = 1, \dots, n\}$ jer je ϕ izomorfizam grafova, iz čega slijedi $\sigma(a_{\varphi^{-1}(i)\psi^{-1}(j)}) = b_{ij}$, za $i, j = 1, \dots, n$. Iz toga također slijedi da permutacija σ čuva frekvencijski vektor $\lambda = (\lambda_1, \dots, \lambda_s)$, jer su A i B kvadrati istog tipa. Dakle, (φ, ψ, σ) je izotopija kvadrata A na kvadrat B . \square

Korolar 1.20 *Frekvencijski kvadrati A i B su izotopni ako i samo ako su pridruženi grafovi $\mathcal{G}(A)$ i $\mathcal{G}(B)$ izomorfni.*

Korolar 1.21 *Puna grupa autotopija frekvencijskog kvadrata A izomorfna je punoj grupi automorfizama pridruženog grafa $\mathcal{G}(A)$.*

Dokaz. U slučaju $A = B$ pridruživanje $(\varphi, \psi, \sigma) \mapsto \phi$ preslikava kompoziciju izotopija u kompoziciju njihovih slika. Vidimo da se radi o izomorfizmu grupe autotopija frekvencijskog kvadrata A i grupe automorfizama grafa $\mathcal{G}(A)$. \square

Graf iz Definicije 1.18 koristimo u programima `isofilter.c` i `fsaut.c`, koji ispituju izotopnost i računaju pune grupe autotopija frekvencijskih kvadrata. Jednostavnim modifikacijama Definicije 1.18 možemo postići da graf $\mathcal{G}(A)$ reprezentira druge relacije ekvivalencije na matricama. Na primjer, ako elemente skupa S obojimo različito, graf reprezentira relaciju induciranu permutacijama redaka i stupaca (“glavnim izotopijama”). Paratopiju latinskih

kvadrata dobivamo ako vrhove u R , C i S obojimo jednako, a izomorfizam ako na graf iz Definicije 1.18 dodamo bridove $\cup_{i=1}^n \{i r_i, i c_i, r_i c_i\}$.

Na kraju navodimo nekoliko referenci o algoritmima za ispitivanje izomorfности i računanje punih grupa automorfizama konačnih struktura: W.Kocay [52], D.L.Kreher, D.R.Stinson [62, poglavlje 7], J.S.Leon [64] i [65], B.D.McKay [69] i R.C.Read, D.G.Corneil [86].

1.3 Algoritmi za klasifikaciju

Funkciju koja iz skupa $S \subseteq X$ izbacuje izomorfne objekte zovemo *filtrar*.

Definicija 1.22 Za funkciju $f : 2^X \rightarrow 2^X$ kažemo da je **filtrar** ako ima svojstva (1) $f(S) \subseteq S$, (2) objekti iz $f(S)$ međusobno su neizomorfni i (3) svaki objekt iz S izomorfan je nekom iz $f(S)$, za sve $S \subseteq X$.

Jedna takva funkcija može se realizirati pomoću kanonskog preslikavanja. Algoritam je opisan u magistarskom radu [55, Algoritam 3.16] i implementiran za incidencijske matrice programom `incfilter.c`, a za frekvencijske kvadrate s relacijom izotopije programom `isofilter.c`.

Naivan pristup problemu klasifikacije bila bi primjena filtra na cijeli skup X . U praksi to ne dolazi u obzir, jer X ima previše elemenata. Na primjer, ukupan broj incidencijskih matrica $TSC(3, 4)$ prostora, klasificiranih u Primjeru 1.36, veći je od $2.3 \cdot 10^{63}$ (to je izračunato na temelju podataka u Tablici 9). Osnovna ideja algoritama za klasifikaciju je postepeno izgrađivanje objekata, proširivanjem neizomorfnih parcijalnih objekata. Incidencijske strukture izgrađuju se dodavanjem točaka ili pravaca, matrice dodavanjem redaka ili stupaca, a grafovi dodavanjem vrhova ili bridova. Za općenit opis postupka potrebno je skup X organizirati u stablo.

Neka je $O \in X$ istaknuti objekt, kojeg zovemo *nulobjekt*, i $p : X \rightarrow X$ nilpotentna funkcija (takva da za neki $n \in \mathbb{N}$ vrijedi $p^n(X) = O$). Funkcija p definira stablo sa skupom vrhova X , pridružujući svakom objektu njegovog roditelja. Red objekta A definiran je sa $\text{ord } A = \min\{k \in \mathbb{N}_0 \mid p^k(A) = O\}$. Skup svih objekata reda k čini k -ti nivo stabla i označavamo ga X_k . Prirodno je također zahtijevati da se red elemenata čuva pri djelovanju grupe G .

Aksiom 0. Za sve $g \in G$ i $A \in X$ vrijedi $\text{ord}(gA) = \text{ord } A$.

U nastavku podrazumijevamo da je ispunjen Aksiom 0. Za formulaciju prvog algoritma za klasifikaciju, koji se u [85] naziva *klasičnim*, treba nam filtrar f i mogućnost izračunavanja praslike $p^{-1}(S) = \{A \in X \mid p(A) \in S\}$ (skupu objekata S pridružuje se skup djece objekata iz S).

Algoritam 1.23

$$\begin{aligned}
&R_0 = \{O\} \\
&\mathbf{za } i = 0, \dots, n - 1 \mathbf{ radi} \\
&[R_{i+1} = f(p^{-1}(R_i))
\end{aligned}$$

Cilj nam je dokazati da algoritam definira skupove predstavnika za sve nivoe stabla X . Koristimo sljedeći aksiom, koji dodatno usklađuje djelovanje grupe G s funkcijom p .

Aksiom 1. Za svaki $g \in G$ postoji $\bar{g} \in G$ takav da za svaki $A \in X$ vrijedi $gp(A) = p(\bar{g}A)$.

Identificiramo li $g \in G$ s preslikavanjem $A \mapsto gA$, u aksiomu zahtijevamo postojanje “proširenja” $\bar{g} \in G$ za koje ovaj dijagram komutira:

$$\begin{array}{ccc}
X & \xrightarrow{g} & X \\
p \uparrow & & \uparrow p \\
X & \xrightarrow{\bar{g}} & X
\end{array}$$

Neposredna posljedica Aksioma 1 je da izomorfni objekti imaju ekvivalentne skupove djece, u sljedećem smislu.

Lema 1.24 *Ako su objekti A i B izomorfni, onda za svaki $\bar{A} \in p^{-1}(A)$ postoji $\bar{B} \in p^{-1}(B)$ izomorfan s \bar{A} .*

Dokaz. Neka za $g \in G$ vrijedi $B = gA$ i neka je $\bar{g} \in G$ proširenje iz Aksioma 1. Tada za $\bar{B} = \bar{g}\bar{A}$ vrijedi $p(\bar{B}) = p(\bar{g}\bar{A}) = gp(\bar{A}) = gA = B$, tj. $\bar{B} \in p^{-1}(B)$. Time je tvrdnja dokazana. □

Trebat će nam i ova generalizacija Aksioma 1.

Lema 1.25 *Za svaki $g \in G$ i $k \in \{1, \dots, n\}$ postoji $\bar{g} \in G$ takav da za svaki $A \in X$ vrijedi $gp^k(A) = p^k(\bar{g}A)$.*

Dokaz. Indukcijom po k . Za $k = 1$ dobivamo tvrdnju Aksioma 1. Pretpostavimo da tvrdnja vrijedi za k i neka je $g \in G$ proizvoljan. Prema Aksiomu 1 postoji $\bar{g} \in G$ takav da je $gp(B) = p(\bar{g}B)$, za svaki $B \in X$. Po pretpostavci indukcije za taj \bar{g} postoji $\bar{\bar{g}} \in G$ takav da je $\bar{g}p^k(A) = p^k(\bar{\bar{g}}A)$, za svaki $A \in X$. Posebno, za $B = p^k(A)$ dobivamo $gp^{k+1}(A) = gp(B) = p(\bar{g}B) = p(\bar{g}p^k(A)) = p^k(p(\bar{g}A)) = p^k(p^k(\bar{\bar{g}}A)) = p^{k+1}(\bar{\bar{g}}A)$, za svaki $A \in X$. □

Dokaz valjanosti Algoritma 1.23 zasniva se na tvrdnji Leme 1.24, slabijem zahtjevu od Aksioma 1.

Propozicija 1.26 *Ako vrijedi tvrdnja Leme 1.24, onda je R_i definiran Algoritmom 1.23 skup predstavnika za X_i , za $i = 0, \dots, n$.*

Dokaz. Objekti u R_i međusobno su neizomorfni jer je R_i rezultat filtriranja. Vidimo također da su objekti u R_i reda i , tj. $R_i \subseteq X_i$. Indukcijom po i dokazujemo da je svaki objekt iz X_i izomorfan nekom iz R_i . Tvrdnja očito vrijedi za $i = 0$. Pretpostavimo da tvrdnja vrijedi za neki $i \in \{0, \dots, n-1\}$ i neka je $\bar{A} \in X_{i+1}$. Po pretpostavci, za $A = p(\bar{A}) \in X_i$ postoji $B \in R_i$ izomorfan s A . Zbog Leme 1.24 postoji $\bar{B} \in p^{-1}(B)$ izomorfan s \bar{A} . Vidimo da je $\bar{B} \in p^{-1}(R_i)$, a R_{i+1} je dobiven filtriranjem skupa $p^{-1}(R_i)$. Prema tome, R_{i+1} sadrži objekt izomorfan s \bar{B} , dakle i s \bar{A} . □

Klasični algoritam definira skupove predstavnika za sve nivoe stabla, što može biti nedostatak. Obično nas zanimaju samo objekti na zadnjem (n -tom) nivou, a parcijalnih objekata ima znatno više. Neki od skupova R_1, \dots, R_{n-1} mogu postat preveliki za pohranjivanje na računalu, a da pritom R_n nema previše elemenata. Algoritam možemo učiniti efikasnijim prikladnim izborom nepraznih podskupova $Y_i \subseteq X_i$, $i = 0, \dots, n$, za koje je ispunjen sljedeći aksiom.

Aksiom 2. Za sve $A \in X_n$, $i = 0, \dots, n-1$ vrijedi: ako je $p^{n-i}(A) \in Y_i$, onda postoji $g \in G$ takav da je $p^{n-i}(gA) = p^{n-i}(A)$ i $p^{n-i-1}(gA) \in Y_{i+1}$.

Algoritam 1.27

$$R_0 = \{O\}$$

za $i = 0, \dots, n-1$ radi

$$[R_{i+1} = f(p^{-1}(R_i) \cap Y_{i+1})$$

Razlika u odnosu na Algoritam 1.23 je što ne filtriramo svu djecu objekata iz R_i , nego samo onu sadržanu u Y_{i+1} . Na primjer, ograničavamo se na incidencijske matrice nekog posebnog oblika, ili na reducirane frekvencijske pravokutnike (Definicija 1.39). Pomoću ovog algoritma dobivamo samo skup predstavnika za zadnji nivo stabla.

Propozicija 1.28 *Ako vrijede Aksiomi 1 i 2, onda je R_n definiran Algoritmom 1.27 skup predstavnika za X_n .*

Dokaz. Očito R_n sadrži međusobno neizomorfne objekte reda n , jer je do-
biven filtriranjem podskupa od Y_n . Dokazat ćemo da za svaki $A \in X_n$,
 $i \in \{0, \dots, n\}$ postoji $g \in G$ takav da je $p^{n-i}(gA) \in R_i$. Posebno, za $i = n$
to znači da je A izomorfan nekom objektu iz R_n , pa je R_n skup predstavnika
za X_n .

Tvrđnju dokazujemo indukcijom po i . Za $i = 0$ vrijedi $p^{n-i}(gA) =$
 $p^n(gA) = O \in R_0$, za bilo koji $g \in G$. Pretpostavimo da za $A \in X_n$,
 $i \in \{0, \dots, n-1\}$ postoji $g \in G$ takav da je $p^{n-i}(gA) \in R_i$ i označimo
 $A' = gA$. Kako je $R_i \subseteq Y_i$, prema Aksiomu 2 postoji $g' \in G$ takav da je
 $p^{n-i}(g'A') = p^{n-i}(A')$ i $p^{n-i-1}(g'A') \in Y_{i+1}$. Vidimo da je za $A'' = g'A'$
objekt $p^{n-i-1}(A'')$ sadržan u $p^{-1}(R_i) \cap Y_{i+1}$, pa je izomorfan nekom objektu
 $B \in R_{i+1}$. Točnije, postoji $g'' \in G$ takav da je $B = g'' p^{n-i-1}(A'')$. Prema
Lemi 1.25 za taj g'' postoji $\bar{g} \in G$ takav da je $p^{n-i-1}(\bar{g}A'') = g'' p^{n-i-1}(A'') =$
 $B \in R_{i+1}$, tj. $p^{n-i-1}(\bar{g}g'A) \in R_{i+1}$. Time je dokazano da tvrdnja vrijedi i
za $i+1$. □

Glavni nedostatak Algoritama 1.23 i 1.27 je što su zasnovani na filtri-
ranju. Novi objekti uspoređuju se sa svim do tada zapamćenim objek-
tima, pa algoritam radi sve sporije što su skupovi R_i veći. Osim toga po-
trebno je međurezultate (skupove R_1, \dots, R_{n-1}) cijele pohranjivati u memo-
riji računala. Kod većih problema klasifikacije skupovi R_i postat će preveliki
bez obzira na izbor skupova Y_i (na primjer, kod klasifikacije frekvencijskih
kvadrata reda 8).

U radovima R.C.Reada [85] i I.A.Faradževa [33] opisani su algoritmi
koji izbjegavaju problem filtriranja. U jednom trenutku pamte vrlo mali
skup objekata (po jedan objekt sa svakog nivoa), a nove objekte ne moraju
uspoređivati s do tada pronađenim predstavnicima. Ovdje opisujemo dva
takva algoritma pomoću uvedenih oznaka.

Neka je zadano kanonsko preslikavanje $c : X \rightarrow X$. Fiksne točke od c
(objekte $A \in X$ sa svojstvom $c(A) = A$) zovemo *kanonski objekti*. Nije teško
provjeriti da kanonski objekti čine skup predstavnika za X . Da bismo ih mo-
gli generirati proširivanjem parcijalnih objekata, potreban je sljedeći aksiom.

Aksiom 3. Ako je $c(A) = A$, onda je $c(p(A)) = p(A)$.

Drugim riječima, roditelj kanonskog objekta također je kanonski objekt.
Idući rekurzivni algoritam zasniva se samo na Aksiomu 3 (Aksiomi 1 i 2
nisu potrebni).

Algoritam 1.29

pretraži(A : objekt, i : nivo stabla)
[ako je $i = n$ onda ispiši A
inače za sve $B \in p^{-1}(A)$ radi
[ako je $c(B) = B$ onda pretraži($B, i + 1$)

Propozicija 1.30 *Ako vrijedi Aksiom 3, pozivom pretraži($O, 0$) rekurzivne funkcije definirane Algoritmom 1.29 ispisat će se svi kanonski objekti na n -tom nivou stabla.*

Dokaz. Očito se ispisuju kanonski objekti reda n . Treba vidjeti da će se ispisati svi takvi objekti. Neka je $C \in X_n$ proizvoljan kanonski objekt. Indukcijom po i dokazujemo da će se dogoditi poziv pretraži($p^{n-i}(C), i$), koji za $i = n$ ispisuje C .

Tvrdnja vrijedi za $i = 0$, jer tada dobivamo inicijalni poziv pretraži($O, 0$). Pretpostavimo da se za neki $i \in \{0, \dots, n-1\}$ dogodio poziv pretraži($p^{n-i}(C), i$). Funkcija rekurzivno poziva samu sebe za sve kanonske objekte $B \in p^{-1}(p^{n-i}(C))$, a među njima je zbog Aksioma 3 i objekt $p^{n-i-1}(C)$. Prema tome, dogodit će se poziv pretraži($p^{n-i-1}(C), i + 1$). □

Algoritam 1.29 ispisuje kanonske objekte na n -tom nivou stabla, ali zapravo pretražuje sve kanonske objekte na prethodnim nivoima. Slično kao kod klasičnog algoritma, moguće je ubrzati klasifikaciju prikladnim izborom podskupova $Y_i \subseteq X_i$, $i = 0, \dots, n$, koji zadovoljavaju sljedeći aksiom.

Aksiom 4. Za svaki kanonski objekt $C \in X_n$ vrijedi $p^{n-i}(C) \in Y_i$, za $i = 0, \dots, n$.

Na primjer, kod klasifikacije orbitnih matrica i frekvencijskih kvadrata ograničavamo se na matrice nekog posebnog oblika, u kojem su sve kanonske matrice.

Algoritam 1.31

pretraži(A : objekt, i : nivo stabla)
[ako je $i = n$ onda ispiši A
inače za sve $B \in p^{-1}(A) \cap Y_{i+1}$ radi
[ako je $c(B) = B$ onda pretraži($B, i + 1$)

Propozicija 1.32 *Ako vrijede Aksiomi 3 i 4, pozivom pretraži($O, 0$) rekurzivne funkcije definirane Algoritmom 1.31 ispisat će se svi kanonski objekti na n -tom nivou stabla.*

Dokaz. Isti kao dokaz Propozicije 1.30. Zbog Aksioma 4 jasno je da se preskaču samo oni parcijalni objekti koje nije moguće proširiti do kanonskog objekta reda n . □

U magistarskom radu [55] opisane su varijante prethodna dva algoritma koje stablo pretražuju po širini (Algoritam 3.19 i 3.22). Oni odjednom pamte cijele skupove predstavnika na nižim nivoima stabla, ali ne vrše filtriranje pa ih mogu pohranjivati na vanjsku memoriju računala. U disertaciji za klasifikaciju frekvencijskih kvadrata i orbitnih matrica koristimo Algoritme 1.29 i 1.31, implementirane programima `fsorderly.c` i `orbmat.c`.

Algoritmi za klasifikaciju koji na ovaj način izbjegavaju filtriranje nazivaju se u [47] *Read-Faradževljevi algoritmi*. R.C.Read [85] svoj algoritam naziva “orderly”, jer na skupu objekata uvodi totalni uređaj, a algoritam ispisuje kanonske objekte u rastućem redoslijedu. Uređaj mora zadovoljavati određene zahtjeve usklađenosti s kanonskim objektima i funkcijom p . Naša formulacija Algoritma 1.29 je slična, ali nije ovisna o izboru totalnog uređaja. Osim toga, kod nas je relacija izomorfizma inducirana djelovanjem grupe G na skup X , što nije slučaj u [85]. Po tome je sličnija formulacija I.A.Faradževa [33], gdje je algoritam opisan u okviru Pólya-de Bruijnoveg modela iz enumerativne kombinatorike. Objekti tog modela su funkcije $f : D \rightarrow H$, a izomorfizam je inducirana djelovanjem direktnog produkta grupa permutacija skupova D i H . U Faradževljevoj formulaciji također je potreban totalni uređaj na skupu D .

Model unutar kojeg su algoritmi za klasifikaciju opisani u ovoj disertaciji najbliži je B.D.McKayeovom modelu iz [71] (uz neka pojednostavljenja), koji se odnosi na jednu drugu vrstu algoritama za klasifikaciju. Read-Faradževljevi algoritmi prihvaćaju samo kanonske objekte, a McKayeovi algoritmi prihvaćaju samo objekte dobivene kanonskim proširivanjem (pri čemu nije važno jesu li objekti koji se proširuju kanonski). Prednost naše formulacije je u jednostavnosti. Algoritam 1.29 zasniva se u biti samo na jednom aksiomu (Aksiomu 3), dok je npr. u [71] formulirano 10 aksioma (Kaski [47] je primijetio da treba dodati i jedanaesti aksiom).

Unutar istog modela formulirali smo klasični algoritam za klasifikaciju, zasnovan na filtriranju. Iako su takvi algoritmi zaista stari (na primjer, A.Sade [89] je 1951. na taj način prebrojio latinske kvadrate reda 7), u literaturi nismo našli općenit opis. Jasno je da su klasični algoritmi daleko manje efikasni od Read-Faradževljevih i sličnih algoritama koji izbjegavaju

filtriranje. Međutim, na današnjim brzim računalima mogu se i na taj način riješiti nezanemarivi problemi klasifikacije. U iduće dvije cjeline pomoću Algoritama 1.23 i 1.27 klasificirali smo nekoliko manjih linearnih prostora, frekvencijske kvadrata reda 7 i djelomično reda 8.

Pored R.C.Read [85], I.A.Faradžev [33] i B.D.McKay [71], još neki radovi u kojima su na općenit način formulirani algoritmi za klasifikaciju su C.J.Colbourn, R.C.Read [25], L.A.Goldberg [39], D.Avis, K.Fukuda [2] i P.Kaski [47]. Potpun pregled rezultata dobivenih algoritmima za klasifikaciju zahtijevao bi puno veću bibliografiju nego u ovoj disertaciji. Spomenut ćemo radove P.C.Dennya i P.B.Gibbonsa [30] i [31] u kojima je prezentiran niz rezultata dobivenih klasičnim algoritmom uz razna poboljšanja, te radove E.Spencea koji je Read-Faradževljevim algoritmom klasificirao simetrične (31, 10, 3) dizajne [92], Hadamardove matrice reda 24 i 28 [93] i Steinerove 2-dizajne $S(2, 4, 25)$ [94]. Neki noviji rezultati su M.Meringer [73] (regularni grafovi), J.Heitzig, J.Reinhold [42] (rešetke) i P.Kaski, P.R.J.Östergård [48], [49], [50] i [81] (2-dizajni).

1.4 Klasifikacija nekih linearnih prostora

Neka su r_1, \dots, r_v stupnjevi točaka, a k_1, \dots, k_b stupnjevi pravaca linearnog prostora. Incidencijska matrica $A = [a_{ij}]$ tog linearnog prostora je $v \times b$ matrica nad $\{0, 1\}$ sa svojstvima:

- (1) $\sum_{i=1}^v a_{ij} = k_j$, za $1 \leq j \leq b$;
- (2) $\sum_{i=1}^v a_{ij}a_{ij'} \leq 1$, za $1 \leq j < j' \leq b$;
- (3) $\sum_{j=1}^b a_{ij} = r_i$, za $1 \leq i \leq v$;
- (4) $\sum_{j=1}^b a_{ij}a_{i'j} = 1$, za $1 \leq i < i' \leq v$.

Klasifikaciju možemo organizirati na više načina. Možemo proširivati parcijalne linearne prostore dodavanjem točaka ili dodavanjem pravaca, čemu odgovara proširivanje parcijalnih incidencijskih matrica dodavanjem redaka ili dodavanjem stupaca. Obično je efikasnije dodavanje redaka, jer je uvjet (4) jači od uvjeta (2). Međutim, za taj pristup moraju biti poznati stupnjevi točaka.

U drugom poglavlju disertacije javljaju se kao fiksne strukture automorfizama Steinerovih 2-dizajna linearni prostori s poznatim brojem točaka v ,

brojem pravac b i stupnjevima pravaca k_1, \dots, k_b , ali bez informacije o stupnjevima točaka. Takve linearne prostore klasificiramo dodavanjem pravaca, odnosno dodavanjem stupaca na parcijalne incidencijske matrice. Nuždan uvjet za postojanje linearnog prostora sa zadanim stupnjevima pravaca je $\binom{v}{2} = \sum_{i=1}^b \binom{k_i}{2}$ (dobiva se prebrojavanjem dvočlanih skupova točaka). Uz pretpostavku da je ispunjen, želimo uklopiti ovu situaciju u model iz prethodne cjeline unutar kojeg su formulirani algoritmi za klasifikaciju.

Neka je X_r skup svih $v \times r$ matrica $A = [a_{ij}]$ nad $\{0, 1\}$ koje zadovoljavaju

$$(1) \quad \sum_{i=1}^v a_{ij} = k_j, \text{ za } 1 \leq j \leq r;$$

$$(2) \quad \sum_{i=1}^v a_{ij} a_{ij'} \leq 1, \text{ za } 1 \leq j < j' \leq r.$$

Zbog relacije $\binom{v}{2} = \sum_{i=1}^b \binom{k_i}{2}$ skup X_b sadrži incidencijske matrice linearnih prostora koje klasificiramo, tj. za $r = b$ ispunjen je i zahtjev (4).

Za skup objekata uzimamo $X = X_0 \cup \dots \cup X_b$, a za funkciju $p : X \rightarrow X$ brisanje zadnjeg stupca matrice. Red matrice $\text{ord } A$ je broj njezinih stupaca. Neka je K_r podgrupa svih permutacija iz S_r koje ostavljaju vektor (k_1, \dots, k_r) invarijantnim. Grupa $G_r = S_v \times K_r$ djeluje na matrice iz X_r permutiranjem redaka i stupaca, a direktan produkt $G = G_0 \times \dots \times G_b$ na prirodan način djeluje na X : $(g_0, \dots, g_b) A = g_{\text{ord } A} A$, za $(g_0, \dots, g_b) \in G$ i $A \in X$. Jasno je da se pri takvom djelovanju čuva red objekata, tj. ispunjen je Aksiom 0. Da bismo mogli koristiti klasični algoritam za klasifikaciju, treba još provjeriti Aksiom 1. Neka je $g = (g_0, \dots, g_b) \in G$ i $g_r = (\alpha, \beta)$, za $\alpha \in S_v$ i $\beta \in K_r$. Definiramo

$$\bar{\beta} \in K_{r+1}, \quad \bar{\beta}(i) = \begin{cases} \beta(i), & \text{za } i \leq r \\ r + 1, & \text{za } i = r + 1 \end{cases}$$

Za $\bar{g}_{r+1} = (\alpha, \bar{\beta})$, $\bar{g} = (\bar{g}_0, \dots, \bar{g}_b)$ i za svaki $A \in X$ vrijedi $g p(A) = p(\bar{g} A)$.

Primjer 1.33 Klasificiramo linearne prostore s $v = 11$ točaka i $b = 16$ pravaca stupnjeva $k_1 = 5$, $k_2 = \dots = k_{16} = 3$, koji se javljaju u dokazu Propozicije 2.3. Za proširivanje parcijalnih incidencijskih matrica koristimo program `linexpand.c`, a za filtriranje `incfilter.c`. Broj matrica u skupovima `definiranim` Algoritmom 1.23 dan je u tablici.

i	1	2	3	4	5	6	7	8
$ R_i $	1	2	7	22	68	195	502	1027
i	9	10	11	12	13	14	15	16
$ R_i $	1483	1381	733	238	42	8	1	1

Vidimo da je **linearni prostor** jedinstven do na izomorfizam. Stupnjevi točkaca su $r_1 = \dots = r_5 = 4$, $r_6 = \dots = r_{11} = 5$.

Primjer 1.34 Klasificiramo linearne prostore s $v = 13$ točkaca i $b = 23$ pravaca stupnjeva $k_1 = \dots = k_{11} = 4$, $k_{12} = \dots = k_{23} = 2$. Oni se javljaju kao fiksne strukture automorfizama reda 2 dizajna $S(2, 4, 37)$ (Propozicija 2.18). Rezultati klasifikacije navedeni su u sljedećoj tablici.

i	1	2	3	4	5	6	7	8	9	10	11	12
$ R_i $	1	2	5	11	18	33	35	22	10	4	1	2
i	13	14	15	16	17	18	19	20	21	22	23	
$ R_i $	7	14	26	34	42	34	26	14	7	2	1	

Vidimo da postoji **samo jedan** takav linearni prostor. Stupnjevi točkaca su $r_1 = \dots = r_6 = 4$, $r_7 = \dots = r_{12} = 6$, $r_{13} = 8$.

Linearni prostori $TSC(k, l)$ imaju $v = k(k-1) + l(l-1) + 1$ točkaca, $b = 2v$ pravaca, svaka točkaca je stupnja $k+l$, točno pola pravaca je stupnja k , a druga polovica je stupnja l . Za njih je efikasnije klasifikaciju provoditi dodavanjem točkaca, odnosno dodavanjem redaka na parcijalne incidencijske matrice.

Neka je X_r skup svih $r \times b$ matrica $A = [a_{ij}]$ nad $\{0, 1\}$ sa svojstvima:

- (1) $\sum_{j=1}^b a_{ij} = k + l$, za $1 \leq i \leq r$;
- (2) $\sum_{j=1}^b a_{ij} a_{i'j} = 1$, za $1 \leq i < i' \leq r$;
- (3) $\sum_{i=1}^v a_{ij} \leq \max\{k, l\}$, za $1 \leq j \leq b$, pri čemu se jednakost dostiže najviše za v indeksa j .

Skup X_v osim incidencijskih matrica $TSC(k, l)$ prostora može sadržati incidencijske matrice drugih linearnih prostora. U sljedećem specijalnom slučaju ipak sadrži samo “dobre” matrice.

Propozicija 1.35 *Ako je $b = 2v$ i $l = k + 1$, skup X_v sadrži samo incidencijske matrice $TSC(k, k + 1)$ prostora.*

Dokaz. Promatramo incidencijsku strukturu reprezentiranu matricom iz X_v . Svaka točka je stupnja $2k + 1$, pa je ukupan broj incidencija $v(2k + 1)$. Ako sa b_1 označimo broj pravaca stupnja najviše k , a sa b_2 broj pravaca

stupnja $k + 1$, broj incidencija nije veći od $k b_1 + (k + 1)b_2$. Iz $b_1 + b_2 = 2v$ i $v(2k + 1) \leq k b_1 + (k + 1)b_2$ slijedi $b_2 \geq v$. U zahtjevu (3) tražimo $b_2 \leq v$, pa je broj pravaca stupnja $k + 1$ točno v . Iz toga također slijedi da su sve ostale točke stupnja k .

Dakle, imamo linearni prostor sa v točaka stupnja $2k + 1$, v pravaca stupnja k i v pravaca stupnja $k + 1$. Prebrojavanjem trojki (P, Q, ℓ) , gdje su P, Q dvije točke na pravcu ℓ , vidimo da je $v = 2k^2 + 1$. Da bi imali $\text{TSC}(k, k + 1)$ prostor, nedostaje još svojstvo (2) iz Definicije 1.8. Neka je r_1 broj pravaca stupnja k , a r_2 broj pravaca stupnja $k + 1$ kroz neku točku P . Vrijedi $r_1 + r_2 = 2k + 1$ i $r_1(k - 1) + r_2k = v - 1 = 2k^2$. Iz toga slijedi $r_1 = k$ i $r_2 = k + 1$, tj. kroz svaku točku prolazi k pravaca stupnja k i $k + 1$ pravaca stupnja $k + 1$. □

Za skup objekata uzimamo uniju $X = X_0 \cup \dots \cup X_v$, a za funkciju $p : X \rightarrow X$ brisanje zadnjeg retka matrice. Red matrice $\text{ord } A$ je broj njezinih redaka. Grupa $G_r = S_r \times S_b$ djeluje na matrice skupa X_r permutiranjem redaka i stupaca, a direktan produkt $G = G_0 \times \dots \times G_v$ djeluje na X isto kao prije: $(g_0, \dots, g_v) A = g_{\text{ord } A} A$, za $(g_0, \dots, g_v) \in G$ i $A \in X$. Aksiom 0 je očito ispunjen, a Aksiom 1 provjeravamo slično kao prije. Za $g = (g_0, \dots, g_v)$, $g_r = (\alpha, \beta)$, $\alpha \in S_r$, $\beta \in S_b$ definiramo

$$\bar{\alpha} \in S_{r+1}, \quad \bar{\alpha}(i) = \begin{cases} \alpha(i), & \text{za } i \leq r \\ r + 1, & \text{za } i = r + 1 \end{cases}$$

Tada za $\bar{g}_{r+1} = (\bar{\alpha}, \beta)$, $\bar{g} = (\bar{g}_0, \dots, \bar{g}_v)$ i za svaki $A \in X$ vrijedi $g p(A) = p(\bar{g} A)$.

Primjer 1.36 Klasificiramo linearne prostore $\text{TSC}(3, 4)$, sa $v = 19$ točaka i $b = 38$ pravaca. Točke su stupnja 7, a pravci stupnja 3 i 4. Algoritam 1.23 nije dovoljno efikasan, pa ograničavamo klasifikaciju na incidencijske matrice posebnog oblika i primjenjujemo Algoritam 1.27. Gornji dio incidencijske matrice bilo kojeg $\text{TSC}(3, 7)$ prostora može se permutiranjem redaka i stupaca dovesti u ovaj oblik:

$$A_0 = \begin{bmatrix} 11111110000000000000000000000000000000000000000000000000000000000000 \\ 10000001111110000000000000000000000000000000000000000000000000000000 \\ 10000000000001111110000000000000000000000000000000000000000000000000 \\ 10000000000000000000000001111110000000000000000000000000000000000000 \\ 01000001000001000001000001000001110000000000000000000000000000000000 \\ 01000000100000100000100000100000011100000000000000000000000000000000 \\ 01000000010000010000010000010000000111000000000000000000000000000000 \end{bmatrix}$$

Oblik se postiže kad prva četiri retka odgovaraju točkama nekog pravca stupnja 4, iduća tri retka točkama nekog drugog pravca stupnja 4 kroz prvu točku

i	7	8	9	10	11	12	13
$ R_i $	1	4	40	612	15379	274387	2146369
i	14	15	16	17	18	19	
$ R_i $	5910638	5415255	1574336	141254	4228	56	

Tablica 1: Klasifikacija TSC(3, 4) prostora.

i ako su stupci sortirani padajuće obzirom na leksikografski uređaj. Za skup $Y_i \subseteq X_i$ uzimamo sve matrice iz X_i koje se s matricom A_0 podudaraju u prvih $\min\{7, i\}$ redaka. Slijedi provjera Aksioma 2.

Neka je $A \in X_{19}$ potpuna incidencijska matrica TSC(3, 4) prostora sa svojstvom $p^{19-i}(A) \in Y_i$, tj. koja se podudara s matricom A_0 u prvih $\min\{7, i\}$ redaka. Za $i \geq 7$ očito je $p^{19-i-1}(A) \in Y_{i+1}$, pa možemo uzeti $g = 1$. S druge strane, za $i < 7$ može se kao što je opisano permutacijom redaka i stupaca $g \in G$ postići da se matrica gA podudara s matricom A_0 u prvih sedam redaka. Za taj g vrijedi $p^{19-i}(gA) = p^{19-i}(A)$ i $p^{19-i-1}(gA) \in Y_{i+1}$.

Klasifikaciju započinjemo od $R_7 = Y_7 = \{A_0\}$ (skupovi Y_1, \dots, Y_7 su jednočlani). Parcijalne incidencijske matrice proširujemo programom `tsc3-4expand.c`, a filtriramo ponovo sa `incfilter.c`. Rezultati klasifikacije dani su u Tablici 1. Dakle, postoji točno 56 neizomorfnih TSC(3, 4) prostora, čija su svojstva navedena u Tablici 9 (u cjelini 2.5). Ovaj rezultat dobiven je u sklopu rada [61].

Linearni prostori bez ograničenja na broj pravaca i stupnjeve točaka i pravaca klasificirani su za $v \leq 12$. Neka je $\text{LIN}(v)$ broj neizomorfnih linearnih prostora s v točaka. Poznate vrijednosti navodimo u sljedećoj tablici.

v	1	2	3	4	5	6	7	8	9	10	11	12
$\text{LIN}(v)$	1	1	2	3	5	10	24	69	384	5250	232 929	28 872 973

Broj $\text{LIN}(11)$ izračunao je C.Pietsch [83], tako da je prvo odredio sve mogućnosti za broj i stupnjeve pravaca, a zatim u svakom pojedinom slučaju klasificirao linearne prostore Read-Faradževljevom algoritmom. A.Betten i D.Betten [9] izračunali su $\text{LIN}(12)$ algoritmom kojeg nazivaju TDO-metoda (zasniva se na taktičkim dekompozicijama incidencijskih matrica). Isti autori su u [8] i [11] klasificirali prave linearne prostore (bez pravaca stupnja 2) s $v = 17$ i $v = 18$ točaka. Broj pravih linearnih prostora označavamo $\text{PLIN}(v)$ i navodimo poznate vrijednosti u tablici.

v	1-6	7	8	9-11	12	13	14	15	16	17	18
$\text{PLIN}(v)$	0	1	0	1	3	7	1	119	398	161 925	2 412 890

1.5 Klasifikacija frekvencijskih kvadrata

U ovoj cjelini određujemo skupove predstavnika svih frekvencijskih kvadrata reda $n \leq 8$ obzirom na relaciju izotopije. Za latinske kvadrate reda $n \leq 8$ broj klasa izotopije i glavnih klasa je poznat, ali među brojevima objavljenim u literaturi ima puno netočnih. H.W.Norton [80] našao je 146 glavnih klasa latinskih kvadrata reda 7. Točnu vrijednost, 147, odredio je A.Sade [89]. J.W.Brown [20] objavio je 1676257 kao broj klasa izotopije latinskih kvadrata reda 8, a V.L.Arlazarov i dr. [1] 283640 kao broj glavnih klasa. Točne vrijednosti, 1676267 i 283657, našli su G.Kolesova, C.W.H.Lam i L.Thiel [53]. Na više mjesta u literaturi navodi se 563 kao broj klasa izotopije latinskih kvadrata reda 7, na primjer u [24, Tablica II.1.6] i [26, Tablica 4.3.2]. U diplomskom radu [54] pronađeno je 564 klasa izotopije, a isti broj dobio je B.D.McKay [71]. Nije jasno odakle potječe pogrešna vrijednost 563 (vjerojatno se prepisuje još od Nortona).

L.J.Brant i G.L.Mullen [18] navode predstavnike klasa izotopije frekvencijskih kvadrata reda $n \leq 6$, osim za frekvencijske vektore $\lambda = (2, 2, 2)$, $(2, 2, 1, 1)$ i $(2, 1, 1, 1, 1)$. Konstruirali su ih filtriranjem skupova reduciranih frekvencijskih kvadrata.

Definicija 1.37 *Za frekvencijski kvadrat kažemo da je **reduciran** ako su brojevi u prvom retku i stupcu poredani uzlazno.*

Skup svih frekvencijskih kvadrata reda n s frekvencijskim vektorom λ označavamo $F(n; \lambda)$, a skup reduciranih frekvencijskih kvadrata $f(n; \lambda)$. Reducirani latinski kvadrati imaju u prvom retku i stupcu vektor $[1 \ 2 \ \cdots \ n]$. Skup svih latinskih kvadrata reda n označavamo $L(n)$, a reduciranih latinskih kvadrata $\ell(n)$.

Broj reduciranih latinskih i frekvencijskih kvadrata vrlo brzo raste s redom n (usp. Tablice 4 i 5). Za veće redove ne možemo dobiti predstavnike klasa izotopije filtriranjem svih reduciranih kvadrata, nego koristimo klasifikacijske algoritme iz cjeline 1.3. Trebaju nam sljedeći pojmovi.

Definicija 1.38 ***Frekvencijski** $k \times n$ **pravokutnik** s frekvencijskim vektorom $\lambda = (\lambda_1, \dots, \lambda_s)$ je matrica dimenzija $k \times n$ nad \mathbb{N}_s u kojoj se broj i javlja najviše λ_i puta u svakom retku i stupcu, za $i = 1, \dots, s$.*

Definicija 1.39 *Za frekvencijski $k \times n$ pravokutnik kažemo da je **reduciran** ako su brojevi u prvom retku poredani uzlazno, a prvi stupac slaže se s prvih k elemenata prvog retka.*

Skup svih frekvencijskih i latinskih $k \times n$ pravokutnika s označavamo $F(k, n; \lambda)$ i $L(k, n)$, a reduciranih frekvencijskih i latinskih pravokutnika $f(k, n; \lambda)$ i $\ell(k, n)$.

Za dani frekvencijski vektor $\lambda = (\lambda_1, \dots, \lambda_s)$ i red $n = \lambda_1 + \dots + \lambda_s$ želimo konstruirati jedan predstavnik iz svake klase izotopije kvadrata u $F(n; \lambda)$. Neka su objekti na k -tom nivou stabla frekvencijski $k \times n$ pravokutnici, $X_k = F(k, n; \lambda)$, a skup svih objekata $X = X_0 \cup \dots \cup X_n$. Funkcija $p : X \rightarrow X$ odbacuje zadnji redak matrice, tako da je $\text{ord}(A)$ broj redaka matrice A . Grupa $G_k = S_k \times S_n \times K$ djeluje na X_k permutiranjem redaka, stupaca i simbola, pri čemu je K podgrupa svih permutacija $\sigma \in S_s$ sa svojstvom $\lambda_i = \lambda_{\sigma(i)}$, $i = 1, \dots, s$ (koje ostavljaju frekvencijski vektor invarijantnim). Na cijelom skupu X djeluje direktan produkt $G = G_0 \times \dots \times G_n$ na prirodan način: $(g_0, \dots, g_n) A = g_{\text{ord}(A)} A$. Djelovanje čuva broj redaka, tj. ispunjen je Aksiom 0.

Klasifikaciju najprije provodimo Algoritmom 1.27 sa $Y_k = f(k, n; \lambda)$ (klasični algoritam uz ograničavanje na reducirane frekvencijske pravokutnike). To je u biti metoda kojom je A.Sade [89] odredio klase izotopije latinskih kvadrata reda 7. Krećemo od jedinstvenog reduciranog $1 \times n$ pravokutnika $R_1 \in f(1, n; \lambda)$, tj. vektora koji se sastoji redom od λ_1 jedinica, λ_2 dvojki i tako dalje. Proširujemo ga na sve moguće načine do reduciranog frekvencijskog $2 \times n$ pravokutnika (iz skupa $f(2, n; \lambda)$) i među njima eliminiramo izotopne. U idućem koraku proširujemo dobivene $2 \times n$ pravokutnike do pravokutnika iz skupa $f(3, n; \lambda)$, eliminiramo izotopne i analogno nastavljamo dalje. Želimo dokazati da u n -tom koraku dobivamo skup predstavnika za $F(n; \lambda)$. To slijedi iz Propozicije 1.28 ako vrijede Aksiomi 1 i 2.

Za provjeru Aksioma 1 uzmimo proizvoljan $g = (g_0, \dots, g_n) \in G$, gdje je $g_k = (\alpha, \beta, \sigma)$, $\alpha \in S_k$, $\beta \in S_n$ i $\sigma \in K$. Definiramo $\bar{g}_{k+1} = (\bar{\alpha}, \beta, \sigma)$, za $\bar{\alpha} \in S_{k+1}$, $\bar{\alpha}(i) = \begin{cases} \alpha(i), & \text{za } i \leq k \\ k+1, & \text{za } i = k+1 \end{cases}$. Tada za $\bar{g} = (\bar{g}_0, \dots, \bar{g}_n)$ i za proizvoljan $A \in X$ vrijedi $p(\bar{g} A) = g p(A)$.

Provjeravamo Aksiom 2; neka je $A = [a_{ij}] \in X_n$ frekvencijski kvadrat čijih prvih k redaka čine reduciran frekvencijski pravokutnik ($p^{n-k}(gA) \in Y_k$). Treba vidjeti da postoji njemu izotopan kvadrat gA koji se s A podudara u prvih k redaka ($p^{n-k}(gA) = p^{n-k}(A)$) i kojem prvih $k+1$ redaka čine reducirani frekvencijski pravokutnik ($p^{n-k-1}(gA) \in Y_{k+1}$). Označimo komponente jedinstvenog reduciranog $1 \times n$ pravokutnika sa $R_1 = [r_1 \ \dots \ r_n]$. Ako je $a_{k+1,1} = r_{k+1}$, možemo uzeti $g = id$. U suprotnom, r_{k+1} se mora pojaviti među brojevima $a_{k+2,1}, \dots, a_{n,1}$, recimo u i -tom retku ($a_{i,1} = r_{k+1}$). Tada za transpoziciju $\alpha = (k+1, i)$ i za $g = (id, \dots, id, (\alpha, id, id))$ vrijedi $p^{n-k}(gA) = p^{n-k}(A)$ i $p^{n-k-1}(gA) \in Y_{k+1}$. Time su provjerene pretpostavke

n	λ	Br. klasa	n	λ	Br. klasa
3	(2, 1)	1	7	(3, 2, 2)	1 939
	(1, 1, 1)	1		(3, 2, 1, 1)	5 300
4	(3, 1)	1		(3, 1, 1, 1, 1)	1 398
	(2, 2)	2		(2, 2, 2, 1)	15 269
	(2, 1, 1)	2		(2, 2, 1, 1, 1)	22 813
	(1, 1, 1, 1)	2		(2, 1, 1, 1, 1, 1)	6 941
5	(4, 1)	1		(1, 1, 1, 1, 1, 1, 1)	564
	(3, 2)	2	8	(7, 1)	1
	(3, 1, 1)	2		(6, 2)	7
	(2, 2, 1)	4		(6, 1, 1)	7
	(2, 1, 1, 1)	3		(5, 3)	51
	(1, 1, 1, 1, 1)	2		(5, 2, 1)	624
6	(5, 1)	1		(5, 1, 1, 1)	370
	(4, 2)	4		(4, 4)	156
	(4, 1, 1)	4		(4, 3, 1)	19 041
	(3, 3)	7		(4, 2, 2)	112 043
	(3, 2, 1)	23		(4, 2, 1, 1)	347 263
	(3, 1, 1, 1)	16		(4, 1, 1, 1, 1)	93 561
	(2, 2, 2)	46		(3, 3, 2)	766 361
	(2, 2, 1, 1)	106		(3, 3, 1, 1)	1 211 710
	(2, 1, 1, 1, 1)	56		(3, 2, 2, 1)	27 865 024
	(1, 1, 1, 1, 1, 1)	22	(3, 2, 1, 1, 1)	29 632 348	
7	(6, 1)	1	(3, 1, 1, 1, 1, 1)	4 735 238	
	(5, 2)	4	(2, 2, 2, 2)	26 983 466	
	(5, 1, 1)	4	(2, 2, 2, 1, 1)	171 710 120	
	(4, 3)	16	(2, 2, 1, 1, 1, 1)	137 000 435	
	(4, 2, 1)	92	(2, 1, 1, 1, 1, 1, 1)	29 163 047	
	(4, 1, 1, 1)	56	(1, 1, 1, 1, 1, 1, 1, 1)	1 676 267	
	(3, 3, 1)	226			

Tablica 2: Broj klasa izotopije frekvencijskih kvadrata.

Propozicije 1.28, pa zaključujemo da Algoritam 1.27 zaista definira skup predstavnika za frekvencijske kvadrate u $F(n; \lambda)$.

Na ovaj način klasificirali smo frekvencijske kvadrate reda 7 i 8, osim za frekvencijske vektore $\lambda = (2, 2, 2, 2)$, $(2, 2, 2, 1, 1)$, $(2, 2, 1, 1, 1, 1)$, $(2, 1, 1, 1, 1, 1, 1)$ i $(1, 1, 1, 1, 1, 1, 1, 1)$. Rezultati su navedeni u Tablici 2. Algoritam 1.27 implementiran je programima `fsexpand.c` (proširivanje reduciranih frekvencijskih pravokutnika jednim retkom) i `isofilter.c` (filtriranje izotopnih pravokutnika). U završnih nekoliko koraka obično je efikasnije zanemariti

filtriranje, jer se proširivanjem jednim retkom dobiva više pravokutnika nego proširivanjem do kraja. Kod klasifikacije kvadrata reda 8 za pojedine frekvencijske vektore filtrirali smo do 5. retka, zatim smo 5×8 pravokutnike proširivali do reduciranih frekvencijskih kvadrata i na kraju eliminirali izotopne (korišten je program `fscomplete.c`).

Za spomenute frekvencijske vektore reda 8 nije bilo moguće provesti klasifikaciju klasičnim algoritmom. Broj neizotopnih frekvencijskih pravokutnika koje treba filtrirati prevelik je za pamćenje u radnoj memoriji računala, a prelazak na vanjsku memoriju previše usporava algoritam. U tim slučajevima klasifikaciju provodimo Read-Faradževljevim algoritmom uz kanonsko preslikavanje $c : X \rightarrow X$, $c(A) = \min\{gA \mid g \in G\}$. Dakle, $c(A)$ je minimalni frekvencijski pravokutnik izotopan pravokutniku A obzirom na leksikografski uređaj [55, Definicija 3.7]. Minimalni predstavnici su reducirani, pa za Algoritam 1.31 možemo uzeti $Y_k = f(k, n; \lambda)$ (tj. ograničiti klasifikaciju na reducirane frekvencijske pravokutnike). Očito je ispunjen Aksiom 4, a u idućoj lemi provjeravamo Aksiom 3.

Lema 1.40 *Ako je $A \in F(k, n; \lambda)$ kanonski frekvencijski pravokutnik (najmanji od svih pravokutnika izotopnih s A), onda je pravokutnik $p(A) \in F(k - 1, n; \lambda)$ također kanonski.*

Dokaz. Pretpostavimo suprotno, da postoji izotopija $g \in G$ takva da je $gp(A) < p(A)$. Provjerili smo Aksiom 2, prema kojem postoji izotopija $\bar{g} \in G$ takva da je $gp(A) = p(\bar{g}A)$. Slijedi $p(\bar{g}A) < p(A)$, a zbog leksikografskog uspoređivanja matrica iz toga slijedi $\bar{g}A < A$. Dobili smo kontradikciju s pretpostavkom da je A minimalni element klase izotopije kojoj pripada. \square

Algoritam 1.31 u ovom je kontekstu implementiran programom `fsorderly.c`. Računanje minimalnih predstavnika klasa izotopije realizirano je tako da se za svaku permutaciju simbola koja čuva frekvencijski vektor pomoću [55, Algoritam 3.10] određuje minimalni predstavnik dobiven permutiranjem redaka i stupaca, te se bira najmanji među njima. To bi se vjerojatno moglo realizirati znatno efikasnije, ali program je dovoljno brz za klasifikaciju svih frekvencijskih kvadrata reda $n \leq 8$ osim za frekvencijski vektor $\lambda = (1, 1, 1, 1, 1, 1, 1, 1)$. Rezultati se slažu u slučajevima koji su prethodno klasificirani klasičnim algoritmom i navedeni su u Tablici 2.

Program `fsorderly.c` najsporiji je za latinske kvadrate, jer kod računanja minimalnih predstavnika provjerava $n!$ permutacija simbola. Latinski kvadrati reda 8 klasificirani su u [53] klasičnim algoritmom. Međutim, nije korištena varijanta A.Sadea [89], u kojoj se klasifikacija ograničava na reducirane kvadrate, nego varijanta J.W.Browna [20], u kojoj se razmatraju

samo latinski kvadrati čija se gornja polovica sastoji od parnih permutacija. U našim oznakama, uzima se $Y_k = \{A \in L(k, n) \mid \text{prvih } \lfloor \frac{n+1}{2} \rfloor \text{ redaka od } A \text{ su parne permutacije}\}$ i primjenjuje Algoritam 1.27. Ponovili smo klasifikaciju na taj način i dobili isti broj predstavnika kao u [53]. Za proširivanje latinskih pravokutnika parnim ili neparnim recima korišten je program `lsexpand.c`.

Kvazigrupa s jedinicom naziva se *petlja* [100]. Konačnim petljama odgovaraju latinski kvadrati koji imaju redak i stupac s elementima u prirodnom poretku (ne nužno prvi, kao kod reduciranih latinskih kvadrata).

Definicija 1.41 *Za latinski kvadrat $A = [a_{ij}] \in L(n)$ kažemo da je **petlja** ako postoji indeks i takav da je $a_{ij} = a_{ji} = j$, za svaki $j = 1, \dots, n$. Indeks i zovemo **jedinica** petlje.*

Skup svih petlji reda n označavamo $P(n)$. Izotop petlje ne mora biti petlja, ali svojstvo postojanja jedinice čuva se pod djelovanjem grupe izomorfizama. Točnije, simetrična grupa S_n djeluje na skup $P(n)$ na sljedeći način: $\varphi A = [\varphi(a_{\varphi^{-1}(i)\varphi^{-1}(j)})]$, za $\varphi \in S_n$, $A = [a_{ij}] \in P(n)$. Neizomorfne petlje reda 6 prebrojane su u [21], a reda 7 u [17]. Broj neizomorfni petlji reda $n \leq 6$ također je naveden u [26, Tablica 4.3.2] i [24, Tablica II.1.6]. Koristeći skup predstavnika klasa izotopije prebrojili smo neizomorfne petlje reda 8.

Poznato je da su latinski kvadrati A , B izotopni ako i samo ako je A izomorfan glavnom izotopu od B [100, Teorem 2.1.9] (glavne izotopije su permutacije redaka i stupaca). Prema tome, svaki latinski kvadrat izomorfan je glavnom izotopu nekog kvadrata iz skupa predstavnika klasa izotopije, a svaka petlja glavnom izotopu koji je i sam petlja. U idućoj propoziciji dokazujemo da među glavnim izotopima latinskog kvadrata reda n ima najviše n^2 petlji.

Propozicija 1.42 *Neka je A latinski kvadrat reda n . Glavni izotop $(\varphi, \psi, id)A$ je petlja točno za n^2 parova $(\varphi, \psi) \in S_n \times S_n$.*

Dokaz. Označimo retke matrice A sa $A(1), \dots, A(n)$, a stupce sa $A^\tau(1), \dots, A^\tau(n)$. Ako retke i stupce promatramo kao permutacije i kompoziciju permutacija označavamo \circ , možemo pisati

$$(\varphi, \psi, id)A = \begin{bmatrix} A(\varphi^{-1}(1)) \circ \psi^{-1} \\ \vdots \\ A(\varphi^{-1}(n)) \circ \psi^{-1} \end{bmatrix} = \begin{bmatrix} A^\tau(\psi^{-1}(1)) \circ \varphi^{-1} \\ \vdots \\ A^\tau(\psi^{-1}(n)) \circ \varphi^{-1} \end{bmatrix}^\tau$$

Vidimo da je $(\varphi, \psi, id)A$ petlja ako i samo ako je $\psi = A(i)$, $\varphi = A^\tau(j)$ za neke $i, j = 1, \dots, n$. □

n	1	2	3	4	5	6	7	8
Br.	1	1	1	2	6	109	23 746	106 228 849

Tablica 3: Broj neizomorfnih petlji reda n .

Petlje prebrojavamo tako da za svaki predstavnik klasa izotopije generiramo glavne izotope koji su petlje, prebrojimo koliko među njima ima neizomorfnih i sumiramo dobivene brojeve. Pritom treba pamtit i najviše n^2 predstavnika, jer latinski kvadrati koji nisu izotopni ne mogu biti izomorfni. Algoritam je realiziran programom `loopcount.c`, a rezultati prebrojavanja navedeni su u Tablici 3 (provjerili smo i brojeve za $n < 8$).

Na početku cjeline naveli smo greške u literaturi kod klasifikacije latinskih kvadrata, koje pokazuju težinu problema. Obzirom na složenost korištenih programa i dugotrajno izvođenje na računalima, opravdano je pitanje o točnosti dobivenih rezultata. Ideju za provjeru preuzimamo iz [53]. U idućoj smo cjelini prebrojili sve reducirane frekvencijske kvadrate reda $n \leq 8$ (Tablica 5). Također koristimo računala, ali prebrojavamo pomoću bitno jednostavnijeg backtracking algoritma. Ukupan broj frekvencijskih kvadrata možemo izračunati iz broja reduciranih kvadrata (Propozicija 1.43), a možemo ga također izračunati pomoću skupa predstavnika klasa izotopije i usporediti rezultate.

Neka je S skup predstavnika pri djelovanju grupe izotopija $G_n = S_n \times S_n \times K$ na skup frekvencijskih kvadrata $F(n; \lambda)$. Ako je $G_n A$ orbita frekvencijskog kvadrata A , a $\text{Aut } A$ grupa autotopija, vrijedi $|G_n| = |G_n A| \cdot |\text{Aut } A|$ ([55, Propozicija 1.18]). Iz toga slijedi $|F(n; \lambda)| = |G_n| \cdot \sum_{A \in S} \frac{1}{|\text{Aut } A|}$. Sjetimo se da je K podgrupa permutacija simbola koje ostavljaju vektor λ invarijantnim. Ako među brojevima $\lambda_1, \dots, \lambda_s$ ima m različitih, koji se javljaju s frekvencijama s_1, \dots, s_m , onda je $|K| = s_1! \cdots s_m!$. Primjenom Propozicije 1.43 dobivamo

$$\binom{n}{\lambda_1, \dots, \lambda_s} \binom{n-1}{\lambda_1-1, \lambda_2, \dots, \lambda_s} |f(n; \lambda)| = (n!)^2 s_1! \cdots s_m! \sum_{A \in S} \frac{1}{|\text{Aut } A|}$$

Pomoću programa `fsaut.c` izračunali smo redove grupa autotopija predstavnika frekvencijskih kvadrata. Koristeći gornju formulu u Mathematica bilježnici `provjera.nb` uspoređujemo rezultate klasifikacije i prebrojavanja frekvencijskih kvadrata reda 6, 7 i 8. Rezultati se u cijelosti slažu, a tablice iz bilježnice `provjera.nb` također navodimo u Dodatku.

1.6 Prebrojavanje frekvencijskih kvadrata

Prebrojavanje latinskih i, općenitije, frekvencijskih kvadrata spada u vrlo teške probleme enumerativne kombinatorike. Objavljeno je nekoliko formula za broj latinskih kvadrata reda n , od kojih je možda najjednostavnija [91] (kompliciranije formule dane su u [38] i [79]). Te formule uključuju sume kojima broj članova raste hipereksponecijalno s n i izraze kao što je permanenta, za koje nisu poznate efikasne metode izračunavanja. Zato ih nije moguće evaluirati već za vrlo male vrijednosti od n . Točan broj latinskih kvadrata poznat je za $n \leq 10$, a vrijednosti su dobivene direktnim prebrojavanjem reduciranih latinskih kvadrata. U idućoj propoziciji dana je veza ukupnog broja frekvencijskih kvadrata i broja reduciranih frekvencijskih kvadrata.

Propozicija 1.43

$$|F(n; \lambda_1, \dots, \lambda_s)| = \binom{n}{\lambda_1, \dots, \lambda_s} \binom{n-1}{\lambda_1-1, \lambda_2, \dots, \lambda_s} |f(n; \lambda_1, \dots, \lambda_s)|$$

Dokaz. L.J.Brant, G.L.Mullen [18], Teorem 2. □

Za latinske kvadrate dobiva se poznata formula $|L(n)| = n!(n-1)!|\ell(n)|$. U Tablici 4 navedeni su brojevi reduciranih latinskih kvadrata za $n \leq 10$ s pripadnim referencama. Starije reference preuzete su iz [26].

Broj reduciranih frekvencijskih kvadrata reda $n \leq 6$ odredili su L.J.Brant i G.L.Mullen [18]. U ovoj disertaciji prebrojili smo reducirane frekvencijske kvadrate reda 7 i 8 pomoću jednostavnog backtracking programa `reduced.c`. Rezultate navodimo u Tablici 5.

n	$ \ell(n) $	Referenca
1	1	
2	1	
3	1	
4	4	
5	56	L.Euler [32], 1779.
6	9 408	M.Frolov [35], 1890.
7	16 942 080	A.Sade [88], 1948.
8	535 281 401 856	M.B.Wells [101], 1967.
9	377 597 570 964 258 816	S.E.Bammel, J.Rothstein [4], 1975.
10	7 580 721 483 160 132 811 489 280	B.D.McKay, E.Rogoyki [72], 1995.

Tablica 4: Broj reduciranih latinskih kvadrata.

n	λ	$ f(n; \lambda) $	n	λ	$ f(n; \lambda) $	
3	(2, 1)	1	7	(3, 2, 2)	4 582 740	
	(1, 1, 1)	1		(3, 2, 1, 1)	3 442 464	
4	(3, 1)	2		(3, 1, 1, 1, 1)	2 586 432	
	(2, 2)	5		(2, 2, 2, 1)	19 969 380	
	(2, 1, 1)	3		(2, 2, 1, 1, 1)	14 998 608	
	(1, 1, 1, 1)	4		(2, 1, 1, 1, 1, 1)	11 270 400	
5	(4, 1)	6		(1, 1, 1, 1, 1, 1, 1)	16 942 080	
	(3, 2)	34		8	(7, 1)	720
	(3, 1, 1)	22			(6, 2)	318 930
	(2, 2, 1)	72			(6, 1, 1)	254 280
	(2, 1, 1, 1)	46	(5, 3)		12 268 464	
(1, 1, 1, 1, 1)	56	(5, 2, 1)	50 377 968			
6	(5, 1)	24	(5, 1, 1, 1)		40 171 008	
	(4, 2)	453	(4, 4)		47 740 325	
	(4, 1, 1)	318	(4, 3, 1)		771 067 692	
	(3, 3)	1 486	(4, 2, 2)		3 971 210 355	
	(3, 2, 1)	3 028	(4, 2, 1, 1)		3 166 707 276	
	(3, 1, 1, 1)	2 128	(4, 1, 1, 1, 1)		2 525 457 024	
	(2, 2, 2)	13 185	(3, 3, 2)		20 826 177 696	
	(2, 2, 1, 1)	9 282	(3, 3, 1, 1)		16 608 228 480	
	(2, 1, 1, 1, 1)	6 552	(3, 2, 2, 1)		85 538 838 240	
(1, 1, 1, 1, 1, 1)	9 408	(3, 2, 1, 1, 1)	68 220 465 792			
7	(6, 1)	120	(3, 1, 1, 1, 1, 1)	54 413 316 096		
	(5, 2)	9 876	(2, 2, 2, 2)	660 892 740 516		
	(5, 1, 1)	7 416	(2, 2, 2, 1, 1)	527 062 142 160		
	(4, 3)	98 484	(2, 2, 1, 1, 1, 1)	420 413 623 488		
	(4, 2, 1)	285 948	(2, 1, 1, 1, 1, 1, 1)	335 390 189 568		
	(4, 1, 1, 1)	214 752	(1, 1, 1, 1, 1, 1, 1, 1)	535 281 401 856		
	(3, 3, 1)	1 185 336				

Tablica 5: Broj reduciranih frekvencijskih kvadrata.

Prebrojavanje reduciranih latinskih kvadrata reda 7 traje na procesoru od 1.5 GHz otprilike jednu minutu. Brzina prebrojavanja je oko 280000 kvadrata u sekundi i dovoljna je za prebrojavanje svih frekvencijskih kvadrata reda 7 i nekih reda 8. Za pojedine frekvencijske kvadrate reda 8 bila je potrebna paralelna verzija programa (`reduced-m.c` i `reduced-s.c`), razvijena u sklopu sustava za distribuirano paralelno računanje PVM [37] (http://www.csm.ornl.gov/pvm/pvm_home.html). Programi su izvođeni na računalima `Laboratorija za napredno računanje` PMF-MO. Korišteno je

oko 20 procesora i postignute su brzine prebrojavanja do 6000000 kvadrata u sekundi.

Zbog jednostavnosti korištenih programa uvjereni smo da su vrijednosti u Tablici 5 točne. Brojevi latinskih kvadrata reda 7 i 8 slažu se s vrijednostima u literaturi (Tablica 4), a moguće je dodatno provjeriti i neke druge brojeve iz Tablice 5. U [72] prebrojani su reducirani latinski pravokutnici za $k \leq n \leq 10$. Te brojeve moguće je usporediti s brojem nekih frekvencijskih kvadrata odgovarajućeg reda.

Propozicija 1.44 $(n - k)! |L(k, n)| = n! (n - 1)! |\ell(k, n)|$

Dokaz. B.D.McKay, E.Rogoyski [72]. □

Propozicija 1.45 $|F(n; n - k, 1, \dots, 1)| = |L(k, n)|$

Dokaz. J.Dénes, G.L.Mullen [28]. □

Korolar 1.46 $|f(n; n - k, 1, \dots, 1)| = (n - k - 1)! |\ell(k, n)|$

Dokaz. Slijedi iz Propozicija 1.43, 1.44 i 1.45. □

Pomoću Korolara 1.46 i brojeva u Tablici 5 dobivamo $|\ell(k, 7)| = 309, 35792, 1293216, 11270400, 16942080$ za $k = 2, \dots, 6$ i $|\ell(k, 8)| = 2119, 1673792, 420909504, 27206658048, 335390189568, 535281401856$ za $k = 2, \dots, 7$. To se slaže s brojevima objavljenim u [72].

Na temelju brojeva u Tablici 5 otkrivena je greška u članku [18]. Frekvencijske vektore kojima su komponente sortirane silazno uspoređujemo leksikografski. Točnije, neka su λ, λ' vektori za koje je $\lambda_1 + \dots + \lambda_s = \lambda'_1 + \dots + \lambda'_{s'} = n$, $\lambda_1 \geq \dots \geq \lambda_s$ i $\lambda'_1 \geq \dots \geq \lambda'_{s'}$. Kažemo da je λ veći od λ' i pišemo $\lambda > \lambda'$ ako postoji indeks i za koji je $\lambda_1 = \lambda'_1, \dots, \lambda_{i-1} = \lambda'_{i-1}, \lambda_i > \lambda'_i$. Ako je $\lambda > \lambda'$ ili $\lambda = \lambda'$ pišemo $\lambda \geq \lambda'$. U [18, Teorem 3] tvrdi se da je broj frekvencijskih kvadrata reda n padajuća funkcija frekvencijskog vektora, tj. $|F(n; \lambda)| \leq |F(n; \lambda')|$ za sve $\lambda \geq \lambda'$. Protuprimjeri su brojevi $|F(8; 5, 2, 1)| = 888667355520$ i $|F(8; 5, 1, 1, 1)| = 2834466324480$, koji su oba veći od $|F(8; 4, 4)| = 116963796250$, te $|F(8; 4, 1, 1, 1, 1)| = 3563924952268800 > 2449158497049600 = |F(8; 3, 3, 2)|$.

U dokazu Teorema 3 u [18] definira se funkcija $\phi : F(n; \lambda') \rightarrow F(n; \lambda)$ i dokazuje da je surjekcija. Definicija te funkcije sadrži grešku. Koristi se sljedeći pojam, iako se u [18] ne spominje eksplicitno.

Definicija 1.47 Za frekvencijski kvadrat $A \in F(n; \lambda_1, \dots, \lambda_s)$ i $k \in \{1, \dots, s\}$ definiramo **k -transverzalu** kao skup od n elemenata matrice A , po jedan u svakom retku i stupcu, koji svi sadrže broj k .

Jasno je da latinski kvadrati imaju jedinstvenu k -transverzalu za svaki k . U frekvencijskim kvadratima također postoje k -transverzale za svaki k .

Propozicija 1.48 Neka je $A = [a_{ij}] \in F(n; \lambda_1, \dots, \lambda_s)$ frekvencijski kvadrat. Za svaki $k \in \{1, \dots, s\}$ postoji k -transverzala u A .

Dokaz. Definiramo bipartitan graf s vrhovima R_1, \dots, R_n i C_1, \dots, C_n u kojem je $R_i C_j$ brid ako i samo ako je $a_{ij} = k$. Prema “teoremu o braku” [99, str. 332] taj graf sadrži savršeno sparivanje, koje nam daje k -transverzalu u A . □

Za razliku od latinskih kvadrata, frekvencijski kvadrati mogu imati više od jedne k -transverzale:

$$\begin{array}{ccc} \boxed{1} & 1 & 2 \\ 1 & 2 & \boxed{1} \\ 2 & \boxed{1} & 1 \end{array} \qquad \begin{array}{ccc} 1 & \boxed{1} & 2 \\ \boxed{1} & 2 & 1 \\ 2 & 1 & \boxed{1} \end{array}$$

U [18] se slika $\phi(A)$ dobiva višestrukim izborom k -transverzale u A i zamjenom broja k na mjestima transverzale nekim drugim brojem. Za izbor k -transverzale koristi se “greedy” algoritam. U prvom koraku bira se najmanji indeks j_1 za koji je $a_{1j_1} = k$, u drugom koraku najmanji $j_2 \neq j_1$ za koji je $a_{2j_2} = k$ i tako dalje. Ako na taj način dođemo do n -tog retka, imat ćemo k -transverzalu $\{(1, j_1), \dots, (n, j_n)\}$. Međutim, za neke frekvencijske kvadrate ne može se doći do n -tog retka bez vraćanja unatrag. Na primjer, ako se traži

2-transverzala u $A = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$ nakon izbora $j_1 = 2, j_2 = 1$ nije moguće izabrati $j_3 \neq j_1, j_2$.

Naravno, k -transverzala mogla bi se birati na neki drugi način, recimo Ford-Fulkersonovim algoritmom primijenjenim na bipartitan graf iz dokaza Propozicije 1.48 (s izvorom i ponorom spojenim na particije). Tada bi funkcija ϕ bila dobro definirana, ali ne bi bilo moguće dokazati surjektivnost kao u [18]. Primjeri pokazuju da ϕ nije surjektivna za svaki izbor frekvencijskih vektora $\lambda > \lambda'$.

Ova metoda ipak daje djelomičnu informaciju o međusobnom odnosu brojeva frekvencijskih kvadrata istog reda. Kao posljedica Teorema 3 u [18] se navodi da latinskih kvadrata ima više od bilo koje druge vrste frekvencijskih kvadrata istog reda (Korolar 4). To se može dokazati pomoću ideja iz [18].

Propozicija 1.49 $|L(n)| \geq |F(n; \lambda)|$ za svaki frekvencijski vektor λ .

Dokaz. Tvrdnju dokazujemo definiranjem surjektivne funkcije $\phi : L(n) \rightarrow F(n; \lambda)$. Neka je $\lambda = (\lambda_1, \dots, \lambda_s)$. Prvo definiramo funkciju $\varphi : \mathbb{N}_n \rightarrow \mathbb{N}_s$, sa

$$\varphi(i) = \begin{cases} i, & \text{za } i \leq s \\ \min\{j \mid \lambda_1 + \dots + \lambda_j - j \geq i - s\}, & \text{za } i > s. \end{cases}$$

Funkcija $\phi : L(n) \rightarrow F(n; \lambda)$ djeluje na latinski kvadrat $A = [a_{ij}]$ supstitucijom simbola: $\phi(A) = [\varphi(a_{ij})]$. Preostaje dokazati surjektivnost od ϕ . Bilo koji frekvencijski kvadrat $B \in F(n; \lambda)$ može se pretvoriti u latinski kvadrat na sljedeći način. Neka je $k = \min\{i \mid \lambda_i > 1\}$. Pronađemo k -transverzalu u B i na odgovarajućim mjestima zamijenimo broj k brojem $s+1$. Tako dobivamo frekvencijski kvadrat iz skupa $F(n; \lambda_1, \dots, \lambda_k - 1, \dots, \lambda_s, 1)$. Višestrukom primjenom ove transformacije dobit ćemo latinski kvadrat A sa svojstvom $\phi(A) = B$. □

1.7 Klasifikacija orbitnih matrica

Klasifikacija orbitnih matrica pomoću Read-Faradževljevog algoritma objašnjena je u magistarskom radu [55, Primjer 3.27]. Ovdje ponavljamo općenit opis radi usklađivanja oznaka. U magistarskom radu korištene su varijante algoritma koje stablo pretražuju po širini [55, Algoritam 3.19 i 3.22]. U disertaciji za klasifikaciju orbitnih matrica koristimo Algoritme 1.29 i 1.31, koji stablo pretražuju po dubini. Primjenu tih algoritama ilustriramo primjerima koje u drugom poglavlju koristimo za konstrukciju Steinerovih 2-dizajna.

Neka su zadani dopustivi parametri blok dizajna v, r, b, k, λ i marginalni vektori $\nu = (\nu_1, \dots, \nu_m)$, $\beta = (\beta_1, \dots, \beta_n)$. Objekti na l -tom nivou stabla su parcijalne orbitne matrice sa l redaka. Točnije, skup X_l sadrži sve $l \times n$ matrice $A = [a_{ij}]$ nad $\mathbb{N} \cup \{0\}$ sa svojstvima:

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

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

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

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

U [55, Primjer 3.27] dokazano je da skup X_m sadrži orbitne matrice u smislu Definicije 1.11, tj. da za $l = m$ vrijedi jednakost u (3). Skup svih objekata neka je unija $X = X_0 \cup \dots \cup X_m$, a funkcija $p : X \rightarrow X$ brisanje zadnjeg retka matrice. Red matrice $\text{ord } A$ je broj njezinih redaka.

Neka su $H_l = \{\sigma \in S_l \mid \nu_{\sigma(i)} = \nu_i, i = 1, \dots, l\}$ i $K = \{\sigma \in S_n \mid \beta_{\sigma(i)} = \beta_i, i = 1, \dots, n\}$ grupe permutacija koje čuvaju marginalne vektore. Direktni produkt $G_l = H_l \times K$ djeluje na X_l permutiranjem redaka i stupaca, a $G = G_0 \times \dots \times G_m$ djeluje na cijeli skup X : $(g_0, \dots, g_m)A = g_{\text{ord } A} A$. Pri takvom djelovanju čuva se red objekata, tj. ispunjen je Aksiom 0.

Matrice uspoređujemo leksikografski [55, Definicija 3.7]. Kanonsko preslikavanje $c : X \rightarrow X$ definiramo sa $c(A) = \max\{gA \mid g \in G\}$. U magistarskom radu [55, Propozicija 3.18] dokazano je da odbacivanjem zadnjeg retka kanonske matrice dobivamo matricu koja je također kanonska. Dakle, vrijedi Aksiom 3.

Često unaprijed možemo reći kako izgleda prvih nekoliko redaka i stupaca kanonske orbitne matrice. Tada ograničavamo klasifikaciju samo na matrice tog oblika. Točnije, uzimamo neki podskup $Y_m \subseteq X_m$ koji sadrži sve kanonske matrice, definiramo $Y_i = p^{m-i}(Y_m)$ i koristimo Algoritam 1.31 umjesto Algoritma 1.29. Za takav izbor podskupova Y_i očito je ispunjen Aksiom 4.

Algoritmi 1.29 i 1.31 implementirani su programom `orbmat.c`. Program na ulazu uzima datoteku koja sadrži parametre v , k , λ , dimenzije orbitnih matrica m , n , marginalne vektore (ν_1, \dots, ν_m) , $(\beta_1, \dots, \beta_n)$ i eventualno prvih nekoliko redaka i/ili stupaca kanonske orbitne matrice. Na izlazu ispisuje sve takve orbitne matrice. Ograničenje programa je da marginalni vektori moraju biti konstantni iznad nepoznatog dijela orbitne matrice. Razlozi za ograničenje su tehnički i ono bi se moglo ukloniti.

Primjer 1.50 U Teoremu 2.9 konstruirani su svi $S(2, 4, 28)$ dizajni s automorfizmom reda 7. Orbitne matrice su dimenzija 4×9 , a marginalni vektori su $\nu = (7, 7, 7, 7)$ i $\beta = (7, 7, 7, 7, 7, 7, 7, 7, 7)$. Ulazna datoteka za program `orbmat.c` izgleda ovako:

28 4 1

4 9

7 7 7 7

7 7 7 7 7 7 7 7 7

?

Upitnik na kraju znači da ne zadajemo unaprijed oblik kanonskih orbitnih matrica, tj. koristimo Algoritam 1.29. Ime ulazne datoteke zadaje se u komandnoj liniji kod poziva programa `orbmat.c`. Program ispisuje sedam matrica:

4 9

7 7 7 7

7 7 7 7 7 7 7 7 7

2 2 2 1 1 1 0 0 0

2 1 0 1 0 0 2 2 1

0 1 0 2 2 1 1 0 2

0 0 2 0 1 2 1 2 1

2 2 2 1 1 1 0 0 0

2 1 0 1 0 0 2 2 1

0 1 0 1 2 2 2 0 1

0 0 2 1 1 1 0 2 2

2 2 2 1 1 1 0 0 0

2 1 0 1 0 0 2 2 1

0 1 1 0 2 1 2 0 2

0 0 1 2 1 2 0 2 1

2 2 2 1 1 1 0 0 0

2 0 0 1 1 1 2 2 0

0 2 0 1 1 1 2 0 2

0 0 2 1 1 1 0 2 2

3 1 1 1 1 1 1 0 0

1 2 1 1 0 0 0 2 2

0 1 1 0 2 2 1 2 0

0 0 1 2 1 1 2 0 2

3 1 1 1 1 1 1 0 0

1 2 1 1 0 0 0 2 2

0 1 1 0 3 1 1 1 1

0 0 1 2 0 2 2 1 1

3 1 1 1 1 1 1 0 0

1 1 1 1 1 0 0 3 1

0 2 1 1 1 2 0 0 2

0 0 1 1 1 1 3 1 1

2 Klasifikacija uz dodatne pretpostavke

2.1 Steinerovi 2-dizajni i njihovi automorfizmi

Istaknutu klasu 2-dizajna čine oni s parametrom $\lambda = 1$. Takvi dizajni nazivaju se *Steinerovim*, a parametri se umjesto $(v, k, 1)$ obično zapisuju u obliku $S(2, k, v)$. Ime je donekle nepravedno vezano uz švicarskog geometričara Jacoba Steinera, jer ih je prije njega proučavao engleski matematičar Thomas P. Kirkman. On je 1847. u [51] riješio problem egzistencije “Steinerovih” sistema trojki $S(2, 3, v)$: nuždan i dovoljan uvjet je $v \equiv 1$ ili $3 \pmod{6}$. Šest godina nakon Kirkmana, Steiner je u [96] samo postavio pitanje o postojanju $S(2, 3, v)$ dizajna (ne znajući za Kirkmanov rad).

Dizajni ponovo postaju aktualni sredinom 20. stoljeća, zbog primjena u statistici i planiranju eksperimenata. H.Hanani [40] je 1961. kombinacijom rekurzivnih i direktnih konstrukcija dokazao da su nužni uvjeti ujedno dovoljni za $k = 4$, a kasnije u [41] i za $k = 5$. Točnije, $S(2, 4, v)$ dizajni postoje ako i samo ako je $v \equiv 1$ ili $4 \pmod{12}$, a $S(2, 5, v)$ dizajni ako i samo ako je $v \equiv 1$ ili $5 \pmod{20}$. Za $k = 6$ tvrdnja ne vrijedi: $S(2, 6, 36)$ dizajn (afina ravnina reda 6) ne postoji iako $v = 36$ zadovoljava nuždan uvjet $v \equiv 1$ ili $6 \pmod{15}$.

Jedan od najvažnijih rezultata na ovom području je R.M.Wilsonov [102], prema kojem su za čvrsti k nužni uvjeti ujedno “asimptotički dovoljni”. Točnije, za svaki k postoji v_0 takav da $S(2, k, v)$ dizajni postoje za sve $v \geq v_0$ koji zadovoljavaju nužne uvjete. Dokaz nažalost nije konstruktivan, a spomenuti v_0 raste hipereksponencijalno kao funkcija od k [22].

Konstruktivni dokazi egzistencije zasnivaju se, slično kao u Hananijevim radovima, na rekurzivnim konstrukcijama i dovoljnom broju malih dizajna. Na primjer, Wilsonov teorem prema ocjeni u [22] garantira egzistenciju $S(2, 6, v)$ dizajna tek za $v \geq \exp(\exp(6^{36}))$, ali u ovom trenutku upitne su samo 32 dopustive vrijednosti v , od kojih je najveća 801. Najnoviji rezultati nalaze se na web stranici knjige Handbook of combinatorial designs [24] (<http://www.emba.uvm.edu/~dinitz/newresults.html>), a opsežan pregled rezultata o $S(2, 6, v)$ dizajnim dan je u [75]. Zbog ovakvog stanja teorije proizlazi važnost direktnih konstrukcija Steinerovih 2-dizajna za zadane parametre.

Potpuna klasifikacija moguća je samo za vrlo male parametre. Najbolje su proučene projektivne i afine ravnine, $S(2, n + 1, n^2 + n + 1)$ i $S(2, n, n^2)$. Klasificirane su za $n \leq 10$, a poznat je i jedini netrivialni uvjet na parametre, Bruck-Ryserov teorem (ako postoji ravnina reda $n \equiv 1$ ili $2 \pmod{4}$, onda se n može prikazati kao zbroj dva kvadrata). Više o klasifikaciji projektivnih i afinih ravnina može se pročitati u diplomskom radu [54]. Točan broj ostalih

Parametri	Broj	Referenca
$S(2, 3, 13)$	2	
$S(2, 3, 15)$	80	R.Mathon i dr. [68], 1983.
$S(2, 4, 25)$	18	E.Spence [94], 1996.
$S(2, 6, 46)$	0	S.K.Houghten i dr. [43], 2001.
$S(2, 3, 19)$	11 084 874 829	P.Kaski, P.R.J.Östergård [49], 2003.

Tablica 6: Broj Steinerovih 2-dizajna do na izomorfizam.

Steinerovih 2-dizajna poznat je samo za nekoliko parametara, navedenih u Tablici 6.

Izuzevši Bruck-Ryserov teorem, potpuna klasifikacija danas je jedini poznati način za dokazati nepostojanje Steinerovog 2-dizajna s dopustivim parametrima (kao u [43]). Međutim, ako dizajni postoje često je moguće konstruirati određen broj primjera i bez potpune klasifikacije. Algoritamske tehnike konstrukcije mogu se ugrubo podijeliti u dvije skupine. U prvoj se postavlja dodatni zahtjev na dizajne koje tražimo (najčešće djelovanje neke grupe automorfizama), pa se potpuno klasificiraju takvi dizajni. Što je dodatni zahtjevi jači, smanjuje se broj mogućnosti koje treba ispitati, ali se može dogoditi da traženi dizajni ne postoje. Druga tehnika je ograničavanje prevelikog broja mogućnosti koje treba ispitati pseudoslučajnim izborom. U ovom poglavlju bavimo se konstrukcijom Steinerovih 2-dizajna i TSC prostora sa zadanom grupom automorfizama, a u idućem poglavlju koristimo algoritme koji spadaju u drugu skupinu.

Metoda konstrukcije blok dizajna sa zadanom grupom automorfizama intenzivno se koristi od 80-tih godina 20. stoljeća (rani počeci nalaze se u radu R.C.Bosea [16] iz 1939.). Posljednji Steinerov 2-dizajn čija je egzistencija utvrđena na taj način našli su Z.Janko i V.D.Tonchev [44], matematičari koji su vjerojatno najzaslužniji za razvoj i širenje metode. U [44] je konstruiran $S(2, 7, 175)$ dizajn na kojem djeluje grupa reda 4200.

U ovoj disertaciji ograničavamo se na grupe prostog reda. Za njih je relativno lako utvrditi red i djelovanje na točke i pravce dizajna, ali računalni dio konstrukcije može biti vrlo zahtjevan. Pretpostavimo da su zadani parametri $S(2, k, v)$. Želimo vidjeti koji prosti brojevi mogu biti redovi automorfizama dizajna s tim parametrima.

Lema 2.1 *Ako $S(2, k, v)$ dizajn ima pravi $S(2, k, v')$ poddizajn, onda je $v \geq k(k^2 - 2k + 2)$.*

Dokaz. Neka je P točka koja ne pripada poddizajnu. Pravci kroz P sadrže najviše jednu točku poddizajna, pa je $r \geq v'$. Iz Fisherove nejednakosti

primijenjene na poddizajn slijedi $v' \geq k^2 - k + 1$ i time $r \geq k^2 - k + 1$. Nejednakost dobivamo iz $r = \frac{v-1}{k-1}$. \square

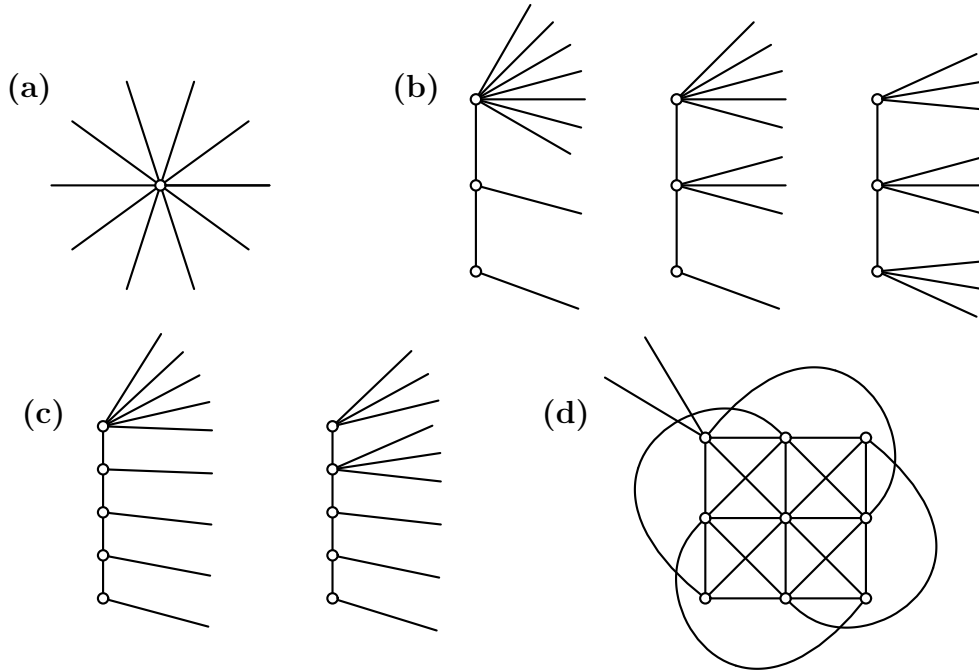
Lema 2.2 *Neka je α automorfizam prostog reda p dizajna $S(2, k, v)$. Ako je $v < k(k^2 - 2k + 2)$ i $p \geq k - 1$, onda α nema fiksnih točaka, ili ima jedinstvenu fiksnu točku, ili fiksira k točaka nekog pravca.*

Dokaz. Ako pravac sadrži dvije fiksne točke, sve točke tog pravca su fiksne (jer nefiksne točke leže u orbitama duljine $p > k - 2$). Kad bi imali tri nekolinearne fiksne točke, skup svih fiksnih točaka činio bi $S(2, k, v')$ poddizajn. To nije moguće zbog Leme 2.1, pa su sve fiksne točke automorfizma α kolinearne. Jasno je da ih ima 0, 1 ili k . \square

Pomoću Leme 2.2 dobivamo odgovor na pitanje o prostim redovima automorfizama Steinerovih 2-dizajna koji zadovoljavaju $v < k(k^2 - 2k + 2)$. Osim prostih brojeva manjih od $k - 1$, jedini kandidati su prosti faktori od v , $v - 1$ i $v - k$. Kad znamo red i strukturu grupe automorfizama, treba ispitati na koji način ona djeluje na točke i pravce dizajna. U slučaju grupe prostog reda p dovoljno je odrediti broj fiksnih točaka i pravaca, jer ostale točke i pravci leže u orbitama duljine p . Broj fiksnih točaka automorfizma reda $p \geq k - 1$ slijedi iz Leme 2.2, a lako se odredi i broj fiksnih pravaca (kao u dokazima Propozicija 2.6, 2.7 i 2.17). Međutim, Lema 2.2 ne odnosi se na automorfizme reda $p < k - 1$ (fiksne točke ne moraju biti kolinearne). U tom slučaju broj fiksnih točaka i pravaca i njihove incidencije možemo odrediti slično kao u [55, Propozicija 5.32]. Rezultat se odnosi na automorfizme reda 3 dizajna $S(2, 5, 41)$, a ovdje radi ilustracije tehnike dokazivanja promatramo automorfizme reda 2.

Propozicija 2.3 *Automorfizam reda 2 dizajna $S(2, 5, 41)$ fiksira jedan od sljedećih skupova točaka i pravaca.*

- (a) *Jedna točka i deset pravaca kroz nju.*
- (b) *Tri točke na pravcu i još devet pravaca kroz neke od fiksnih točaka. Dolaze u obzir tri rasporeda tih devet pravaca: $7 + 1 + 1$, $5 + 3 + 1$ i $3 + 3 + 3$.*
- (c) *Pet točaka na pravcu i još devet pravaca kroz neke od fiksnih točaka. Dolaze u obzir dva rasporeda tih devet pravaca, $5 + 1 + 1 + 1 + 1$ i $3 + 3 + 1 + 1 + 1$.*
- (d) *Devet točaka i dvanaest pravaca koji čine afinu ravninu reda 3, te još dva pravca kroz jednu od fiksnih točaka.*



Slika 1: Fiksne strukture automorfizma reda 2 dizajna $S(2, 5, 41)$.

Dokaz. Označimo broj orbita duljine 2 na točkama i pravicima redom sa m i n . Tada je broj fiksnih točaka $f = 41 - 2m$, a broj fiksnih pravaca $g = 82 - 2n$. Neka je \mathcal{B}_i skup pravaca incidentnih s i fiksnih točaka i $b_i = |\mathcal{B}_i|$, za $i = 0, \dots, 5$. Skupovi \mathcal{B}_2 i \mathcal{B}_4 očito su prazni. Pravci u \mathcal{B}_3 i \mathcal{B}_5 su fiksni, pravci u \mathcal{B}_0 nisu fiksni, a pravci u \mathcal{B}_1 mogu biti jedno i drugo. Označimo sa \mathcal{B}'_1 skup svih fiksnih, a \mathcal{B}''_1 skup svih nefiksnih pravaca u \mathcal{B}_1 , te $b'_1 = |\mathcal{B}'_1|$ i $b''_1 = |\mathcal{B}''_1|$. Ukupan broj pravaca i broj fiksnih pravaca možemo izraziti na sljedeći način:

$$b_0 + b'_1 + b''_1 + b_3 + b_5 = 82$$

$$b'_1 + b_3 + b_5 = g = 82 - 2n$$

Pravci iz skupa \mathcal{B}'_1 sadrže dvije orbite točaka duljine 2, a pravci iz \mathcal{B}_3 jednu.

$$2b'_1 + b_3 = m$$

Iduće dvije jednadžbe dobivamo prebrojavanjem parova fiksnih točaka i parova nefiksnih točaka.

$$3b_3 + 10b_5 = \binom{f}{2} = (20 - m)(41 - 2m)$$

$$10b_0 + 6(b'_1 + b''_1) + b_3 = \binom{2m}{2} = m(2m - 1)$$

Ovih pet jednadžbi imaju jedinstveno rješenje za dane m i n :

$$\begin{aligned} b_0 &= 18m - 8n \\ b'_1 &= \frac{m(m - 37)}{2} + 5n \\ b''_1 &= -18m + 10n \\ b_3 &= m(38 - m) - 10n \\ b_5 &= 82 + \frac{m(m - 39)}{2} + 3n \end{aligned}$$

Komponente rješenja su nenegativne za sedam parova $(m, n) \in \{1, \dots, 20\} \times \{1, \dots, 41\}$, navedenih u sljedećoj tablici.

R.br.	m	n	b_0	b'_1	b''_1	b_3	b_5	f	g
1	20	36	72	10	0	0	0	1	10
2	19	36	54	9	18	1	0	3	10
3	18	36	36	9	36	0	1	5	10
4	17	35	26	5	44	7	0	7	12
5	16	35	8	7	62	2	3	9	12
6	16	34	16	2	52	12	0	9	14
7	15	33	6	0	60	15	1	11	16

Prva tri retka tablice odgovaraju fiksnim strukturama (a), (b) i (c), a šesti redak strukturi (d). Četvrti, peti i sedmi redak opisuju nemoguće fiksne strukture. Struktura opisana petim retkom ima tri pravca iz skupa \mathcal{B}_5 . Za to bi nam trebalo bar 12 fiksnih točaka, a imamo $f = 9$. Preostaje eliminirati četvrti i sedmi redak tablice.

Primijetimo najprije da broj fiksnih pravaca kroz fiksnu točku mora biti paran, jer su nefiksni pravci grupirani u orbite duljine 2. Sedam točaka i sedam \mathcal{B}_3 -pravaca strukture opisane četvrtim retkom čine projektivnu ravninu reda 2. U njoj su stupnjevi točaka 3, pa bi morali imati bar još jedan fiksni pravac kroz svaku od sedam fiksnih točaka. Međutim, u četvrtom retku imamo samo pet pravaca u \mathcal{B}'_1 . Konačno, sedmi redak opisuje linearni prostor sa 11 točaka i 16 pravaca, od kojih je jedan stupnja 5, a ostali su stupnja 3. U Primjeru 1.33 utvrđeno je da postoji samo jedan takav linearni prostor, koji ima 6 točaka stupnja 5. Zato ne može biti fiksna struktura involutornog automorfizma $S(2, 5, 41)$ dizajna (u sedmom retku tablice je $b'_1 = 0$). \square

Poznato je ukupno 15 dizajna $S(2, 5, 41)$, od kojih su 9 pronađeni u magistarskom radu [55, Teorem 5.33], a jedan u [56]. U njihovim grupama automorfizama javljaju se involucije tipa (a), (b) i (c). Pritom su \mathcal{B}'_1 -pravci kod tipa (b) uvijek raspoređeni na način $3 + 3 + 3$, a kod tipa (c) na način $5 + 1 + 1 + 1 + 1$.

Dokaz sljedeće leme o involutornim automorfizmima $S(2, 4, v)$ dizajna sličan je prvom dijelu dokaza Propozicije 2.3.

Lema 2.4 *Neka je α automorfizam reda 2 dizajna s parametrima $S(2, 4, v)$. Označimo sa f i g broj točaka i pravaca koje α fiksira, a sa m i n broj orbita duljine 2 na točkama i pravcima. Neka je b_i broj pravaca koji sadrže točno i fiksnih točaka, a b'_0 i b''_0 broj fiksnih, odnosno nefiksnih pravaca koji ne sadrže fiksnu točku. Tada vrijedi:*

$$\begin{aligned} f &= v - 2m & b_1 &= 8n - \frac{2m(v-4)}{3} \\ g &= \frac{v(v-1)}{12} - 2n & b_2 &= m(v-m-2) - 6n \\ b'_0 &= \frac{m(m-v+3)}{2} + 3n & b_3 &= 0 \\ b''_0 &= \frac{2m(v-4)}{3} - 6n & b_4 &= \frac{v(v-1)}{12} + \frac{m(m-v+1)}{2} + n \end{aligned}$$

Dokaz. Očito je $f = v - 2m$, a druga jednakost slijedi iz $b = \frac{v(v-1)}{12}$. Ako pravac sadrži tri fiksne točke, četvrta točka tog pravca također je fiksna. Dakle, $b_3 = 0$. Ostale veličine s lijeve strane zadovoljavaju sljedeći sustav jednadžbi:

$$\begin{aligned} b'_0 + b''_0 + b_1 + b_2 + b_4 &= b = \frac{v(v-1)}{12} \\ b'_0 + b_2 + b_4 &= g = \frac{v(v-1)}{12} - 2n \\ 2b'_0 + b_2 &= m \\ b_2 + 6b_4 &= \binom{f}{2} = \frac{(v-2m)(v-2m-1)}{2} \\ 6(b'_0 + b''_0) + 3b_1 + b_2 &= \binom{2m}{2} = m(2m-1) \end{aligned}$$

Prve tri jednadžbe dobivamo izražavanjem preko b_i -ova ukupnog broja pravaca, broja fiksnih pravaca i broja orbita duljine 2 na točkama. Iduće dvije jednadžbe dobivamo dvostrukim prebrojavanjem parova fiksnih točaka i parova nefiksnih točaka. Formule za b'_0 , b''_0 , b_1 , b_2 i b_4 slijede rješavanjem ovog sustava jednadžbi. □

Lemu 2.4 koristimo u dokazima Propozicija 2.8 i 2.18. Za zadani v lako nalazimo parove (m, n) za koje su b_i -ovi nenegativni cijeli brojevi. Tako dobivamo sve mogućnosti za broj fiksnih točaka i pravaca i njihove međusobne incidencije.

2.2 Dizajni $S(2, 4, 28)$ s netrivialnim automorfizmima

Dizajni $S(2, 4, 28)$ pripadaju jednoj važnoj porodici, *unitalima*. Prema najopćenitijoj definiciji, unitali su Steinerovi 2-dizajni s parametrima oblika $S(2, q+1, q^3+1)$. Poznate su dvije beskonačne serije takvih dizajna. Klasični (ili hermitski) unitali dobivaju se kao skup apsolutnih točaka i neapsolutnih pravaca unitarnog polariteta projektivne ravnine $PG(2, q^2)$. Druga serija dobiva se pomoću jednostavnih Reeovih grupa (vidjeti [66]). Na oba načina moguće je konstruirati $S(2, 4, 28)$ dizajne, s punom grupom automorfizama reda 12096 i 1512.

U ovoj cjelini konstruiramo sve $S(2, 4, 28)$ dizajne s netrivialnim automorfizmima. Rezultati su već objavljeni u članku [58]. Prvo trebamo vidjeti koji prosti brojevi mogu biti redovi automorfizama $S(2, 4, 28)$ dizajna i odrediti fiksne strukture.

Propozicija 2.5 *Ako $S(2, 4, 28)$ dizajn ima automorfizam prostog reda p , onda je $p = 2, 3$ ili 7 .*

Dokaz. Slijedi iz Leme 2.2. □

Propozicija 2.6 *Automorfizam reda 7 dizajna $S(2, 4, 28)$ nema fiksnih točaka, niti pravaca.*

Dokaz. Ponovo koristimo Lemu 2.2. Fiksne točke ne postoje jer $v - 1 = 27$ i $v - k = 24$ nisu djeljivi sa 7. Fiksni pravci morali bi sadržati četiri fiksne točke. □

Propozicija 2.7 *Automorfizam reda 3 dizajna $S(2, 4, 28)$ fiksira jedan od sljedećih skupova točaka i pravaca.*

- (a) *Jedna točka i g pravaca kroz nju, za $g = 0, 3, 6$ ili 9 .*
- (b) *Četiri točke na pravcu i još dva pravca kroz svaku od fiksnih točaka.*

Dokaz. Kroz svaku fiksnu točku očito prolazi 0, 3, 6 ili 9 fiksnih pravaca. Prema Lemi 2.2, automorfizam ima jedinstvenu fiksnu točku, ili 4 fiksne točke na nekom pravcu ℓ . Prvi slučaj opisan je pod (a). U drugom slučaju kroz svaku od fiksnih točaka prolazi fiksni pravac ℓ i prema tome bar još dva fiksna pravca. Osam fiksnih pravaca i ℓ pokrivaju svih 28 točaka dizajna. Zato kroz svaku od 4 fiksne točke osim ℓ prolaze još točno dva fiksna pravca, kao što se tvrdi pod (b). □

Propozicija 2.8 *Automorfizam reda 2 dizajna $S(2, 4, 28)$ fiksira jedan od sljedećih skupova točaka i pravaca.*

- (a) *Sedam pravaca i f točaka na jednom od njih, za $f = 0, 2$ ili 4.*
- (b) *Četiri točke u općem položaju (nikoje tri kolinearne), šest spojnica fiksnih točaka i još tri pravca koji ne prolaze kroz fiksne točke.*
- (c) *Šest točaka, od kojih su četiri na pravcu; devet spojnica po dvije fiksne točke i još jedan pravac koji ne prolazi kroz fiksne točke.*

Fiksne strukture (b) i (c) prikazane su na Slici 2.



Slika 2: Fiksne strukture automorfizma reda 2 dizajna $S(2, 4, 28)$.

Dokaz. Osim oznaka iz Leme 2.4 koristimo \mathcal{B}_i za skup pravaca koji sadrže i fiksnih točaka, a \mathcal{B}'_0 i \mathcal{B}''_0 za skup fiksnih, odnosno nefiksnih pravaca iz \mathcal{B}_0 . Uvrštavanjem $v = 28$ u Lemu 2.4 dobivamo sljedeće formule.

$$\begin{aligned}
 b'_0 &= \frac{m(m-25)}{2} + 3n \\
 b''_0 &= 16m - 6n \\
 b_1 &= 8n - 16m \\
 b_2 &= m(26 - m) - 6n \\
 b_4 &= 63 + \frac{m(m-27)}{2} + n
 \end{aligned}$$

Ovi brojevi su nenegativni za devet parova $(m, n) \in \{1, \dots, 14\} \times \{1, \dots, 31\}$, navedenih u tablici:

R.br.	m	n	b'_0	b''_0	b_1	b_2	b_4	f	g
1	14	28	7	56	0	0	0	0	7
2	13	28	6	40	16	1	0	2	7
3	12	28	6	24	32	0	1	4	7
4	12	27	3	30	24	6	0	4	9
5	11	26	1	20	32	9	1	6	11
6	11	27	4	14	40	3	2	6	9
7	10	26	3	4	48	4	4	8	11
8	10	25	0	10	40	10	3	8	13
9	9	24	0	0	48	9	6	10	15

Prva tri retka odgovaraju fiksnim strukturama (a), četvrti redak strukturi (b), a peti strukturi (c). Treba dokazati da ostali reci opisuju nemoguće konfiguracije. U šestom retku imamo dva fiksna pravca sa po četiri fiksne točke. Oni se sijeku najviše u jednoj točki, pa bi trebali imati bar sedam fiksnih točaka. Međutim, u šestom retku je $f = 6$. Analogno, za tri ili više \mathcal{B}_4 -pravaca trebali bi bar 9 fiksnih točaka, a u sedmom i osmom retku imamo $f = 8$.

Na kraju razmotrimo incidencijsku strukturu sastavljenu od 10 fiksnih točaka i šest \mathcal{B}_4 -pravaca koja odgovara devetom retku tablice. Neka su stupnjevi točaka u toj strukturi r_1, \dots, r_{10} . Ukupan broj incidencija je 24, pa je $r_1 + \dots + r_{10} = 24$. Prebrojimo trojke (P, ℓ_1, ℓ_2) , gdje su ℓ_1 i ℓ_2 dva pravca kroz točku P :

$$\sum_{i=1}^{10} \binom{r_i}{2} = \sum_{i=1}^{10} \frac{r_i(r_i - 1)}{2}$$

Ova kvadratna funkcija uz uvjet $r_1 + \dots + r_{10} = 24$ poprima minimalnu vrijednost 16.8 za $r_1 = \dots = r_{10} = 2.4$. Prema tome, imamo bar 17 trojki. S druge strane, trojki ne može biti više od $\binom{6}{2} = 15$ jer se parovi pravaca sijeku najviše u jednoj točki. Time je dokazano da struktura opisana devetim retkom tablice nije moguća. □

Za konstrukciju dizajna sa zadanom grupom automorfizama koristimo poznatu metodu, koja se sastoji od tri koraka:

1. potpuna klasifikacija orbitnih matrica,
2. indeksiranje (transformacija orbitnih matrica u incidencijske matrice dizajna) i
3. provjera izomorfности dobivenih dizajna.

U prvom koraku koristimo program `orbmat.c`, zasnovan na Algoritmu 1.31. Za indeksiranje koristimo program `index1.c`, koji radi brže od verzije iz magistarskog rada [55]. U trećem koraku koristimo `incfilter.c`, bez većih promjena u odnosu na verziju iz [55]. Metoda je detaljno opisana u petom poglavlju magistarskog rada, a u dokazima idućih teorema ograničavamo se na kratak opis provedenih računa i pregled međurezultata.

Teorem 2.9 *Postoji točno 11 neizomorfnih $S(2, 4, 28)$ dizajna s automorfizmom reda 7.*

Dokaz. Prema Propoziciji 2.6 automorfizam reda 7 sastoji se isključivo od ciklusa duljine 7. Odgovarajuće orbitne matrice klasificirane su u Primjeru 1.50. Ima ih 7, od čega je 5 moguće indeksirati (korišten je program `index1.c`). Dobiva se ukupno 288 incidencijskih matrica $S(2, 4, 28)$ dizajna, a filtriranjem (pomoću programa `incfilter.c`) vidi se da među njima ima 11 neizomorfnih. □

A.E.Brouwer [19] navodi 8 kao broj $S(2, 4, 28)$ dizajna s automorfizmom reda 7. Usporedbom Tablice 7 s tablicom u [19, odjeljak C] zaključujemo da je propustio dva dizajna s punom grupom automorfizama reda 21 i jednog s punom grupom automorfizama reda 7.

Teorem 2.10 *Postoji 1978 dizajna $S(2, 4, 28)$ s automorfizmom reda 3.*

Dokaz. Prema Propoziciji 2.7 imamo pet mogućnosti za fiksne strukture automorfizma reda 3. Fiksnim strukturama odgovaraju različite orbitne matrice, klasificirane u Primjeru 1.51. Broj orbitnih matrica i neizomorfnih dizajna dobivenih indeksiranjem dan je u sljedećoj tablici (korišteni su programi `index1.c` i `incfilter.c`).

Tip automorfizma	Broj orb. matrica	Broj dizajna
(a), $g = 0$	13083	1635
(a), $g = 3$	9017	297
(a), $g = 6$	267	0
(a), $g = 9$	11	8
(b)	29	43

Jedan dizajn može imati više automorfizama reda 3 s različitim fiksnim strukturama. Zato ukupan broj dizajna ne dobivamo zbrajanjem brojeva u zadnjem stupcu tablice, nego je potrebno ponovo filtrirati sve konstruirane incidencijske matrice. Među njima ima ukupno 1978 neizomorfnih. □

Teorem 2.11 *Postoji 2590 dizajna $S(2, 4, 28)$ s automorfizmom reda 2.*

Dokaz. Automorfizam reda 2 također dopušta 5 mogućnosti za fiksne strukture (Propozicija 2.8). Odgovarajuće orbitne matrice klasificirane su u Primjeru 1.52. Rezultati klasifikacije i indeksiranja sažeto su prikazani u tablici:

Tip automorfizma	Broj orb. matrica	Broj dizajna
(a), $f = 0$	52281	121
(a), $f = 2$	58538	226
(a), $f = 4$	3513	788
(b)	28835	473
(c)	16259	1333

Ukupan broj dizajna s automorfizmom reda 2 utvrđen je filtriranjem svih konstruiranih incidencijskih matrica. □

Teorem 2.12 *Ukupan broj $S(2, 4, 28)$ dizajna s netrivialnom grupom automorfizama je 4466.*

Dokaz. Slijedi primjenom programa `incfilter.c` na dizajne konstruirane u prethodna tri teorema. □

U Tablici 7 dana je distribucija $S(2, 4, 28)$ dizajna s netrivialnim automorfizmima prema redu pune grupe automorfizama. Ovdje se još bavimo poddizajnama konstruiranih $S(2, 4, 28)$ dizajna. U članku [58] osim toga razmatramo rješivost i binarne kodove razapete incidencijskim vektorima pravaca.

Propozicija 2.13 *Pravi poddizajn $S(2, 4, 28)$ dizajna ima parametre $S(2, 3, v)$, za $v = 7$ ili 9.*

Aut	Br. diz.	Aut	Br. diz.	Aut	Br. diz.	Aut	Br. diz.
12096	1	48	12	18	1	6	60
1512	1	42	1	16	10	4	374
216	1	32	2	12	12	3	1849
192	2	27	1	9	18	2	2028
72	1	24	12	8	71		
64	1	21	6	7	2		

Tablica 7: Distribucija $S(2, 4, 28)$ dizajna prema redu pune grupe automorfizama.

Dokaz. Prema Lemi 2.1, dizajni $S(2, 4, 28)$ ne mogu imati prave $S(2, 4, v)$ poddizajne. Dolaze u obzir jedino $S(2, 3, v)$ poddizajni, za koje iz [55, Lema 2.6] dobivamo ocjene $v \leq 19$ i $v^2 - 28v + 189 \geq 0$. Nejednakosti zadovoljavaju tri dopustive vrijednosti, $v = 7, 9$ i 19 . Preostaje dokazati da $S(2, 3, 19)$ poddizajni nisu mogući. Za parametre $S(2, 4, 28)$ i $S(2, 3, 19)$ broj pravaca kroz danu točku je $r = 9$. Zato svi pravci kroz neku točku poddizajna pripadaju poddizajnu i sadrže ukupno tri točke poddizajna. Promotrimo li pravce kroz točku izvan poddizajna, dobivamo particiju točaka poddizajna na tročlane podskupove. To nije moguće jer 19 nije djeljiv s 3 . \square

Pomoću programa `subsearch.c` prebrojili smo koliko od 4466 konstruiranih dizajna zaista ima poddizajne. Točno 39 ima obje vrste poddizajna, 1511 ima samo $S(2, 3, 7)$ poddizajne, a 89 samo $S(2, 3, 9)$ poddizajne. M.Meszka i A.Rosa [74] bave se problemom ulaganja $S(2, 3, 7)$ i $S(2, 3, 9)$ dizajna u $S(2, 4, v)$ dizajne. Koristeći dizajne iz Teorema 2.12 (točnije, iz [58, Teorem 3.4]) dokazali su da je u prvom slučaju ulaganje moguće za sve dopustive v , a u drugom eventualno uz jedan izuzetak. Primjer za taj otvoreni slučaj pronađen je u idućoj cjelini disertacije.

A.E.Brouwer [19] bavi se problemom ulaganja unitala $S(2, 4, 28)$ u projekтивne ravnine reda 9. Konstruirao je ukupno 138 primjera, od kojih se 12 ulažu (među njima je, naravno, klasični $S(2, 4, 28)$). Problem su potpuno riješili T.Pentilla i G.F.Royle [82]. Pokazali su da ima ukupno 18 unitala u projektivnim ravninama reda 9: dva u $PG(2, 9)$, četiri u Hallovoj ravnini i isto toliko u dualnoj, te osam u Hughesovoj ravnini reda 9. Svih 18 imaju netrivialne grupe automorfizama (redovi su navedeni u [82, Tablica 5]).

A.Betten, D.Betten i V.D.Tonchev [12] konstruirali su 909 dizajna $S(2, 4, 28)$ razmatrajući pridružene dualne kodove i njima definirane taktičke dekompozicije. Među tim dizajnama 187 ima trivijalnu punu grupu automorfizama. Zaključujemo da postoji barem 4653 neizomorfni $S(2, 4, 28)$ dizajna. Brouwer [19] je također našao 26 primjera s trivijalnom grupom automorfizama, ali nije jasno jesu li izomorfni onima iz [12]. Ukupan broj $S(2, 4, 28)$ dizajna bez ikakvih ograničenja za sada je nepoznat.

2.3 Neki novi $S(2, 4, 37)$ dizajni

U ovoj cjelini proučavamo automorfizme $S(2, 4, 37)$ dizajna i koristimo ih za konstrukciju velikog broja novih primjera. Rezultati su također izloženi u [60]. Iduće tri propozicije slijede direktno iz Leme 2.2.

Propozicija 2.14 *Ako $S(2, 4, 37)$ dizajn ima automorfizam prostog reda p , onda je $p = 2, 3, 11$ ili 37 .*

Propozicija 2.15 Automorfizam reda 37 dizajna $S(2, 4, 37)$ djeluje bez fiksnih točaka i pravaca.

Propozicija 2.16 Automorfizam reda 11 dizajna $S(2, 4, 37)$ fiksira četiri točke na jedinstvenom fiksnom pravcu.

Fiksne strukture automorfizama reda 3 također možemo odrediti pomoću Leme 2.2, a za automorfizme reda 2 koristimo Lemu 2.4.

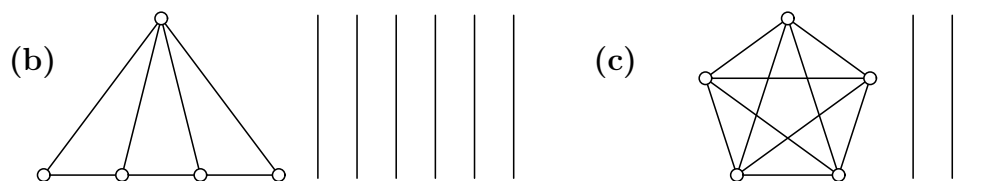
Propozicija 2.17 Automorfizam reda 3 dizajna $S(2, 4, 37)$ fiksira jedan od sljedećih skupova točaka i pravaca.

- (a) Jedna točka i g pravaca kroz nju, za $g = 0, 3, 6, 9$ ili 12 .
- (b) Četiri točke na pravcu i još dva pravca kroz svaku od fiksnih točaka.
- (c) Četiri točke na pravcu i još pet pravaca kroz jednu od fiksnih točaka, a dva pravca kroz ostale fiksne točke.

Dokaz. Broj fiksnih točaka (1 ili 4) slijedi iz Leme 2.2. Broj fiksnih pravaca kroz fiksnu točku djeljiv je s 3, pa (a) opisuje sve fiksne strukture s jednom fiksnom točkom. Iz istog razloga u drugom slučaju, kad imamo četiri fiksne točke na fiksnom pravcu ℓ , kroz svaku od točaka prolaze bar još dva fiksna pravca. Jedanaest fiksnih pravaca i ℓ pokrivaju svih 37 točaka. Zato su strukturama (b) i (c) iscrpljene sve mogućnosti u drugom slučaju. \square

Propozicija 2.18 Automorfizam reda 2 dizajna $S(2, 4, 37)$ fiksira jedan od sljedećih skupova točaka i pravaca.

- (a) Jedna točka i devet pravaca bez incidencija.
- (b) Četiri točke na pravcu i još jedna točka izvan tog pravca. Spojnice fiksnih točaka i dodatnih šest pravaca bez incidencija.
- (c) Pet točaka u općem položaju (nikoje tri kolinearne), deset spojnica fiksnih točaka i još tri pravca bez incidencija.
- (d) Jedinstveni linearni prostor s 13 točaka i 23 pravaca, od kojih su 11 incidentni s četiri točke, a preostalih 12 s dvije točke.



Slika 3: Fiksne strukture automorfizma reda 2 dizajna $S(2, 4, 37)$.

Fiksne strukture (b) i (c) prikazane su na Slici 3. Linearni prostor (d) dobiva se od projektivne ravnine reda 3 tako da se dva pravca zamijene dvočlanim podskupovima točaka.

Dokaz. Koristimo iste oznake kao u dokazu Propozicije 2.8. Uvrštavanjem $v = 37$ u Lemu 2.4 slijedi

$$\begin{aligned}
 b'_0 &= \frac{m(m-34)}{2} + 2n \\
 b''_0 &= 22m - 6n \\
 b_1 &= 8n - 22m \\
 b_2 &= m(35-m) - 6n \\
 b_4 &= 111 + \frac{m(m-36)}{2} + n
 \end{aligned}$$

Sedam parova $(m, n) \in \{1, \dots, 18\} \times \{1, \dots, 55\}$ daju nenegativne vrijednosti za b_i -ove:

R.br.	m	n	b'_0	b''_0	b_1	b_2	b_4	f	g
1	18	51	9	90	12	0	0	1	9
2	16	50	6	52	48	4	1	5	11
3	16	49	3	58	40	10	0	5	13
4	14	49	7	14	84	0	6	9	13
5	14	48	4	20	76	6	5	9	15
6	14	47	1	26	68	12	4	9	17
7	12	44	0	0	88	12	11	13	23

Prva tri retka tablice odgovaraju fiksnim strukturama (a), (b) i (c). Strukture opisane četvrtim, petim i šestim retkom nisu moguće. Imaju devet točaka ($f = 9$), što to je premalo za četiri ili više \mathcal{B}_4 -pravca ($b_4 \geq 4$). Sedmi redak odgovara linearnom prostoru (d). Jedinstvenost takvog linearnog prostora utvrđena je u Primjeru 1.34. □

U knjizi Handbook of combinatorial designs [24, Tablica I.1.28] navodi se da su poznata tri $S(2, 4, 37)$ dizajna. Daljnji primjeri konstruirani su u radovima [34], [63] i [74]. Dva od tri primjera iz [24] su ciklički, i to su jedini $S(2, 4, 37)$ dizajni s automorfizmom reda 37. Dobivaju se od sljedećih diferencijskih familija u grupi \mathbb{Z}_{37} :

$$D_1 = \{0, 1, 3, 24\} \quad D_2 = \{0, 4, 9, 15\} \quad D_3 = \{0, 7, 17, 25\}$$

$$D_1 = \{0, 1, 3, 24\} \quad D_2 = \{0, 4, 26, 32\} \quad D_3 = \{0, 7, 17, 25\}$$

Više o diferencijskim familijama može se pročitati u četvrtom poglavlju magistrarskog rada [55].

M.Meszka i A.Rosa su u sklopu rada [74] klasificirali $S(2, 4, 37)$ dizajne s automorfizmom reda 11, ali o rezultatima ne navode nikakve detalje. Ovdje ponavljamo klasifikaciju.

Teorem 2.19 *Postoji 284 dizajna $S(2, 4, 37)$ s automorfizmom reda 11.*

Dokaz. Iz Propozicije 2.16 slijedi format orbitnih matrica i marginalni vektori $\nu = (1, 1, 1, 1, 11, 11, 11)$ i $\beta = (1, 11, \dots, 11)$. Pomoću programa `orbmat.c` ustanovili smo da postoji samo jedna takva orbitna matrica:

$$\begin{bmatrix} 1 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 3 & 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 1 & 1 & 1 & 0 & 3 & 1 & 2 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 3 & 2 & 2 & 0 \end{bmatrix}$$

Indeksiranjem i filtriranjem dobiva se 284 neizomorfnih $S(2, 4, 37)$ dizajna. \square

Orbitnih matrica koje odgovaraju automorfizmima reda 2 i 3 ima previše za potpunu klasifikaciju. Ograničavamo se na slučaj (a), $g = 12$ iz Propozicije 2.17 i slučaj (d) iz Propozicije 2.18, koji su povezani sa $(12, 4, 3)$ i $(12, 3, 2)$ blok dizajnima.

Automorfizam reda 3 dizajna $S(2, 4, 37)$ koji fiksira jednu točku i sve pravce kroz nju definira orbitnu matricu sljedećeg oblika:

$$\begin{bmatrix} j_{12}^t & 0_{33}^t \\ I_{12} & M \end{bmatrix}$$

Ovdje su 0_n i j_n oznake za n -vektor popunjen nulama, odnosno jedinicama, a I_n je jedinična matrica reda n . Koristeći svojstva iz Definicije 1.11 može

se dokazati da je M incidencijska matrica $(12, 4, 3)$ blok dizajna, tj. 12×33 matrica nad $\{0, 1\}$ koja zadovoljava $M \cdot M^t = 8I_{12} + 3J_{12}$ i $M^t \cdot j_{12} = 4j_{33}$ (J_n označava kvadratnu matricu reda n popunjenu jedinicama). Prema [24, Tablica I.1.28], postoji više od 17 milijuna neizomorfnih $(12, 4, 3)$ dizajna. Točan broj nije poznat, ali i to je previše za indeksiranje svih odgovarajućih orbitnih matrica. Indeksirali smo manji broj orbitnih matrica, dobivenih na nekoliko načina.

Najprije smo promatrali orbitne matrice koje odgovaraju $(12, 4, 3)$ blok dizajnim s nekim dodatnim svojstvima. L.B.Morales i C.Velarde [78] klasificirali su rješive $(12, 4, 3)$ dizajne. Ima ih pet, a indeksirati je moguće orbitne matrice dobivene od prva tri (prema numeraciji u [78]). Dobiva se devet $S(2, 4, 37)$ dizajna, od kojih jedan ima automorfizam reda 11 i već je konstruiran u Teoremu 2.19.

Prvi i peti rješivi $(12, 4, 3)$ dizajn imaju automorfizam reda 3 bez fiksnih točaka i pravaca. Konstruirali smo sve takve blok dizajne i ispitali koji među njima generiraju Steinerove 2-dizajne $S(2, 4, 37)$.

Propozicija 2.20 *Postoji točno 1197 blok dizajna $(12, 4, 3)$ koji imaju automorfizam reda 3 bez fiksnih točaka i pravaca.*

Dokaz. Pomoću programa `orbmat.c` brzo se dobiva 11 orbitnih matrica. Sve osim jedne moguće je indeksirati (korišten je program `fpindex.c`). Nakon filtriranja ostaje ukupno 1197 neizomorfnih dizajna. □

Od 1197 orbitnih matrica koje odgovaraju blok dizajnim iz prethodne propozicije, samo je 182 moguće indeksirati. Dobiva se 217 neizomorfnih $S(2, 4, 37)$ dizajna, od kojih su šest već konstruirani (pomoću prvog rješivog $(12, 4, 3)$ dizajna). Zanimljivo je da većina konstruiranih dizajna (214 od 217) ima punu grupu automorfizama reda 9 ili više, iako pri indeksiranju nismo uzimali u obzir automorfizme orbitnih matrica.

Na kraju smo pomoću programa `tabubibd.c` iz trećeg poglavlja disertacije konstruirali otprilike 500000 blok dizajna $(12, 4, 3)$, pretežno s trivijalnom punom grupom automorfizama. Oko 1700 odgovarajućih orbitnih matrica bilo je moguće indeksirati i dobili smo 1745 neizomorfnih $S(2, 4, 37)$ dizajna. Svi imaju punu grupu automorfizama reda 3 i nijedan nije izomorfan prethodno konstruiranim dizajnim.

Bavili smo se isključivo automorfizmima reda 3 koji fiksiraju jednu točku i 12 pravaca, ali neki od 2250 do sada konstruiranih $S(2, 4, 37)$ dizajna (uključujući cikličke) imaju automorfizme reda 3 s drugim fiksnim strukturama. Osim tipa (a), $g = 12$ javljaju se automorfizmi tipa (a), $g = 0$ i tipa (b). Ostali tipovi automorfizama iz Propozicije 2.17 nisu se pojavili.

Za automorfizme reda 2 najzanimljiviji je slučaj (d) iz Propozicije 2.18. D.L.Kreher, D.R.Stinson i L.Zhu dokazali su u [63] ovaj teorem.

Teorem 2.21 *Neka je f broj fiksnih točaka automorfizma prostog reda p Steinerovog 2-dizajna $S(2, k, v)$. Tada vrijedi*

$$f \leq \begin{cases} r + k - p - 1, & \text{za } p \leq k - 1, \\ r - \frac{p-1}{k-1}, & \text{za } p \geq k. \end{cases}$$

Ako se nejednakost dostiže, dizajn se naziva p -MFP(v, k) (prema engleskom “maximum fixed point”). Dizajni $S(2, 4, 37)$ s involutornim automorfizmom tipa (d) su 2-MFP(37, 4). Primjer takvog dizajna konstruirali su Kreher, Stinson i Zhu u [63]. Ukratko ćemo opisati njihovu konstrukciju i usporediti je s konstrukcijom pomoću orbitnih matrica.

Nefiksne točke i pravci 2-MFP(37, 4) dizajna čine strukturu GDD(3, 2, 24) [55, Definicija 2.25]. Radi se o incidencijskoj strukturi ekvivalentnoj $S(2, 3, 25)$ dizajnu iz kojeg je izbačena jedna točka i pravci kroz nju. U [63] prvo se konstruiraju takve strukture, a zatim se dodaju fiksne točke i pravci (tj. linearni prostor iz Primjera 1.34). Nedostatak ovog pristupa je što dijelovi koji se spajaju moraju biti usklađeni da bi tvorili $S(2, 4, 37)$ dizajn. Nije moguće nadopuniti svaki GDD(3, 2, 24), nego on mora zadovoljavati komplicirane dodatne uvjete (precizan opis dan je u [63]).

Naš pristup preko orbitnih matrica razlikuje se u dva aspekta. Kao prvo, nefiksni dio orbitne matrice sadrži samo informaciju o incidencijama orbita duljine dva, ne o incidencijama pojedinačnih točaka i pravaca (kao u strukturi GDD(3, 2, 24)). U ovom slučaju nefiksni dio orbitne matrice je incidencijska matrica (12, 3, 2) blok dizajna. Tek nakon indeksiranja dobivamo incidencijsku matricu strukture GDD(3, 2, 24). Druga razlika je što orbitne matrice ne konstruiramo spajanjem potpunih (12, 3, 2) dizajna s fiksnom strukturom (d), nego ih izgrađujemo postepeno, redak po redak. Koristimo program `orbmat.c`, koji u svakom koraku uzima u obzir potrebne veze između fiksnog i nefiksnog dijela orbitne matrice.

P.R.J.Östergård [81] potpuno je klasificirao (12, 3, 2) blok dizajne. Postoji točno 242 995 846 dizajna, od kojih 88 616 310 nema višestruke blokove. Veza s orbitnim matricama koje proučavamo nije jednostavna. Neke od incidencijskih matrica (12, 3, 2) blok dizajna ne mogu se proširiti do orbitne matrice, a druge se proširuju na više neekvivalentnih načina. Nismo uspjeli potpuno klasificirati orbitne matrice, ali smo pomoću programa `orbmat.c` brzo dobili više od 5000 neizomorfni primjera. Orbitne matrice čiji nefiksni dio odgovara (12, 3, 2) dizajnu s višestrukim blokovima nije moguće indeksirati. S druge strane, sve ispitane orbitne matrice kojima odgovara (12, 3, 2)

Aut	Br. diz.	Aut	Br. diz.	Aut	Br. diz.	Aut	Br. diz.
111	1	33	4	11	280	2	49152
54	4	27	2	9	203		
37	1	18	7	3	1748		

Tablica 8: Distribucija konstruiranih $S(2, 4, 37)$ dizajna prema redu pune grupe automorfizama.

dizajn bez višestrukih blokova bilo je moguće **indeksirati** i dobili smo uvijek 2^{12} ili 2^{13} dizajna $S(2, 4, 37)$. Većina od preko 12 milijuna konstruiranih $S(2, 4, 37)$ dizajna vjerojatno su neizomorfni, ali provjera bi zahtijevala previše procesorskog vremena i memorije. Filtrirali smo **49152** dizajna dobivenih indeksiranjem prvih 12 konstruiranih orbitnih matrica. Među njima nema izomorfni i svi imaju punu grupu automorfizama reda 2, pa ne mogu biti izomorfni niti prethodno konstruiranim dizajnima. Neki od dizajna s automorfizmima reda 3 ili 11 također imaju involutorne automorfizme. Oni su tipa (a) i (c), a tip (b) iz Propozicije 2.18 se ne pojavljuje.

Primjeri konstruirani u ovoj cjelini daju novu ocjenu za broj neizomorfnih $S(2, 4, 37)$ dizajna.

Propozicija 2.22 *Postoji barem 51402 Steinerovih 2-dizajna $S(2, 4, 37)$.*

Međutim, točan broj očito je znatno veći. Distribucija konstruiranih dizajna prema redu pune grupe automorfizama dana je u Tablici 8. Proučit ćemo njihove poddizajne i skoro-rješivost.

Parametri $S(2, 4, 37)$ ne zadovoljavaju nuždan uvjet za rješivost, ali zadovoljavaju za skoro-rješivost. Dizajn je *skoro-rješiv* ako se izbacivanjem jedne točke i pravaca kroz nju dobiva rješiva incidencijska struktura [55, Definicija 2.20]. Pomoću programa **nrsearch.c** ustanovili smo da je točno 10 od 51402 konstruiranih dizajna skoro-rješivo. Među njima su **devet** $S(2, 4, 37)$ dizajna dobivenih od rješivih $(12, 4, 3)$ blok dizajna.

Propozicija 2.23 *Pravi poddizajn $S(2, 4, 37)$ dizajna ima parametre $S(2, 3, v)$, za $v = 7, 9$ ili 13.*

Dokaz. Iz Leme 2.1 u disertaciji i iz Leme 2.6 u [55] slijedi da su jedine mogućnosti za parametre poddizajna $S(2, 3, v)$, $v = 7, 9, 13, 15$ i 25. Poddizajni $S(2, 3, 15)$ nisu mogući zbog Leme 16 u [74]. U prvom slučaju te leme tvrdi se da je nuždan uvjet za postojanje $S(2, 3, 24t + 15)$ poddizajna u $S(2, 4, 36t + 25 + 12s)$ dizajnu $s \geq 0$ i $12t^2 + (4 - 24s)t + 12s^2 - 14s \geq 3$. Za $t = 0$, $s = 1$ dobivamo naše parametre, a uvjet nije zadovoljen. Za parametre $S(2, 3, 25)$ svih 12 pravaca kroz točku poddizajna pripada poddizajnu. Prema

tome, pravci kroz točku izvan poddizajna sadrže 0 ili 3 točke poddizajna, a to nije moguće jer 25 nije djeljiv s 3. □

M.Meszka i A.Rosa [74] definiraju *spektar ulaganja* $E(v)$ kao skup svih w za koje postoji $S(2, 4, w)$ dizajn sa $S(2, 3, v)$ poddizajnom. Dokazali su da je $E(7) = \{w \mid w \equiv 1, 4 \pmod{12}, w \geq 25\}$, a jedini slučaj za $E(9)$ koji nisu riješili je $w = 37$. Potraga za poddizajnama naših 51402 dizajna (pomoću programa [subsearch.c](#)) pokazala je da 84 ima obje vrste poddizajna, 49595 ima samo $S(2, 3, 7)$ poddizajne, a 160 samo $S(2, 3, 9)$ poddizajne. Jedan primjer dobiva se razvojem sljedećih blokova nad \mathbb{Z}_9 .

$$\begin{array}{cccc} \{\infty, a_0, a_3, a_6\}, & \{\infty, b_0, b_3, b_6\}, & \{\infty, c_0, c_3, c_6\}, & \{\infty, d_0, d_3, d_6\}, \\ \{a_0, a_1, b_3, c_0\}, & \{a_0, a_5, b_6, c_6\}, & \{a_0, a_7, d_0, d_1\}, & \{a_0, b_0, b_4, c_3\}, \\ \{a_1, c_3, c_8, d_0\}, & \{a_2, c_6, c_7, d_0\}, & \{a_3, b_8, d_0, d_7\}, & \{a_4, b_2, b_3, d_0\}, \\ \{b_0, c_1, d_0, d_5\}, & \{b_5, b_7, c_0, d_0\}, & \{b_6, c_2, c_4, d_0\} & \end{array}$$

Točke $\{a_0, a_3, a_6, b_0, b_3, b_6, c_0, c_3, c_6\}$ tvore $S(2, 3, 9)$ poddizajn. Prema tome, [74, Teorem 21] može se osnažiti:

Teorem 2.24 *Steinerov 2-dizajn $S(2, 4, w)$ s poddizajnom $S(2, 3, 9)$ postoji ako i samo ako je $w = 13$, ili je $w \geq 28$, $w \equiv 1, 4 \pmod{12}$.*

Niti jedan od 51402 konstruiranih $S(2, 4, 37)$ dizajna nema $S(2, 3, 13)$ poddizajn. Postojanje takvog poddizajna za sada je otvoreno, i to je najmanji otvoren slučaj u spektru ulaganja $E(13)$.

2.4 Još neki rezultati o Steinerovim 2-dizajnama

U ovoj cjelini nadopunjujemo nekoliko rezultata iz magistarskog rada [55] i primjenjujemo metodu konstrukcije pomoću orbitnih matrica na još neke Steinerove 2-dizajne. U [55, Propozicija 5.35] dokazano je da su jedini kandidati za proste redove automorfizama $S(2, 6, 61)$ dizajna $p = 2, 3$ i 5 . U Propoziciji 5.36 dokazano je da automorfizam reda 5 fiksira jednu točku i 2, 7 ili 12 pravaca kroz nju. Iduća propozicija eliminira slučaj 12 fiksnih pravaca.

Propozicija 2.25 *Automorfizam reda 5 Steinerovog 2-dizajna $S(2, 6, 61)$ fiksira jednu točku i 2 ili 7 pravaca kroz nju.*

Dokaz. U slučaju 12 fiksnih pravaca orbitne matrice su sljedećeg oblika:

$$\begin{bmatrix} j_{12}^t & 0_{22}^t \\ I_{12} & M \end{bmatrix}$$

Pritom je M incidencijska matrica $(12, 6, 5)$ blok dizajna, tj. 12×22 matrica nad $\{0, 1\}$ sa svojstvima $M \cdot M^t = 6I + 5J$, $M^t \cdot j_{12} = 6j_{22}$. Takve orbitne matrice klasificirali smo pomoću progama `orbmat.c`. Dobiveni broj, **11603**, slaže se s brojem $(12, 6, 5)$ dizajna u [24, Tablica I.1.28]. **Indeksiranjem** smo ustanovili da niti jednu orbitnu matricu nije moguće transformirati u incidencijsku matricu $S(2, 6, 61)$ dizajna. Zaključujemo da automorfizmi s 12 fiksnih pravaca nisu mogući. □

U magistarskom radu nismo mogli provesti indeksiranje **11603** orbitnih matrica [55, Napomena 5.37]. Napredak je omogućen ubrzanjem programa `index1.c`. To nam je također omogućilo eliminaciju automorfizama reda 17 dizajna $S(2, 7, 85)$ (vidjeti [55, Napomena 5.40]).

Propozicija 2.26 *Ako Steinerov 2-dizajn $S(2, 7, 85)$ ima automorfizam prostog reda p , onda je $p = 2, 3, 5$ ili 7 .*

Dokaz. U [55, Propozicija 5.39] dokazano je $p \in \{2, 3, 5, 7, 17\}$. Ovdje dokazujemo $p \neq 17$. Automorfizam reda 17 djeluje bez fiksnih točaka i pravaca (Lema 2.2). Odgovarajuće orbitne matrice su formata 5×10 . Pomoću programa `orbmat.c` brzo se vidi da ih do na izomorfizam ima **313**. Nakon dužeg računa pokazalo se da niti jednu orbitnu matricu nije moguće **indeksirati** do incidencijske matrice $S(2, 7, 85)$ dizajna. □

Slijedi nekoliko rezultata za parametre koji nisu razmatrani u magistarskom radu.

Propozicija 2.27 *Ako Steinerov 2-dizajn $S(2, 5, 45)$ ima automorfizam prostog reda p , onda je $p = 2, 3$ ili 5 .*

Dokaz. Iz Leme 2.2 direktno slijedi $p \in \{2, 3, 5, 11\}$. Automorfizam reda 11 fiksira bi samo jednu točku. Postoji **13** odgovarajućih orbitnih matrica, ali nije ih moguće **indeksirati**. □

Teorem 2.28 *Automorfizam reda 5 Steinerovog 2-dizajna $S(2, 4, 45)$ nema fiksnih točaka i fiksira 4 ili 9 pravaca. Postoji samo **jedan** $S(2, 4, 45)$ dizajn s automorfizmom reda 5 koji fiksira 4 pravca, a **dva** s automorfizmom reda 5 koji fiksira 9 pravaca.*

Dokaz. Prema Lemi 2.2 automorfizam reda 5 mogao bi djelovati bez fiksnih točaka ili s 5 fiksnih točaka na pravcu. U jednom i u drugom slučaju fiksni

pravci se ne sijeku i ima ih 4 ili 9. Ima ih barem toliko jer je $b = 99 \equiv 4 \pmod{5}$, a ne može ih biti više jer 9 paralelnih pravaca pokriva svih 45 točaka. Prema tome, treba razmotriti četiri slučaja. Orbitne matrice su klasificirane u Primjeru 1.53.

1. *Četiri fiksna pravca bez fiksni točaka.* Postoji 574985 orbitnih matrica, ali samo je jednu moguće indeksirati. Dobiva se jedan $S(2, 5, 45)$ dizajn.
2. *Četiri fiksna pravca i pet fiksni točaka.* Orbitna matrica je jedinstvena i ne može se indeksirati.
3. *Devet fiksni pravaca bez fiksni točaka.* Postoji 11 orbitnih matrica od kojih je dvije moguće indeksirati. Dobivaju se dva $S(2, 5, 45)$ dizajna.
4. *Devet fiksni pravaca i pet fiksni točaka.* Orbitna matrica je jedinstvena i ne može se indeksirati.

□

Dizajni iz prethodnog teorema imaju pune grupe automorfizama reda 160, 40 i 360 (redom kojim se spominju u dokazu). Ova tri dizajna vjerojatno su među 16 poznatih $S(2, 4, 45)$ dizajna iz [24, Tablica I.1.28]. Daljnje primjere s automorfizmom reda 2 koji fiksira maksimalan broj točaka konstruirao je C.J.Colbourn [23] (prema oznaci iz [63] radi se o 2-MFP(45, 5)).

Propozicija 2.29 *Ako Steinerov 2-dizajn $S(2, 6, 66)$ ima automorfizam prostog reda p , onda je $p = 2, 3, 5, 11$ ili 13.*

Dokaz. Slijedi direktno iz Leme 2.2.

□

Teorem 2.30 *Postoje točno tri dizajna $S(2, 6, 66)$ s automorfizmom reda 13.*

Dokaz. Automorfizam reda 13 fiksira samo jednu točku. Pomoću programa `orbmat.c` pronađeno je 197 orbitnih matrica, od čega je dvije moguće indeksirati. Od prve se dobiva jedan dizajn, a od druge dva.

□

Tri dizajna iz prethodnog teorema imaju punu grupu automorfizama reda 39. U [24, Tablica I.1.28] spominje se samo jedan $S(2, 6, 66)$ dizajn, kojeg je našao R.H.F.Denniston [29].

2.5 TSC prostori

Rezultati u ovoj cjelini prethodno su izloženi u radu s J.Šiftarom [61]. TSC prostori su konačni linearni prostori čiji se skup pravaca može rastaviti na dva podskupa, od kojih svaki čini simetričnu konfiguraciju (Definicija 1.8). Duljine pravaca u tim konfiguracijama (k i l) jednoznačno određuju ukupan broj točaka i pravaca.

Propozicija 2.31 *Broj točaka TSC(k, l) prostora je $v = k(k-1) + l(l-1) + 1$, a broj pravaca dvostruko veći, $b = 2v$.*

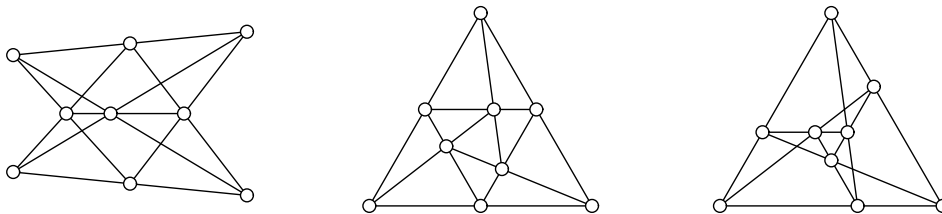
Dokaz. Za danu točku p_0 prebrojimo parove (L, p) , gdje je L pravac kroz p_0 , a $p \neq p_0$ točka na L . Točke p i p_0 jednoznačno određuju pravac, pa parova ima $v - 1$. S druge strane, kroz p_0 prolazi k pravaca duljine k i l pravaca duljine l , pa je broj parova $k(k-1) + l(l-1)$. Izjednačavanjem slijedi izraz za broj točaka. Broj pravaca je dvostruko veći jer pravci čine dvije simetrične konfiguracije s v točaka. □

Najmanji netrivialni primjer TSC prostora ima parametre $(2, 3)$. Dobiva se od (9_3) konfiguracije dodavanjem pravca duljine 2 za svaki par točaka koje nisu spojene pravcem konfiguracije. Na isti način može se nadopuniti simetrična (v_l) konfiguracija, $v = l^2 - l + 3$, do TSC($2, l$) prostora.

Propozicija 2.32 *Linearni prostori TSC($2, l$) ekvivalentni su simetričnim konfiguracijama deficijencije $d = 2$.*

Dokaz. Deficijencija (v_r, b_k) konfiguracije je $d = v - r(k-1) - 1$. Za simetrične konfiguracije ($r = k = l$) uvjet $d = 2$ ekvivalentan je sa $v = l^2 - l + 3$. □

Poznato je da osim Papusove konfiguracije postoje još točno dvije simetrične (9_3) konfiguracije (Slika 4). Postoje točno četiri (15_4) konfiguracije [10], i prema tome isto toliko TSC($2, 4$) prostora. Nije nam poznat točan broj (23_5)



Slika 4: Simetrične konfiguracije (9_3) .

konfiguracija, ali one se mogu konstruirati pomoću tabu search algoritma iz [trećeg poglavlja](#) (Primjer 3.6). Za $l \geq 6$ taj pristup ne daje rezultate, a prema [24, Tablica IV.6.10] pitanje egzistencije (33_6) konfiguracija je otvoreno.

Ako parametri (k, l) zadovoljavaju $2 < k < l$, kažemo da se radi o *pravom* TSC prostoru. Najmanji slučaj, TSC(3, 4), potpuno je klasificiran u Primjeru 1.36. Postoji točno 56 takvih linearnih prostora i njihova svojstva su navedena u Tablici 9. Tablica sadrži red pune grupe automorfizama ($|\text{Aut}|$), broj potpunih četverovrha sastavljenih od pravaca duljine četiri (4-Q), ukupan broj potpunih četverovrha (Q) i maksimalan broj paralelnih pravaca duljine tri i četiri (3-P i 4-P).

Za veće parametre nije bilo moguće provesti potpunu klasifikaciju, a ni pristup pomoću tabu search algoritma nije dao rezultate. Primjere konstruiramo uz pretpostavku djelovanja određenih grupa automorfizama. Prvo promatramo slučaj u kojem grupa automorfizama djeluje regularno na točke TSC prostora. Takve incidencijske strukture konstruiraju se pomoću diferencijskih familija. Osnovne definicije i neki rezultati za Steinerove 2-dizajne navedeni su u četvrtom poglavlju magistarskog rada [55]. Ovdje prilagođavamo pojam diferencijske familije TSC prostorima.

Definicija 2.33 *Neka je G aditivno zapisana grupa i $K, L \subseteq G$ dva njezina podskupa sa $k = |K|$ i $l = |L|$ elemenata. Za $\{K, L\}$ kažemo da je (k, l) -diferencijska familija u G , ako vrijedi:*

- (1) K i L imaju trivijalne stabilizatore i nisu ekvivalentni pod djelovanjem grupe G lijevim translacijama;
- (2) svaki element $g \in G \setminus \{0\}$ može se na jedinstven način prikazati kao $g = (-x) + y$, pri čemu su $x, y \in K$ ili $x, y \in L$.

Propozicija 2.34 *Ako imamo (k, l) -diferencijsku familiju $\{K, L\}$ u grupi G , onda je $\text{dev}\{K, L\} = \{g + K \mid g \in G\} \cup \{g + L \mid g \in G\}$ TSC prostor za (k, l) na kojem G djeluje kao grupa automorfizama regularno na točke.*

Dokaz. Skup pravaca $\text{dev}\{K, L\}$ podijeljen je na skup lijevih translata od K i skup lijevih translata od L . Ta dva skupa su disjunktni zbog pretpostavke da K i L nisu ekvivalentni pod lijevim translacijama.

Promotrimo proizvoljnu točku $a \in G$. Kroz a prolazi translacija od K ako i samo ako postoji $g \in G$ takav da je $a \in g + K$, tj. $(-g) + a \in K$. Vidimo da je to ispunjeno točno za k elemenata g , a njima odgovara k različitih pravaca u $\text{dev}\{K, L\}$ jer K ima trivijalan stabilizator. Analogno se vidi da kroz a prolazi točno l lijevih translata od L .

Br.	Aut	4-Q	Q	3-P	4-P	Br.	Aut	4-Q	Q	3-P	4-P
1	57	19	99	4	3	29	1	29	108	5	4
2	57	19	93	4	3	30	1	29	91	6	3
3	12	22	114	5	3	31	1	28	97	6	3
4	12	22	107	6	3	32	1	28	94	6	4
5	12	8	101	5	4	33	1	27	102	6	4
6	4	30	116	6	3	34	1	27	100	6	3
7	4	24	102	6	3	35	1	27	98	6	4
8	4	24	95	6	3	36	1	27	95	6	3
9	4	22	102	6	3	37	1	27	94	5	3
10	4	10	107	5	3	38	1	27	92	6	4
11	3	32	111	6	4	39	1	27	89	6	3
12	3	31	98	6	3	40	1	26	104	6	4
13	3	29	106	6	4	41	1	26	98	6	4
14	3	28	104	5	4	42	1	26	98	6	3
15	3	28	83	5	3	43	1	26	96	5	3
16	3	26	116	6	4	44	1	26	95	6	3
17	3	26	101	5	3	45	1	26	92	6	3
18	3	26	91	6	4	46	1	25	108	5	4
19	3	25	105	6	4	47	1	25	102	6	4
20	3	25	101	6	4	48	1	25	97	6	4
21	3	25	101	6	3	49	1	25	97	5	4
22	3	25	94	5	3	50	1	25	94	5	4
23	3	25	88	5	3	51	1	24	98	6	4
24	3	22	109	5	3	52	1	23	102	5	4
25	3	22	101	5	4	53	1	23	101	6	4
26	3	19	100	5	4	54	1	23	91	5	4
27	1	31	94	6	3	55	1	21	100	5	4
28	1	31	88	6	3	56	1	21	98	6	4

Tablica 9: Svojstva TSC(3, 4) prostora.

Treba još dokazati da je $\text{dev}\{K, L\}$ linearni prostor. Neka su $a, b \in G$ dvije točke. One su spojene lijevom translatom od K ako i samo ako postoje $x, y \in K$ takvi da je $a - x = b - y$, tj. $(-a) + b = (-x) + y$. Analogno, točke a i b spojene su lijevom translatom od L ako i samo ako se $(-a) + b$ može prikazati kao razlika elemenata iz L , tj. $(-a) + b = (-x) + y$ za neke $x, y \in L$. Prema definiciji diferencijske familije $(-a) + b$ se na jedinstven način prikazuje kao razlika elemenata iz K ili L . Zaključujemo da su točke a

i b spojene jedinstvenim pravcem u $\text{dev}\{K, L\}$.

Vidjeli smo da je $\text{dev}\{K, L\}$ linearni prostor $\text{TSC}(k, l)$ sa skupom točaka G . Grupa G djeluje regularno na samu sebe lijevim translacijama. Pritom se čuva skup pravaca, pa je ona ujedno grupa automorfizama od $\text{dev}\{K, L\}$. \square

Korolar 2.35 *Ako postoji (k, l) -diferencijska familija u grupi G , onda je red grupe $v = k(k - 1) + l(l - 1) + 1$.*

Slučaj $k = l$ detaljno je obrađen u četvrtom poglavlju magistarskog rada [55]. Tamo je razvijen program koji sustavno traži diferencijske familije za Steinerove 2-dizajne u cikličkim grupama. Pomoću prilagođene verzije programa (`tscdf.c`) pronađene su sve cikličke diferencijske familije za TSC prostore s parametrima $2 \leq k < l < 10$. One postoje za $k = 2, l = 3, 4, 5$ i za $k = 3, l = 4, 5, 6, 7, 8$. Primjeri iz kojih dobivamo neizomorfne TSC prostore navedeni su u Tablici 10.

(k, l)	Grupa	Diferencijske familije
(2, 3)	\mathbb{Z}_9	$K = \{0, 1\}, L = \{0, 2, 5\}$
(2, 4)	\mathbb{Z}_{15}	$K = \{0, 1\}, L = \{0, 2, 5, 9\}$ $K = \{0, 3\}, L = \{0, 1, 5, 7\}$ $K = \{0, 5\}, L = \{0, 1, 3, 7\}$
(2, 5)	\mathbb{Z}_{23}	$K = \{0, 1\}, L = \{0, 2, 6, 15, 18\}$
(3, 4)	\mathbb{Z}_{19}	$K = \{0, 1, 8\}, L = \{0, 2, 5, 15\}$ $K = \{0, 1, 8\}, L = \{0, 2, 6, 16\}$
(3, 5)	\mathbb{Z}_{27}	$K = \{0, 1, 5\}, L = \{0, 2, 8, 15, 18\}$ $K = \{0, 1, 5\}, L = \{0, 2, 11, 14, 21\}$
(3, 6)	\mathbb{Z}_{37}	$K = \{0, 1, 11\}, L = \{0, 2, 5, 18, 25, 33\}$ $K = \{0, 1, 11\}, L = \{0, 2, 6, 14, 21, 34\}$ $K = \{0, 1, 11\}, L = \{0, 2, 6, 22, 25, 30\}$ $K = \{0, 1, 11\}, L = \{0, 2, 9, 14, 17, 33\}$
(3, 7)	\mathbb{Z}_{49}	$K = \{0, 1, 19\}, L = \{0, 2, 8, 12, 15, 35, 40\}$ $K = \{0, 1, 19\}, L = \{0, 2, 11, 16, 36, 39, 43\}$
(3, 8)	\mathbb{Z}_{63}	$K = \{0, 9, 27\}, L = \{0, 1, 3, 7, 15, 20, 31, 41\}$ $K = \{0, 9, 27\}, L = \{0, 1, 11, 35, 41, 43, 48, 60\}$

Tablica 10: Cikličke diferencijske familije za TSC prostore.

TSC prostori dobiveni od $(3, 8)$ -diferencijskih familija posebno su pravilni. Imaju grupu automorfizama reda 10584 koja se ulaže u punu grupu automorfizama affine ravnine reda 8 (za analizu je korišten programski paket GAP [36]). Generalizacijom tog primjera dobivena je sljedeća općenita konstrukcija TSC prostora.

Teorem 2.36 *Ako postoje projektivne ravnine reda m i reda n , za $n = m^2 + m + 1$ ili $n = m^2 + m + 2$, onda postoji linearni prostor $TSC(m + 1, n)$.*

Dokaz. Neka je P projektivna ravnina reda n i B zatvoren gust podskup od P koji nije podravnina. Skup B se sastoji od svih točaka nekog pravca i svih pravaca kroz jednu od njih, ili od svih točaka nekog pravca, jedne točke van tog pravca i spojnice odabranih točaka. Izbacivanjem skupa B iz P dobivamo strukturu $GDD(n, n, n^2)$, odnosno $GDD(n, n - 1, n^2 - 1)$ [55, Definicija 2.25]. Veličina grupa (skupova točaka koje nisu spojene pravcima) u prvom slučaju je n , a u drugom $n - 1$. Red n odabran je tako da je veličina grupa jednaka broju točaka projektivne ravnine P' reda m . Ako grupe pokrijemo kopijama ravnine P' , dobivamo linearni prostor s pravcima duljine $m + 1$ i n . Kroz proizvoljnu točku prolazi $m + 1$ pravaca duljine $m + 1$ i n pravaca duljine n . Dakle, dobili smo $TSC(m + 1, n)$. □

Napominjemo da konstrukcija nije moguća ako se za B izabere Baerova podravnina ravnine P . Uklanjanjem takve podravnine ostaje struktura GDD s grupama veličine $n - \sqrt{n}$. Taj broj je paran, a broj točaka projektivne ravnine neparan, pa ne možemo pokriti grupe kao u dokazu Teorema 2.36.

Redovi svih poznatih projektivnih ravnina su prim potencije. Prema tome, da bismo pomoću Teorema 2.36 zaista dobili TSC prostore, m i n moraju biti potencije prostih brojeva. Poznata je hipoteza da su m i $n = m^2 + m + 1$ oba prosti beskonačno mnogo puta (općenitija hipoteza postavljena je u [90]). Ako je to točno, u prvom slučaju dobivamo beskonačnu seriju TSC prostora, koja započinje parametrima $(3, 7)$, $(4, 13)$, $(6, 31)$, $(9, 73)$ itd.

U drugom slučaju $n = m^2 + m + 2$ je paran, pa za naše potrebe mora biti potencija od 2. Jednadžba $m^2 + m + 2 = 2^r$ supstitucijom $x = 2m + 1$, $y = r + 2$ prelazi u Nagell-Ramanujanovu diofantsku jednadžbu $x^2 + 7 = 2^y$. Ona ima točno pet rješenja: $(x, y) = (1, 3)$, $(3, 4)$, $(5, 5)$, $(11, 7)$ i $(181, 15)$ (elementaran dokaz dan je u [45]). Njima odgovaraju brojevi $m = 0, 1, 2, 5$ i 90 , među kojima su 2 i 5 prosti, a ostali nisu prim potencije. Dakle, m i n su oba prim potencije jedino za $m = 2$, $n = 8$ i $m = 5$, $n = 32$. Zaključujemo da u drugom slučaju od ravnina čiji su redovi prim potencije dobivamo jedino $TSC(3, 8)$ i $TSC(6, 32)$ prostore.

Dokaz Teorema 2.36 ostavlja puno slobodnog izbora, što omogućuje konstrukciju mnogih neizomorfnih TSC prostora s istim parametrima. Ako postoji više neizomorfnih projektivnih ravnina odgovarajućeg reda, možemo izabrati bilo koju. Nadalje, izborom različitih podskupova B općenito dobivamo neizomorfne strukture GDD (osim ako je P Desarguesova projektivna ravnina, u kojoj se svaka dva zatvorena gusta podskupa istog tipa mogu preslikati jedan na drugi kolineacijom). Čak ako imamo samo jednu strukturu GDD, ipak možemo dobiti neizomorfne TSC prostore promjenom redoslijeda točaka ravnine P' u jednoj ili više grupa. Na primjer, možemo konstruirati mnogo neizomorfnih TSC(3, 7) prostora iako su projektivne ravnine reda 2 i 7 jedinstvene i sve strukture GDD(7, 7, 49) međusobno izomorfne. Zanimljivo je da niti jedan nije izomorfan cikličkim TSC(3, 7) prostorima, jer njihove (49_7) konfiguracije nisu GDD(7, 7, 49). Nasuprot tome, ciklički TSC(3, 8) prostori mogu se konstruirati i pomoću Teorema 2.36.

Sljedeći cilj je prilagoditi metodu konstrukcije pomoću orbitnih matrica TSC prostorima. Neka na TSC(k, l) prostoru, $k < l$, djeluje grupa automorfizama G . Označimo orbite točaka $\mathcal{P}_1, \dots, \mathcal{P}_m$, a orbite pravaca $\mathcal{L}_1, \dots, \mathcal{L}_n$. Bez smanjena općenitosti možemo pretpostaviti da orbite $\mathcal{L}_1, \dots, \mathcal{L}_s$ sadrže kratke pravce (duljine k), a orbite $\mathcal{L}_{s+1}, \dots, \mathcal{L}_n$ duge pravce (duljine l). Komponente marginalnih vektora $\nu = (\nu_1, \dots, \nu_m)$, $\beta = (\beta_1, \dots, \beta_n)$ su duljine orbite, $\nu_i = |\mathcal{P}_i|$ i $\beta_j = |\mathcal{L}_j|$. Očito je $\nu_1 + \dots + \nu_m = \beta_1 + \dots + \beta_s = \beta_{s+1} + \dots + \beta_n = v$.

Orbite čine taktičku dekompoziciju [55, Propozicija 5.2]. Zato su sljedeće definicije dobre:

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

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

U idućih nekoliko rezultata proučavamo svojstva matrica $A = [a_{ij}]$ i $B = [b_{ij}]$.

Lema 2.37 $\nu_i a_{ij} = \beta_j b_{ij}$, za $1 \leq i \leq m$, $1 \leq j \leq n$.

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

Lema 2.38 $\sum_{j=1}^s a_{ij} = k$, $\sum_{j=s+1}^n a_{ij} = l$, za $1 \leq i \leq m$.

Dokaz. Vrijedi zato što kroz točku T prolazi k kratkih i l dugih pravaca. \square

Lema 2.39 $\sum_{i=1}^m b_{ij} = \begin{cases} k, & \text{za } 1 \leq j \leq s \\ l, & \text{za } s+1 \leq j \leq n. \end{cases}$

Dokaz. Vrijedi zato što orbite $\mathcal{L}_1, \dots, \mathcal{L}_s$ sadrže kratke, a $\mathcal{L}_{s+1}, \dots, \mathcal{L}_n$ duge pravce. □

Lema 2.40 $\sum_{j=1}^n a_{i'j} b_{ij} = \begin{cases} \nu_i, & \text{ako je } i \neq i' \\ k + l + \nu_i - 1, & \text{ako je } i = i' \end{cases}$, za $1 \leq i, i' \leq m$.

Dokaz. Neka je zadana točka $T \in \mathcal{P}_{i'}$. Prebrojavamo na dva načina parove $\{(P, \ell) \mid P \in \mathcal{P}_i, T, P I \ell\}$. Točku P možemo izabrati na ν_i načina. Ako je $i \neq i'$, točke T i P sigurno su različite i određuju jedinstven pravac ℓ . Ako je $i = i'$, imamo $k + l$ izbora pravca za $P = T$ i jedan izbor pravca za svaku od $\nu_i - 1$ točaka $P \neq T$. Prema tome, broj parova je ν_i za $i \neq i'$, a $k + l + \nu_i - 1$ za $i = i'$.

Kad prvo biramo pravac ℓ , broj izbora točke P ovisi o orbiti kojoj pripada izabrani pravac. Kroz točku T prolazi $a_{i'j}$ pravaca $\ell \in \mathcal{L}_j$, a na svakom od njih leži b_{ij} točaka $P \in \mathcal{P}_i$. Prebrojavanjem na ovaj način dobivamo $\sum_{j=1}^n a_{i'j} b_{ij}$ za broj parova (P, ℓ) . Izjednačavanjem slijedi tvrdnja leme. □

Propozicija 2.41 *Matrica* $A = [a_{ij}]$ *ima sljedeća svojstva:*

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

$$(2) \quad \sum_{j=1}^s a_{ij} = k, \quad \sum_{j=s+1}^n a_{ij} = l, \quad \text{za } 1 \leq i \leq m;$$

$$(3) \quad \sum_{i=1}^m \frac{\nu_i}{\beta_j} a_{ij} = \begin{cases} k, & \text{za } 1 \leq j \leq s, \\ l, & \text{za } s + 1 \leq j \leq n; \end{cases}$$

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

Dokaz. Slijedi iz prethodne četiri leme. □

Definicija 2.42 *Svaka* $m \times n$ *matrica* $A = [a_{ij}]$ *nad* $\mathbb{N} \cup \{0\}$ *sa svojstvima iz Propozicije 2.41 naziva se* **orbitna matrica** *za* $TSC(k, l)$ *s marginalnim vektorima* $\nu = (\nu_1, \dots, \nu_m)$ *i* $\beta = (\beta_1, \dots, \beta_n)$.

Indeksiranje ovakvih orbitnih matrica do incidencijskih matrica $TSC(k, l)$ prostora potpuno je analogno odgovarajućem postupku za Steinerove 2-dizajne. Koristimo program `tscindex.c`, koji je jednostavna modifikacija programa `index1.c` (razlika je samo u zadavanju parametara). Međutim, klasifikacija orbitnih matrica za TSC prostore može se organizirati na više načina.

Prirodno je kod parcijalnih orbitnih matrica također razlikovati kratke i duge pravce. Za skup X_t objekata reda t uzimamo sve $t \times n$ matrice sa svojstvima iz Propozicije 2.41, osim što u (3) zamijenimo jednakost s nejednakosti. Grupa $H_t = \{\sigma \in S_t \mid \nu_{\sigma(i)} = \nu_i, i = 1, \dots, t\}$ permutira retke matrica iz X_t , a grupa $K = \{\sigma \in S_n \mid \sigma(\{1, \dots, s\}) = \{1, \dots, s\}, \beta_{\sigma(i)} = \beta_i, i = 1, \dots, n\}$ permutira stupce. Razlika u odnosu na klasifikaciju blok dizajna je što ne dozvoljavamo permutacije stupaca koje preslikavaju prvih s stupaca (koji odgovaraju kratkim pravcima) na idućih $n - s$ stupaca (koji odgovaraju dugim pravcima). Sve ostalo je analogno kao u cjelini 1.7. Klasifikacijski Algoritam 1.29 implementiran je programom `tscorbmat.c`.

Nedostatak ovog pristupa je što na nižim nivoima stabla dobivamo puno više neizomornih parcijalnih orbitnih matrica nego kod problema odgovarajuće veličine za Steinerove 2-dizajne. To možemo otkloniti tako da kod parcijalnih orbitnih matrica ne razlikujemo orbite kratkih i dugih pravaca, slično kao kod klasifikacije $TSC(3, 4)$ prostora u Primjeru 1.36. Skup X_t neka sadrži $t \times n$ matrice $A = [a_{ij}]$ nad $\mathbb{N} \cup \{0\}$ sa sljedećim svojstvima:

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

$$(2) \quad \sum_{j=1}^n a_{ij} = k + l, \quad \text{za } 1 \leq i \leq t;$$

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

$$(4) \quad \sum_{j=1}^n \frac{\nu_i}{\beta_j} a_{ij} a_{i'j} = \begin{cases} \nu_i, & \text{ako je } i \neq i' \\ k + l + \nu_i - 1, & \text{ako je } i = i' \end{cases}, \quad \text{za } 1 \leq i, i' \leq t.$$

Za $t = m$ takve matrice zovemo *generalizirane orbitne matrice* za $TSC(k, l)$. Klasifikaciju organiziramo isto kao u cjelini 1.7 (dozvoljavamo sve permutacije stupaca koje čuvaju vektor β). Klasifikacijski Algoritmi 1.29 i 1.31 implementirani su programom `tscgorbmat.c`.

Kod drugog pristupa problem je što indeksiranjem generaliziranih orbitnih matrica možemo dobiti incidencijske strukture koje nisu TSC prostori. Pod (3) zahtijevamo samo da nema pravaca duljine veće od l . U specijalnom

slučaju $l = k + 1$ iz toga slijedi da su pola pravaca duljine k , a druga polovica duljine l , ali općenito to ne mora vrijediti. Na kraju je lako izabrati generalizirane orbitne matrice sa svojstvima iz Propozicije 2.41, ali to može značiti da smo klasificirali puno veći skup objekata od onog koji nas zanima.

Koji je od ova dva pristupa efikasniji ovisi o parametrima. Uspoređujemo ih na nizu primjera za TSC prostore s automorfizmom prostog reda p bez fiksnih točaka i pravaca. Marginalni vektori ν, β su u svim primjerima oblika (p, p, \dots, p) i duljine $m = v/p, n = 2m$.

Primjer 2.43 Klasificiramo orbitne matrice koje odgovaraju $\text{TSC}(4, 5)$ prostorima s automorfizmom reda $p = 11$ bez fiksnih točaka i pravaca. Pomoću oba programa (`tscorbm.c` i `tscgorbm.c`) dobivamo u vrlo kratkom vremenu točno 4 matrice. Dakle, u ovom slučaju sve generalizirane orbitne matrice imaju svojstva iz Propozicije 2.41 (ako stupce koji odgovaraju orbitama kratkih pravaca stavimo na početak).

Primjer 2.44 Klasificiramo orbitne matrice za $\text{TSC}(4, 5)$ s automorfizmom reda $p = 3$. Ovo je znatno veći problem i nije svejedno kako organizirati klasifikaciju. Pomoću oba programa dobili smo jednak broj matrica, 29712. Programi su izvođeni paralelno na više računala. Ukupno vrijeme izvođenja programa `tscgorbm.c` na procesorima od 1.5 GHz iznosi približno mjesec dana, a programa `tscorbm.c` oko tri puta više. Dakle, u ovom slučaju pristup preko generaliziranih orbitnih matrica je efikasniji.

Primjer 2.45 Za $\text{TSC}(4, 7)$, $p = 11$ postoje generalizirane orbitne matrice koje nemaju svojstva iz Propozicije 2.41. Pomoću programa `tscorbm.c` dobivamo 65 matrica, a pomoću programa `tscgorbm.c` dobivamo 390. Od tih 390 matrica točno 65 su orbitne matrice za $\text{TSC}(4, 7)$ (to smo provjerili pomoću programa `tsctest.c`). Klasifikacija je nešto brža na prvi način, ali vrijeme izvođenja oba programa iznosi svega nekoliko sekundi.

Primjer 2.46 Za $\text{TSC}(4, 8)$, $p = 23$ postoje tri generalizirane orbitne matrice, od čega su dvije “dobre”.

Primjer 2.47 Za $\text{TSC}(4, 9)$, $p = 17$ postoji 142 orbitnih matrica i 1125 generaliziranih orbitnih matrica. Na procesoru od 1.2 GHz vrijeme izvođenja programa `tscorbm.c` je oko 2 sekunde, a programa `tscgorbm.c` oko jednu minutu.

Primjer 2.48 Za $\text{TSC}(5, 6)$, $p = 17$ nema razlike između orbitnih matrica i generaliziranih orbitnih matrica. Pomoću oba programa dobivamo 6 matrica.

Primjer 2.49 Za $TSC(5, 8)$, $p = 11$ prvi način klasifikacije ima najveću prednost. Postoji ukupno 1 347 779 generaliziranih orbitnih matrica, a među njima su 84 256 orbitne matrice za $TSC(5, 8)$. Program `tscgorbmat.c` izvodio se na procesoru od 1.5 GHz oko 14 dana, a `tscorbmat.c` oko 20 sati.

Primjer 2.50 Za $TSC(5, 9)$, $p = 31$ postoje 4 orbitne matrice i 7 generaliziranih orbitnih matrica.

Primjer 2.51 Za $TSC(6, 8)$, $p = 29$ postoje 4 orbitne matrice i 6 generaliziranih orbitnih matrica.

Pomoću programa `tscindex.c` proveli smo indeksiranje svih konstruiranih orbitnih matrica, osim onih iz Primjera 2.49 (za koje bi trebalo previše procesorskog vremena). Tako su dobiveni sljedeći rezultati.

Teorem 2.52 *Postoji točno 12 prostora $TSC(4, 5)$ s automorfizmom reda 3 bez fiksnih točaka i pravaca.*

Dokaz. Slijedi indeksiranjem orbitnih matrica iz Primjera 2.44 i izbacivanjem izomorfničkih incidencijskih matrica (pomoću programa `incfilter.c`). Od 29712 orbitnih matrica samo je 12 moguće indeksirati. □

Teorem 2.53 *Za sljedeće parametre ne postoje $TSC(k, l)$ prostori s automorfizmom reda p bez fiksnih točaka i pravaca:*

1. $TSC(4, 5)$, $p = 11$
2. $TSC(4, 7)$, $p = 11$
3. $TSC(4, 8)$, $p = 23$
4. $TSC(4, 9)$, $p = 17$
5. $TSC(5, 6)$, $p = 17$
6. $TSC(5, 9)$, $p = 31$
7. $TSC(6, 8)$, $p = 29$

Dokaz. Odgovarajuće orbitne matrice, klasificirane u prethodnim primjerima, nije moguće indeksirati. □

3 Nepotpuna potraga

3.1 Egzistencija blok dizajna kao optimizacijski problem

U ovom poglavlju formuliramo pitanje egzistencije blok dizajna kao problem kombinatorne optimizacije i koristimo heurističke algoritme za njegovo rješavanje. Dio rezultata opisan je i u [59].

Neka je X konačan skup i $c : X \rightarrow \mathbb{N} \cup \{0\}$ funkcija. Elemente skupa X zovemo *rješenja*, a elemente u kojima je vrijednost funkcije jednaka nuli *optimalna rješenja*. Cilj je pronaći optimalno rješenje, ako postoji. Dakle, imamo problem kombinatorne optimizacije s jednostavnim kriterijem za optimalnost, ali su u problemima koji nas zanimaju optimalna rješenja vrlo rijetka i teško se nalaze.

Neka je zadana funkcija susjedstva $N : X \rightarrow 2^X$. Algoritam lokalne potrage kreće od nekog početnog rješenja $x_0 \in X$ i sukcesivno ga zamjenjuje rješenjem iz njegovog susjedstva. Heuristika je pravilo prema kojem se bira rješenje iz susjedstva $N(x_0)$. Izbor ne mora biti deterministički i nema garancije da će algoritam pronaći optimalno rješenje. Međutim, za dobre heuristike u praksi se pokazuje da algoritam često pronalazi optimalna rješenja, ili barem dobre aproksimacije. Primjeri heurističkih algoritama su hill-climbing, simulated annealing, tabu search i genetički algoritmi (koji se donekle razlikuju od prethodnih jer umjesto s jednim rješenjem rade s populacijom rješenja). Uvod u heurističke algoritme nalazi se u petom poglavlju knjige [62].

U zadnje vrijeme objavljeno je nekoliko radova u kojima su pomoću heurističke lokalne potrage konstruirani blok dizajni. U [13], [76] i [77] na taj način su konstruirani blok dizajni s cikličkim, regularnim i 1-rotacijskim grupama automorfizama. Ovdje objašnjavamo kako pomoću lokalne potrage možemo konstruirati blok dizajne bez ikakvih dodatnih pretpostavki.

Sjetimo se da je incidencijska matrica (v, k, λ) blok dizajna $v \times b$ matrica A nad $\{0, 1\}$ sa svojstvima $A \cdot A^t = (r - \lambda)I_v + \lambda J_v$ i $A^t \cdot j_b = k j_v$. Vrijedi i obrat, tj. svaka matrica s tim svojstvima reprezentira (v, k, λ) blok dizajn. Za skup X uzimamo skup svih $v \times b$ matrica nad $\{0, 1\}$ kojima su sume redaka r i sume stupaca k :

$$X = \left\{ A = [a_{ij}] \mid \sum_{i=1}^v a_{ij} = k, \sum_{j=1}^b a_{ij} = r \right\}$$

Skup sadrži sve incidencijske matrice (v, k, λ) blok dizajna, ali to nisu jedine matrice u X . Nedostaje svojstvo da su skalarni produkti različitih redaka matrice jednaki λ . Funkciju $c : X \rightarrow \mathbb{N} \cup \{0\}$ definiramo tako da “mjeri odstupanje” od tog svojstva:

$$c(A) = \sum_{i < i'} \left(\sum_{j=1}^b a_{ij} a_{i'j} - \lambda \right)^2$$

Očito je $c(A) = 0$ ako i samo ako je $A = [a_{ij}]$ incidencijska matrica (v, k, λ) blok dizajna. Za lokalnu potragu treba nam funkcija susjedstva $N : X \rightarrow 2^X$. Koristimo sljedeći teorem H.J.Rysera iz 1957, koji je u [87] dokazan indukcijom, a ovdje dokaz formuliramo kao algoritam.

Teorem 3.1 *Neka su A i B matrice dimenzija $v \times b$ nad $\{0, 1\}$. Sume redaka i stupaca u matrici A jednake su odgovarajućim sumama u matrici B ako i samo ako se konačnim nizom zamjena podmatrica*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad i \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

matrice A i B mogu transformirati jedna u drugu.

Dokaz. Zamjene podmatrica očito ne mijenjaju sume redaka i stupaca. Zato matrice koje se mogu transformirati jedna u drugu imaju jednake sume redaka i stupaca. Za obrat pretpostavimo da matrice $A = [a_{ij}]$ i $B = [b_{ij}]$ imaju jednake sume redaka i stupaca. Opisat ćemo kako se zamjenama podmatrica može postići da A i B postanu jednake.

Pretpostavimo da se matrice razlikuju u prvom retku. Na primjer, neka je $a_{1i} = 1$, $b_{1i} = 0$ za neki i . Zbog jednakosti sume prvog retka postoji j takav da je $a_{1j} = 0$, $b_{1j} = 1$. Dokazujemo da postoji $k \geq 2$ takav da je $(a_{ki}, a_{kj}) = (0, 1)$ ili $(b_{ki}, b_{kj}) = (1, 0)$. Označimo sa $A(x, y)$ broj elemenata skupa $\{k \mid 2 \leq k \leq v, (a_{ki}, a_{kj}) = (x, y)\}$ i analogno za $B(x, y)$. Izjednačavanjem sume i -tog stupca dobivamo $1 + A(1, 0) + A(1, 1) = B(1, 0) + B(1, 1)$, a j -tog stupca $A(0, 1) + A(1, 1) = 1 + B(0, 1) + B(1, 1)$. Oduzimanjem slijedi $A(0, 1) + B(1, 0) = 2 + A(1, 0) + B(0, 1) \geq 2$, pa je $A(0, 1) > 0$ ili $B(1, 0) > 0$. U prvom slučaju mijenjamo podmatricu od A , u drugom slučaju podmatricu od B , i tako izjednačavamo dva unosa u prvim recima matrica A i B . Analogno nastavljamo dok ne izjednačimo prve retke. Zatim isti postupak ponavljamo s drugim, trećim, četvrtim... recima dok ne izjednačimo sve elemente matrica A i B . □

Iz prethodnog teorema slijedi da od proizvoljne matrice iz skupa X konačnim nizom zamjena podmatrica možemo dobiti incidencijsku matricu (v, k, λ) blok dizajna, ako dizajni postoje. Prirodan izbor susjedstva $N(A)$ je skup svih matrica koje od A dobivamo zamjenom jedne podmatrice. Iduća propozicija govori o veličini tog skupa.

Propozicija 3.2 Za svaku matricu $A \in X$ vrijedi $|N(A)| \geq \binom{v}{2}(r - \lambda)^2$. Jednakost se dostiže ako i samo ako je A incidencijska matrica (v, k, λ) blok dizajna.

Dokaz. Prebrojavamo podmatrice od A oblika $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ili $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Ako su zadani reci i, j u kojima biramo podmatricu, možemo izabrati bilo koji stupac koji na i -tom mjestu ima jedinicu, a na j -tom nulu, i bilo koji drugi stupac u kojem je obratno. Izboru ima $(r - \lambda_{ij})^2$, gdje je $\lambda_{ij} = \sum_{k=1}^b a_{ik}a_{jk}$ broj stupaca koji na i -tom i j -tom mjestu imaju jedinicu. Prema tome, $|N(A)| = \sum_{i < j} (r - \lambda_{ij})^2$. Dvostrukim prebrojavanjem trojki $\{(i, j, k) \mid a_{ik} = a_{jk} = 1\}$ slijedi $\sum_{i < j} \lambda_{ij} = b \cdot \binom{k}{2}$. Uz taj uvjet izraz za $|N(A)|$ (shvaćen kao kvadratna funkcija u varijablama λ_{ij}) poprima minimalnu vrijednost $\binom{v}{2}(r - \lambda)^2$ kad je $\lambda_{ij} = \lambda$ za sve $i < j$. Taj slučaj upravo odgovara incidencijskim matricama (v, k, λ) blok dizajna. \square

Nakon definicije skupa rješenja X , funkcije susjedstva N i ciljne funkcije c slijedi izbor heuristike. Hill-climbing heuristika ponaša se dobro za probleme kod kojih su većina lokalnih minimuma ujedno globalni. Opisani optimizacijski problem za (v, k, λ) blok dizajne takav je samo za $k = 3$. Za $k > 3$ funkcija $c : X \rightarrow \mathbb{N} \cup \{0\}$ ima puno lokalnih minimuma koji nisu globalni, pa se bolje ponašaju heuristike simulated annealing i tabu search.

R.Mathon [67] je u ovom kontekstu koristio simulated annealing. Prema [67], pomoću njegove implementacije mogu se konstruirati Hadamardovi dizajni $(4m - 1, 2m - 1, m - 1)$ za $m < 6$ i projektivne ravnine $S(2, n + 1, n^2 + n + 1)$ za $n < 9$. U našoj implementaciji tabu search se pokazao efikasnijim od simulated annealing heuristike. Program `tabubibd.c` lako nalazi i Hadamardove dizajne za $m = 6$. Međutim, oba naša programa nisu našli projektivne ravnine reda 7 i 8 niti nakon duže potrage (Primjer 3.5). U idućoj cjelini opisujemo implementaciju tabu search algoritma i dobivene rezultate.

3.2 Tabu search algoritam za blok dizajne i konfiguracije

Algoritmi lokalne potrage definiraju niz rješenja (x_i) tako da u svakoj iteraciji zamjenjuju trenutno rješenje x_i nekim rješenjem iz njegovog susjedstva $x_{i+1} \in N(x_i)$. Kod hill-climbing algoritma novo rješenje ne smije povećati vrijednost ciljne funkcije, tj. mora vrijediti $c(x_{i+1}) \leq c(x_i)$. Tabu search je jednostavna generalizacija tog pravila. Kad algoritam zapne u lokalnom minimumu (u kojemu je $0 < c(x_i) \leq c(x)$ za sve $x \in N(x_i)$), dozvoljavamo potez koji povećava vrijednost ciljne funkcije. Algoritam će se u idućih

nekoliko iteracija vjerojatno vratiti u isti lokalni minimum i nakon toga se niz počinje ponavljati. Da bi se to izbjeglo, zadnjih nekoliko rješenja (ili poteza koji su do njih doveli) pamte se u *tabu listi*. Rješenja u tabu listi su zabranjena, a u svakoj iteraciji najstariji član liste zamjenjuje se trenutnim rješenjem (tabu lista je *red*, tj. FIFO lista).

Program `tabubibd.c` počinje potragu od pseudoslučajne matrice $A \in X$. Generira se ciklička matrica iz X i primjenjuje određen broj pseudoslučajnih zamjena podmatrice kao u Teoremu 3.1. Iteracija se sastoji od promjene jedne podmatrice. Bira se podmatrica koja najviše smanjuje ciljnu funkciju, ako je to moguće. U tabu listi se pamte podmatrice koje su se mijenjale u zadnjih nekoliko iteracija i njih se ne smije izabrati.

Optimalnu veličinu tabu liste određujemo eksperimentiranjem. U [76] i [77] preporučuju se tabu liste od 3 do 7 unosa, ali naš program se najbolje ponaša s tabu listom od 20 do 30 unosa. Razlika se može objasniti time što su kod nas skupovi susjednih rješenja $N(A)$ puno veći nego u [76] i [77] (Propozicija 3.2).

Tabu lista ne može potpuno spriječiti cikličko ponavljanje rješenja. Ako algoritam ne pronade optimalno rješenje nakon nekoliko tisuća iteracija, obično se isplati ponovo započeti potragu od pseudoslučajne matrice. Koristimo još jedno pravilo koje poboljšava performanse programa. Može se dogoditi da tabu lista sprječava pronalaženje optimalnog rješenja, jer sadrži indekse podmatrice koju treba promijeniti da bi se dobila incidencijska matrica blok dizajna. U takvim slučajevima dozvoljavamo “tabu iznimke”. Ako zamjenom podmatrice dobivamo matricu u kojoj je vrijednost ciljne funkcije manja nego u svim prethodnim iteracijama, takva zamjena je dozvoljena bez obzira na tabu listu. Zbog ovog pravila očito ne može doći do cikličkog ponavljanja rješenja.

Program `tabubibd.c` korišten je u cijelini 2.3 za konstrukciju (12, 4, 3) blok dizajna. U iduća tri primjera detaljnije analiziramo njegovo ponašanje.

Primjer 3.3 U ovom primjeru cilj je poboljšati neke od donjih ocjena za broj neizomornih blok dizajna u [24, Tablica I.1.28]. Pomoću programa `tabubibd.c` konstruiramo niz incidencijskih matrica, zatim pomoću programa `incfilter.c` ispitujemo izomornost. Za čvrste parametre koristimo najviše jedan dan procesorskog vremena i konstruiramo najviše 10000 neizomornih dizajna. U Tablici 11 navedeni su parametri za koje je na taj način bitno poboljšana ocjena iz [24]. Stupci sadrže redni broj dizajna iz [24, Tablica I.1.28], parametre, staru i novu ocjenu za broj neizomornih dizajna. Zanimljivo je da se među konstruiranim blok dizajnima nije pojavio niti jedan par međusobno izomornih. To znači da je stvarni broj dizajna s parametrima iz Tablice 11 izuzetno velik i da su nove ocjene također vrlo grube.

R.br.	(v, k, λ)	Handbook	Novo	R.br.	(v, k, λ)	Handbook	Novo
69	(19, 4, 2)	423	10^4	361	(19, 4, 4)	424	5000
70	(13, 4, 3)	3702	10^4	416	(11, 5, 10)	3337	10^4
102	(15, 5, 4)	207	10^4	447	(14, 4, 6)	4	2500
123	(16, 5, 4)	11	10^4	520	(29, 4, 3)	1	200
124	(13, 5, 5)	30	10^4	525	(15, 5, 8)	104	10^4
128	(16, 6, 5)	15	300	529	(15, 6, 10)	118	10^4
147	(25, 4, 2)	17	1000	606	(16, 5, 8)	12	5000
148	(17, 4, 3)	1	10^4	607	(13, 5, 10)	31	10^4
149	(13, 4, 4)	2462	10^4	688	(17, 4, 6)	1	250
220	(20, 4, 3)	1	2500	742	(16, 6, 11)	1	10^4
221	(20, 5, 4)	1	400	785	(18, 4, 6)	1	100
238	(31, 4, 2)	1	50	788	(18, 6, 10)	4	1000
239	(21, 4, 3)	1	2500	825	(15, 5, 10)	1	1000
242	(11, 4, 6)	1	10^4	835	(16, 7, 14)	1	1000
246	(17, 5, 5)	1	5000	1000	(20, 5, 8)	1	1000
247	(11, 5, 8)	4394	10^4	1036	(16, 6, 13)	1	1000
284	(16, 6, 7)	1	5000	1037	(14, 6, 15)	1	5000
340	(24, 4, 3)	1	1000	1094	(17, 5, 10)	1	1000

Tablica 11: Nove donje ocjene za broj neizomorfnih blok dizajna.

Većina konstruiranih dizajna ima trivijalnu punu grupu automorfizama (zapravo, netrivialnu grupu imaju samo dizajni s višestrukim blokovima, koji se mogu permutirati). Prema tome, ovi dizajni ne bi se mogli konstruirati metodom korištenom u [drugom poglavlju](#) disertacije.

Primjer 3.4 U ovom primjeru uspoređujemo naš tabu search algoritam za blok dizajne s dva slična algoritma iz literature. P.Bofill i C.Torras [14], [15] testirali su niz optimizacijskih algoritama za neuralne mreže na problemu konstrukcije blok dizajna. Najuspješniji se pokazao algoritam koji koristi heuristiku simulated annealing (označavat ćemo ga NN-SA). S.Prestwich [84] uspoređuje taj algoritam s randomiziranom verzijom backtrackinga kojeg naziva “constrained local search” (CLS). Usporedba se vrši za sve parametre iz [24, Tablica I.1.28] koji zadovoljavaju $vb \leq 1000$. To su ujedno svi dopustivi parametri za $2k \leq v$, $r \leq 41$ i $vb \leq 1000$. Ima ih 129, ali u četiri slučaja dizajni ne postoje: (15, 5, 2), (22, 7, 2), (21, 6, 2) i (29, 8, 2). Za preostalih 125 parametara NN-SA nalazi dizajne u 54 slučaja (43.2%), a CLS u 93 slučaja (74.4%). Za svaki od 125 parametara pozivali smo program `tabubibd.c` pedeset puta, pri čemu je maksimalan broj iteracija bio 1000, a duljina tabu

(v, k, λ)	Br.	(v, k, λ)	Br.	(v, k, λ)	Br.	(v, k, λ)	Br.	(v, k, λ)	Br.
(7, 3, 1)	50	(10, 4, 4)	50	(6, 3, 16)	50	(25, 9, 3)	11	(12, 4, 6)	46
(6, 3, 2)	50	(16, 4, 1)	42	(16, 8, 7)	0	(15, 5, 4)	48	(12, 6, 15)	50
(7, 3, 2)	50	(9, 3, 3)	50	(11, 5, 8)	50	(21, 7, 3)	0	(9, 4, 15)	50
(9, 3, 1)	50	(9, 4, 6)	47	(9, 4, 9)	50	(7, 3, 13)	50	(13, 4, 5)	48
(8, 4, 3)	50	(8, 4, 9)	50	(7, 3, 10)	50	(16, 4, 2)	49	(11, 5, 14)	45
(6, 3, 4)	50	(13, 3, 1)	50	(13, 4, 3)	50	(16, 6, 5)	6	(9, 3, 8)	50
(11, 5, 2)	50	(13, 4, 2)	50	(13, 5, 5)	50	(9, 3, 6)	50	(21, 5, 2)	0
(7, 3, 3)	50	(13, 6, 5)	40	(16, 6, 4)	0	(9, 4, 12)	50	(21, 6, 3)	0
(10, 4, 2)	50	(7, 3, 7)	50	(15, 3, 1)	50	(15, 7, 9)	32	(21, 10, 9)	0
(9, 4, 3)	50	(6, 3, 12)	50	(15, 6, 5)	11	(13, 3, 2)	48	(16, 6, 7)	41
(13, 4, 1)	50	(10, 5, 8)	49	(12, 3, 2)	49	(13, 4, 4)	46	(10, 3, 6)	50
(6, 3, 6)	50	(19, 9, 4)	24	(12, 6, 10)	50	(13, 6, 10)	50	(10, 4, 12)	49
(10, 5, 4)	50	(11, 5, 6)	50	(23, 11, 5)	6	(10, 5, 16)	48	(15, 7, 12)	47
(7, 3, 4)	50	(14, 7, 6)	10	(7, 3, 11)	50	(19, 9, 8)	0	(18, 6, 5)	0
(9, 3, 2)	50	(16, 6, 3)	49	(9, 3, 5)	50	(11, 5, 12)	48	(22, 11, 10)	0
(8, 4, 6)	49	(7, 3, 8)	50	(10, 5, 12)	45	(22, 8, 4)	0	(15, 5, 6)	50
(15, 7, 3)	28	(12, 4, 3)	50	(8, 4, 15)	50	(14, 7, 12)	50	(16, 4, 3)	50
(6, 3, 8)	50	(6, 3, 14)	50	(17, 8, 7)	0	(27, 13, 6)	0	(16, 8, 14)	29
(11, 5, 4)	50	(9, 3, 4)	50	(7, 3, 12)	50	(21, 9, 6)	0	(31, 6, 1)	26
(7, 3, 5)	50	(7, 3, 9)	50	(10, 3, 4)	49	(10, 4, 10)	47	(31, 10, 3)	0
(16, 6, 2)	20	(21, 5, 1)	41	(10, 4, 8)	49	(25, 5, 1)	35	(31, 15, 7)	0
(12, 6, 5)	50	(8, 3, 6)	49	(11, 3, 3)	48	(9, 3, 7)	50	(11, 5, 16)	45
(7, 3, 6)	50	(8, 4, 12)	50	(11, 4, 6)	49	(20, 10, 9)	0	(22, 7, 4)	0
(6, 3, 10)	50	(10, 4, 6)	50	(11, 5, 10)	49	(16, 5, 4)	43	(9, 3, 9)	50
(10, 3, 2)	50	(15, 7, 6)	1	(18, 9, 8)	0	(16, 6, 6)	23	(25, 10, 6)	0

Tablica 12: Broj konstruiranih dizajna u 50 poziva tabu search algoritma.

liste 30. Rezultati su navedeni u Tablici 12. Bar jedan dizajn pronađen je u 106 slučaja (84.8%). Za preostalih 19 parametara program je izvođen 1000 puta s maksimalnim brojem iteracija 2000 (u [84] se također dozvoljava maksimalno 2 000 000 iteracija algoritma CLS). Pronađeni su (16, 8, 7), (16, 6, 4) i (18, 6, 5) blok dizajni. Među 16 parametara za koje ni tada nije pronađen dizajn nalaze se i parametri (22, 8, 4), za koje je problem egzistencije otvoren.

Glavna prednost našeg algoritma je što pretražuje samo matrice sa sumama redaka r i sumama stupaca k (narušen je jedino uvjet na skalarnu produkte redaka). Algoritmi NN-SA i CLS pretražuju veće skupove matrica, u kojima svi uvjeti mogu biti narušeni.

Primjer 3.5 U ovom primjeru primjenjujemo program `tabubibd.c` na Steinerove 2-dizajne. Ponašanje se jako razlikuje za $k = 3$ i za $k > 3$. Program lako nalazi $S(2, 3, v)$ dizajne čak i za velike v . Poznato je da se Steinerovi sistemi trojki mogu uspješno konstruirati hill-climbing algoritmom, korištenim na primjer u [95] (opis algoritma nalazi se u petom poglavlju knjige [62]). Međutim, za $k > 4$ na ovaj način dobili smo jedino projektivne i afine ravnine reda $n \leq 5$ ($S(2, 4, 13)$, $S(2, 4, 16)$, $S(2, 5, 21)$, $S(2, 5, 25)$ i $S(2, 6, 31)$). Za sve ostale parametre koje smo testirali nije pronađen niti jedan dizajn. Potrošeno je nekoliko dana procesorskog vremena za projektivne i afine ravnine reda $n = 7, 8$ i za svaki od parametara $S(2, 4, 25)$, $S(2, 4, 28)$ i $S(2, 4, 37)$. Zaljučujemo da za Steinerove 2-dizajne ovaj pristup ne može biti alternativa metodi konstrukcije pomoću grupa automorfizama, korištenoj u drugom poglavlju disertacije.

Tabu search algoritam uz male preinake možemo koristiti i za konstrukciju drugih incidencijskih struktura. Na primjer, za konstrukciju konfiguracija (Definicija 1.6) dovoljno je promijeniti ciljnu funkciju:

$$c(A) = \sum_{i < i'} \left[\left(\sum_{j=1}^b a_{ij} a_{i'j} \right)^2 - \sum_{j=1}^b a_{ij} a_{i'j} \right]$$

Izraz u uglatoj zagradi jednak je nuli ako je skalarni produkt redaka i, i' nula ili jedan, a inače je pozitivan. Prema tome, $c(A) = 0$ ako i samo ako je A incidencijska matrica (v_r, b_k) konfiguracije. Prilagođeni program `tabuconf.c` koristimo za konstrukciju konfiguracija u Primjeru 3.6 i u idućoj cjelini.

Primjer 3.6 U ovom primjeru konstruiramo simetrične (v_k) konfiguracije pomoću programa `tabuconf.c`. Nuždan uvjet za postojanje konfiguracija je $v \geq k^2 - k + 1$, a program smo testirali za $v \leq 100$. Za $k = 3$ i $k = 4$ program vrlo brzo nalazi konfiguracije za sve parametre v koji zadovoljavaju uvjete. Za $k = 5$ jedina iznimka je $v = 22$, ali poznato je da (22_5) konfiguracija ne postoji [24, Tablica IV.6.10]. Među ostalim primjerima konstruirane su (23_5) konfiguracije, ekvivalentne linearnim prostorima TSC(2, 5) (Propozicija 2.32).

Prema [24, Tablica IV.6.10] konfiguracije s $k = 6$ ne postoje za $v = 32$, a za $v = 33$ i 34 pitanje egzistencije je otvoreno. Naš program brzo nalazi (31_6) konfiguraciju (projektivnu ravninu reda 5), a uz malo više računanja (34_6) i (35_6) konfiguracije. Svi konstruirani primjeri za (34_6) izomorfni su konfiguraciji koju ovdje navodimo.

{1, 6, 10, 15, 23, 27}	{19, 25, 27, 29, 30, 33}	{9, 13, 14, 22, 23, 29}
{7, 8, 17, 19, 23, 32}	{11, 14, 17, 20, 27, 31}	{10, 12, 13, 19, 20, 26}
{3, 4, 5, 14, 15, 19}	{4, 8, 9, 16, 18, 27}	{2, 11, 13, 15, 18, 33}
{4, 6, 13, 17, 21, 30}	{1, 2, 4, 12, 25, 32}	{6, 8, 14, 25, 26, 34}
{4, 7, 10, 11, 29, 34}	{2, 6, 9, 19, 24, 31}	{1, 18, 19, 21, 28, 34}
{1, 5, 9, 11, 26, 30}	{6, 11, 12, 16, 22, 28}	{2, 7, 21, 22, 26, 27}
{5, 10, 17, 18, 22, 25}	{1, 8, 20, 22, 24, 33}	{15, 16, 17, 24, 26, 29}
{2, 3, 8, 10, 28, 30}	{7, 12, 14, 18, 24, 30}	{15, 22, 30, 31, 32, 34}
{3, 6, 18, 20, 29, 32}	{1, 3, 7, 13, 16, 31}	{2, 5, 16, 20, 23, 34}
{5, 8, 12, 21, 29, 31}	{10, 14, 16, 21, 32, 33}	{7, 9, 15, 20, 25, 28}
{3, 9, 12, 17, 33, 34}	{5, 13, 24, 27, 28, 32}	{3, 11, 21, 23, 24, 25}
{4, 23, 26, 28, 31, 33}		

Za $v = 33$ i $36 \leq v \leq 42$ nije pronađena niti jedna konfiguracija s $k = 6$, ali ih program lako nalazi za $v \geq 43$. Ponašanje programa je slično za $k = 7$. Lako se nalaze konfiguracije sa $v \geq 68$, a nije pronađena niti jedna konfiguracija s manjim v . Na temelju ovih primjera čini se da za čvrsti k postoji v_0 za kojeg program lako nalazi (v_k) konfiguracije za sve $v \geq v_0$.

3.3 Dizajni $S(2, k, 2k^2 - 2k + 1)$ kao TSC prostori

Prema Definiciji 1.8, svaki $TSC(k, k)$ prostor je Steinerov 2-dizajn s dvostruko više pravaca nego točaka ($b = 2v$). Takvi Steinerovi 2-dizajni imaju parametre oblika $S(2, k, 2k^2 - 2k + 1)$ i bili su tema magistarskog rada [55]. Postavlja se pitanje je li svaki takav dizajn ujedno $TSC(k, k)$ prostor, tj. može li se skup pravaca rastaviti na dvije simetrične (v_k) konfiguracije? U slučaju $k < l$ particija $TSC(k, l)$ prostora na dvije simetrične konfiguracije je jedinstvena i dobiva se razdvajanjem “kratkih” i “dugih” pravaca. Međutim, ako su svi pravci jednake duljine particija ne mora biti jedinstvena i nije jasno da li postoji. U ovoj cjelini ispitujemo poznate primjere $S(2, k, 2k^2 - 2k + 1)$ dizajna.

Postoje točno 2 dizajna $S(2, 3, 13)$ [55, Primjer 3.21] i 18 dizajna $S(2, 4, 25)$ [94]. Pomoću programa `tscpartition.c` prebrojili smo sve moguće rastave na dvije simetrične konfiguracije. Rezultati su navedeni u Tablici 13, u kojoj su dizajni označeni isto kao u [55, Tablica 1]. Svaki dizajn dopušta bar dva rastava, pa zaključujemo:

Propozicija 3.7 *Svi dizajni $S(2, 3, 13)$ i $S(2, 4, 25)$ su TSC prostori.*

Dizajni $S(2, 5, 41)$ nisu potpuno klasificirani. R.Mathon i A.Rosa [24, Tablica I.1.28] konstruirali su 4 primjera s automorfizmom reda 5 i još jedan primjenom određene transformacije. U magistarskom radu [55, Teo-

Dizajn	Br.	Dizajn	Br.	Dizajn	Br.	Dizajn	Br.
S3.1	14	S4.4	140	S4.9	5	S4.14	23
S3.2	14	S4.5	23	S4.10	14	S4.15	8
S4.1	1064	S4.6	11	S4.11	2	S4.16	5
S4.2	26	S4.7	59	S4.12	5	S4.17	3
S4.3	98	S4.8	5	S4.13	26	S4.18	6

Tablica 13: Broj rastava na dvije simetrične konfiguracije.

rem 5.33] konstruirani su $S(2, 5, 41)$ dizajni s automorfizmom reda 3 (rezultat je također objavljen u [57]). Postoji 12 takvih dizajna, od kojih su 9 bili novi. Još jedan primjer s punom grupom automorfizama reda 2 konstruiran je u [56]. Tih 15 dizajna su jedini poznati primjeri za $S(2, 5, 41)$.

Program `tspartition.c` nalazi particije na dvije simetrične konfiguracije ispitujući sve mogućnosti. Zbog “backtrackinga” ispituje se puno manje od $\binom{2v}{v}$ podskupova pravaca, ali ipak previše u slučaju $S(2, 5, 41)$ dizajna. Za njih particije nalazimo nepotpunom lokalnom potragom, pomoću hill-climbing programa `tschillpart.c`. Ukratko opisujemo algoritam pomoću oznaka iz prethodne cjeline.

Skup rješenja X sadrži v -člane podskupove pravaca. Susjedni su podskupovi koji se razlikuju samo u jednom pravcu (dakle, podskupove u $N(x)$ dobivamo izbacivanjem jednog pravca iz x i dodavanjem nekog drugog). Označimo sa $r_P(x)$ broj pravaca iz x incidentnih s točkom P . Tada funkciju cilja definiramo sa $c(x) = \sum_P (r_P(x) - k)^2$. Incidencijske strukture sastavljene od pravaca iz skupa x i njemu komplementarnog skupa su konfiguracije ako i samo ako je $c(x) = 0$.

Program počinje od pseudoslučajno izabranog skupa pravaca $x \in X$. U svakoj iteraciji pseudoslučajnim izborom bira se pravac iz skupa x i drugi pravac koji ne pripada skupu x . Pravci se zamjenjuju ako se time smanjuje vrijednost ciljne funkcije, a u suprotnom se prelazi na sljedeću iteraciju bez zamjene. Na taj način vrlo brzo smo dobili particije 15 poznatih $S(2, 5, 41)$ dizajna na dvije simetrične (41_5) konfiguracije.

Na ovom problemu vidi se prednost nepotpune heurističke potrage nad potpunom potragom s backtrackingom. Za particioniranje 18 dizajna $S(2, 4, 25)$ pomoću programa `tspartition.c` potrošeno je nekoliko tjedana procesorskog vremena, a pomoću programa `tschillpart.c` mogu se particionirati u svega nekoliko sekundi. Nedostatak je, naravno, što dobivamo samo jednu particiju za svakog, a kod potpune potrage sve moguće particije.

Egzistencija $S(2, k, k^2 - 2k + 1)$ dizajna je za $k \geq 6$ otvoren problem. Zaključujemo da su svi poznati primjeri $S(2, k, 2k^2 - 2k + 1)$ dizajna ujedno

TSC prostori, ali primjera ima premalo da bi na osnovu toga formulirali općenitu hipotezu. “Protuprimjere” nalazimo među bliskim incidencijskim strukturama, konfiguracijama s dvostruko više točaka nego pravaca. Pomoću programa `tabuconf.c` konstruirali smo 100 konfiguracija $(14_6, 28_3)$, zatim smo primjenjivali program `tscpartition.c`. Tako je pronađena **sljedeća** $(14_6, 28_3)$ konfiguracija koju nije moguće rastaviti na dvije simetrične (14_3) konfiguracije:

{1, 2, 12}	{1, 3, 5}	{1, 6, 10}	{1, 7, 13}	{1, 8, 9}
{1, 11, 14}	{2, 3, 13}	{2, 4, 6}	{2, 5, 7}	{2, 8, 10}
{2, 9, 11}	{3, 4, 8}	{3, 7, 10}	{3, 9, 14}	{3, 11, 12}
{4, 5, 13}	{4, 7, 11}	{4, 9, 12}	{4, 10, 14}	{5, 6, 11}
{5, 8, 14}	{5, 9, 10}	{6, 7, 9}	{6, 8, 12}	{6, 13, 14}
{7, 12, 14}	{8, 11, 13}	{10, 12, 13}		

Za primjer nerastavljive $(15_6, 30_3)$ konfiguracije bilo je potrebno pretražiti oko 10000 konfiguracija konstruiranih programom `tabuconf.c`. Pomoću programa `tschillpart.c` brzo smo izdvojili one koji se mogu rastaviti, a na ostale smo primjenjivali sporiji program `tscpartition.c`. Pronađena je **sljedeća** $(15_6, 30_3)$ konfiguracija koju nije moguće rastaviti na dvije simetrične (15_3) konfiguracije:

{1, 2, 11}	{1, 3, 14}	{1, 4, 5}	{1, 6, 15}	{1, 7, 8}
{1, 9, 10}	{2, 4, 14}	{2, 5, 12}	{2, 6, 9}	{2, 8, 10}
{2, 13, 15}	{3, 4, 10}	{3, 5, 15}	{3, 6, 7}	{3, 9, 12}
{3, 11, 13}	{4, 6, 11}	{4, 7, 13}	{4, 8, 12}	{5, 6, 8}
{5, 7, 9}	{5, 10, 13}	{6, 12, 13}	{7, 10, 14}	{7, 11, 12}
{8, 9, 15}	{8, 11, 14}	{9, 13, 14}	{10, 11, 15}	{12, 14, 15}

Istom tehnikom pronađena je **sljedeća** nerastavljiva $(16_6, 32_3)$ konfiguracija:

{1, 2, 6}	{1, 3, 16}	{1, 4, 14}	{1, 5, 12}	{1, 7, 8}
{1, 9, 10}	{2, 3, 8}	{2, 4, 13}	{2, 5, 15}	{2, 7, 11}
{2, 10, 16}	{3, 5, 14}	{3, 6, 12}	{3, 7, 9}	{3, 11, 15}
{4, 6, 16}	{4, 8, 11}	{4, 9, 12}	{4, 10, 15}	{5, 7, 16}
{5, 8, 10}	{5, 11, 13}	{6, 8, 13}	{6, 9, 11}	{6, 14, 15}
{7, 10, 14}	{7, 13, 15}	{8, 12, 14}	{9, 13, 14}	{9, 15, 16}
{10, 11, 12}	{12, 13, 16}			

Dakle, ako se može dokazati da se svaki $S(2, k, v)$ dizajn s $v = 2k^2 - 2k + 1$ rastavlja na dvije simetrične (v_k) konfiguracije, u dokazu se mora koristiti svojstvo da su svake dvije točke spojene jedinstvenim pravcem (koje nedostaje u definiciji konfiguracije). S druge strane, ako tvrdnja ne vrijedi,

za dokaz je potrebno naći primjer nerastavljivog $S(2, k, 2k^2 - 2k + 1)$ dizajna. Vidjeli smo da se svi poznati primjeri mogu rastaviti, a procjenjujemo da će nove primjere biti vrlo teško konstruirati.

4 Dodatak

Provjera rezultata klasifikacije i prebrojavanja frekvencijskih kvadrata

■ Broj (reduciranih) frekvencijskih kvadrata

λ	$ f(6; \lambda) $	$ F(6; \lambda) $
{5, 1}	24	720
{4, 2}	453	67950
{4, 1, 1}	318	190800
{3, 3}	1486	297200
{3, 2, 1}	3028	5450400
{3, 1, 1, 1}	2128	15321600
{2, 2, 2}	13185	35599500
{2, 2, 1, 1}	9282	100245600
{2, 1, 1, 1, 1}	6552	283046400
{1, 1, 1, 1, 1, 1}	9408	812851200

λ	$ f(7; \lambda) $	$ F(7; \lambda) $
{6, 1}	120	5040
{5, 2}	9876	3110940
{5, 1, 1}	7416	9344160
{4, 3}	98484	68938800
{4, 2, 1}	285948	1801472400
{4, 1, 1, 1}	214752	5411750400
{3, 3, 1}	1185336	9956822400
{3, 2, 2}	4582740	86613786000
{3, 2, 1, 1}	3442464	260250278400
{3, 1, 1, 1, 1}	2586432	782137036800
{2, 2, 2, 1}	19969380	2264527692000
{2, 2, 1, 1, 1}	14998608	6803368588800
{2, 1, 1, 1, 1, 1}	11270400	20449013760000
{1, 1, 1, 1, 1, 1, 1}	16942080	61479419904000

λ	$ f(8; \lambda) $	$ F(8; \lambda) $
{7, 1}	720	40320
{6, 2}	318930	187530840
{6, 1, 1}	254280	598066560
{5, 3}	12268464	24046189440
{5, 2, 1}	50377968	888667355520
{5, 1, 1, 1}	40171008	2834466324480
{4, 4}	47740325	116963796250
{4, 3, 1}	771067692	30225853526400
{4, 2, 2}	3971210355	350260753311000
{4, 2, 1, 1}	3166707276	1117214326972800
{4, 1, 1, 1, 1}	2525457024	3563924952268800
{3, 3, 2}	20826177696	2449158497049600
{3, 3, 1, 1}	16608228480	7812510676992000
{3, 2, 2, 1}	85538838240	90534306393216000
{3, 2, 1, 1, 1}	68220465792	288818163977011200
{3, 1, 1, 1, 1, 1}	54413316096	921456860096102400
{2, 2, 2, 2}	660892740516	1049233314843201600
{2, 2, 2, 1, 1}	527062142160	3347055427572864000
{2, 2, 1, 1, 1, 1}	420413623488	10679178698392780800
{2, 1, 1, 1, 1, 1, 1}	335390189568	34077789757322035200
{1, 1, 1, 1, 1, 1, 1, 1}	535281401856	108776032459082956800

■ **Klasifikacija frekvencijskih kvadrata obzirom na izotopiju**

$n = 6$ $\lambda = \{5, 1\}$

|Aut| Br.klasa

720 1

$\Sigma =$ 1

720 True

$n = 6$ $\lambda = \{4, 2\}$

|Aut| Br.klasa

12 1

32 1

72 1

384 1

$\Sigma =$ 4

67950 True

$n = 6$ $\lambda = \{4, 1, 1\}$

|Aut| Br.klasa

12 1

16 1

36 1

96 1

$\Sigma =$ 4

190800 True

$n = 6$ $\lambda = \{3, 3\}$

|Aut| Br.klasa

8 1

24 3

48 1

64 1

5184 1

$\Sigma =$ 7

297200 True

$n = 6$ $\lambda = \{3, 2, 1\}$

|Aut| Br.klasa

1 6

2 5

3 1

4 3

6 4

8 1

12 1

24 1

72 1

$\Sigma =$ 23

5450400 True

$n = 6$ $\lambda = \{3, 1, 1, 1\}$

|Aut| Br.klasa

1 1

2 5

4 2

6 4

12 3

108 1

$\Sigma =$ 16

15321600 True

$n = 6$ $\lambda = \{2, 2, 2\}$

|Aut| Br.klasa

1 3

2 9

4 9

6 3

8 3

12 4

16 3

24 4

36 3

48 2

288 2

1152 1

$\Sigma =$ 46

35599500 True

$n = 6$ $\lambda = \{2, 2, 1, 1\}$

|Aut| Br.klasa

1 22

2 37

3 1

4 19

6 3

8 12

12 7

24 4

96 1

$\Sigma =$ 106

100245600 True

n = 6 $\lambda = \{2, 1, 1, 1, 1\}$

|Aut| Br.klasa

1 10

2 17

4 9

6 3

8 7

12 5

18 1

24 3

36 1

$\Sigma =$ 56

283046400 True

n = 6 $\lambda = \{1, 1, 1, 1, 1, 1\}$

|Aut| Br.klasa

4 5

8 4

12 3

24 1

36 3

72 1

108 1

120 3

216 1

$\Sigma =$ 22

812851200 True

n = 7 $\lambda = \{6, 1\}$

|Aut| Br.klasa

5040 1

$\Sigma =$ 1

5040 True

$n = 7$ $\lambda = \{5, 2\}$

|Aut| Br.klasa

14 1

40 1

48 1

192 1

$\Sigma =$ 4

3110940 True

$n = 7$ $\lambda = \{5, 1, 1\}$

|Aut| Br.klasa

14 1

20 1

24 1

48 1

$\Sigma =$ 4

9344160 True

$n = 7$ $\lambda = \{4, 3\}$

|Aut| Br.klasa

2 2

3 1

4 3

6 1

8 2

14 1

16 1

32 1

48 2

168 1

864 1

$\Sigma =$ 16

68938800 True

$n = 7$	$\lambda = \{4, 2, 1\}$
$ \text{Aut} $	Br.klasa
1	55
2	30
4	2
7	2
14	1
24	1
48	1
-----	-----
$\Sigma =$	92
1801472400	True

$n = 7$	$\lambda = \{4, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	21
2	27
3	1
6	3
14	1
21	1
24	1
72	1
-----	-----
$\Sigma =$	56
5411750400	True

$n = 7$	$\lambda = \{3, 3, 1\}$
$ \text{Aut} $	Br.klasa
1	175
2	36
3	4
4	2
6	4
7	1
8	2
14	1
42	1
-----	-----
$\Sigma =$	226
9956822400	True

$n = 7$	$\lambda = \{3, 2, 2\}$
$ \text{Aut} $	Br.klasa
1	1512
2	353
4	60
7	1
8	7
14	3
16	2
32	1
-----	-----
$\Sigma =$	1939
86613786000	True

$n = 7$	$\lambda = \{3, 2, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	4951
2	341
4	2
7	4
14	2
-----	-----
$\Sigma =$	5300
260250278400	True

$n = 7$	$\lambda = \{3, 1, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	1185
2	178
3	15
4	13
6	1
8	3
14	1
21	1
24	1
-----	-----
$\Sigma =$	1398
782137036800	True

$n = 7$ $\lambda = \{2, 2, 2, 1\}$

|Aut| Br.klasa

1 14473

2 747

3 18

4 15

6 7

7 1

8 3

14 2

21 1

42 1

48 1

 $\Sigma =$ 15269

2264527692000 True

$n = 7$ $\lambda = \{2, 2, 1, 1, 1\}$

|Aut| Br.klasa

1 21836

2 960

4 11

7 1

8 2

14 3

 $\Sigma =$ 22813

6803368588800 True

$n = 7$	$\lambda = \{2, 1, 1, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	6491
2	425
4	16
5	1
8	4
10	3
14	1
-----	-----
$\Sigma =$	6941
20449013760000	True

$n = 7$	$\lambda = \{1, 1, 1, 1, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	415
2	118
3	7
4	6
5	5
6	3
8	6
12	1
24	1
168	1
294	1
-----	-----
$\Sigma =$	564
61479419904000	True

$n = 8$	$\lambda = \{7, 1\}$
$ \text{Aut} $	Br.klasa
40320	1
-----	-----
$\Sigma =$	1
40320	True

$n = 8$ $\lambda = \{6, 2\}$

|Aut| Br.klasa

16 1

48 1

60 1

128 1

256 1

288 1

6144 1

$\Sigma =$ 7

187530840 True

$n = 8$ $\lambda = \{6, 1, 1\}$

|Aut| Br.klasa

16 1

24 1

30 1

64 2

72 1

768 1

$\Sigma =$ 7

598066560 True

$n = 8$	$\lambda = \{5, 3\}$
$ \text{Aut} $	Br.klasa
1	5
2	11
4	10
8	9
12	2
16	5
24	2
32	2
48	1
64	1
360	1
864	1
1152	1
-----	-----
$\Sigma =$	51
24046189440	True

$n = 8$	$\lambda = \{5, 2, 1\}$
$ \text{Aut} $	Br.klasa
1	495
2	90
4	21
8	7
12	3
16	2
30	1
32	2
60	1
64	1
128	1
-----	-----
$\Sigma =$	624
888667355520	True

$n = 8$	$\lambda = \{5, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	236
2	97
3	2
4	15
6	5
8	2
12	1
16	5
18	1
30	1
32	2
48	1
64	1
192	1
-----	-----
$\Sigma =$	370
2834466324480	True

$n = 8$	$\lambda = \{4, 4\}$
$ \text{Aut} $	Br.klasa
1	11
2	22
4	37
8	22
12	5
16	13
24	1
32	15
48	2
64	6
96	2
128	6
192	2
256	2
288	2
384	1
1024	2
4096	1
4608	2
5184	1
1327104	1
-----	-----
$\Sigma =$	156
116963796250	True

$n = 8$	$\lambda = \{4, 3, 1\}$
$ \text{Aut} $	Br.klasa
1	18225
2	678
3	10
4	79
6	12
8	20
12	3
16	9
24	1
48	1
64	1
72	1
1152	1
-----	-----
$\Sigma =$	19041
30225853526400	True

$n = 8$	$\lambda = \{4, 2, 2\}$
$ \text{Aut} $	Br.klasa
1	104196
2	6508
4	954
8	253
16	72
32	35
64	13
128	4
256	5
512	1
2048	1
4096	1
-----	-----
$\Sigma =$	112043
350260753311000	True

$n = 8$	$\lambda = \{4, 2, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	340250
2	6492
4	406
8	87
16	18
32	6
64	2
128	1
256	1
-----	-----
$\Sigma =$	347263
1117214326972800	True

$n = 8$	$\lambda = \{4, 1, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	89481
2	3446
3	62
4	405
6	19
8	89
12	6
16	32
24	4
32	8
64	3
96	1
128	2
192	1
256	1
768	1
-----	-----
$\Sigma =$	93561
3563924952268800	True

$n = 8$	$\lambda = \{3, 3, 2\}$
$ \text{Aut} $	Br.klasa
1	741377
2	22754
3	1
4	1891
6	4
8	215
12	17
16	78
24	10
32	7
64	3
96	2
128	2
-----	-----
$\Sigma =$	766361
2449158497049600	True

$n = 8$	$\lambda = \{3, 3, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	1191820
2	18577
3	5
4	1088
6	19
8	127
12	20
16	28
24	8
32	12
64	4
96	2
-----	-----
$\Sigma =$	1211710
7812510676992000	True

$n = 8$	$\lambda = \{3, 2, 2, 1\}$
Aut	Br.klasa
1	27824782
2	39397
4	717
8	102
16	21
32	2
64	1
128	2
-----	-----
$\Sigma =$	27865024
90534306393216000	True

$n = 8$	$\lambda = \{3, 2, 1, 1, 1\}$
Aut	Br.klasa
1	29587375
2	43910
3	63
4	823
6	27
8	107
12	4
16	32
24	1
32	4
48	2
-----	-----
$\Sigma =$	29632348
288818163977011200	True

$n = 8$	$\lambda = \{3, 1, 1, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	4711984
2	22370
3	155
4	547
6	48
8	73
10	3
12	9
16	33
24	6
32	5
48	1
64	3
192	1
-----	-----
$\Sigma =$	4735238
921456860096102400	True

$n = 8$	$\lambda = \{2, 2, 2, 2\}$
$ \text{Aut} $	Br.klasa
1	26807345
2	163022
3	231
4	10385
6	132
8	1674
12	52
16	375
24	29
32	123
48	13
64	38
96	6
128	19
192	1
256	11
768	2
1024	4
1536	2
8192	1
24576	1
-----	-----
$\Sigma =$	26983466
1049233314843201600	True

$n = 8$	$\lambda = \{2, 2, 2, 1, 1\}$
Aut	Br.klasa
1	171432492
2	271401
3	647
4	4841
6	203
8	359
12	35
16	108
24	7
32	15
48	4
64	6
256	1
768	1
-----	-----
$\Sigma =$	171710120
3347055427572864000	True

$n = 8$	$\lambda = \{2, 2, 1, 1, 1, 1\}$
Aut	Br.klasa
1	136712035
2	277816
4	9180
8	1124
16	199
32	60
64	13
128	4
256	4
-----	-----
$\Sigma =$	137000435
10679178698392780800	True

$n = 8$	$\lambda = \{2, 1, 1, 1, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	29066158
2	93679
3	114
4	2511
5	24
6	105
8	296
10	6
12	25
16	86
24	7
32	18
48	6
64	8
128	2
384	2
-----	-----
$\Sigma =$	29163047
34077789757322035200	True

$n = 8$	$\lambda = \{1, 1, 1, 1, 1, 1, 1, 1\}$
$ \text{Aut} $	Br.klasa
1	1644434
2	28767
3	310
4	1854
5	12
6	136
7	2
8	397
10	12
12	55
16	172
24	21
32	36
42	5
48	7
64	14
96	8
128	12
192	6
256	3
512	2
1536	1
10752	1
-----	-----
$\Sigma =$	1676267
108776032459082956800	True

■ Klasifikacija petlji obzirom na izomorfizam

$n = 8$

$ \text{Aut} $	Br.klasa
1	106185390
2	41088
3	1574
4	411
5	156
6	175
7	2
8	28
10	12
12	4
24	3
42	5
168	1
-----	-----
$\Sigma =$	106228849
535281401856	True

Literatura

- [1] V.L.Arlazarov, A.M.Baraev, J.U.Golfand, I.A.Faradžev, *Postroenie pomostciu EVM vseh latinskih kvadratov porjadka 8*, Algoritmiceskie Issledovanija v Kombinatorike, Nauka, Moskva, 1978.
- [2] D.Avis, K.Fukuda, *Reverse search for enumeration*, Discrete Applied Mathematics **65** (1996), 21-46.
- [3] L.M.Batten, A.Beutelspacher, *The theory of finite linear spaces*, Cambridge University Press, 1993.
- [4] S.E.Bammel, J.Rothstein, *The number of 9×9 Latin squares*, Discrete Mathematics **11** (1975), 93–95.
- [5] T.Beth, D.Jungnickel, H.Lenz, *Design theory, Vol. I.*, 2nd ed., Encyclopedia of Mathematics and Its Applications **69**, Cambridge University Press, 1999.
- [6] T.Beth, D.Jungnickel, H.Lenz, *Design theory, Vol. II.*, 2nd ed., Encyclopedia of Mathematics and Its Applications **78**, Cambridge University Press, 1999.
- [7] A.Betten, D.Betten, *Regular linear spaces*, Beiträge zur Algebra und Geometrie **38** (1997), 111–124.
- [8] A.Betten, D.Betten, *The proper linear spaces on 17 points*, Discrete Applied Mathematics **95** (1999), 83-108.
- [9] A.Betten, D.Betten, *Linear spaces with at most 12 points*, Journal of Combinatorial Designs **7** (1999), 119-145.
- [10] A.Betten, D.Betten, *Tactical decompositions and some configurations v_4* , Journal of Geometry **66** (1999), 27–41.
- [11] A.Betten, D.Betten, *Note on the proper linear spaces on 18 points*, Algebraic combinatorics and applications. Proceedings of the Euroconference ALCOMA, Springer, 2001, pp. 40-54.
- [12] A.Betten, D.Betten, V.D.Tonchev, *Unitals and codes*, Discrete Mathematics **267** (2003), 23–33.
- [13] I.Bluskov, *Optimization algorithms and cyclic designs*, Journal of Geometry **67** (2000), 42–49.

- [14] P.Bofill, *Optimizing neural networks for the generation of block designs*, Technical Report UPC-DAC-1997-76 (engleska verzija disertacije), Universitat Politècnica de Catalunya, 1997.
- [15] P.Bofill, C.Torras, *Neural cost functions and search strategies for the generation of block designs: an experimental evaluation*, International Journal of Neural Systems **11** (2001), 189–202.
- [16] R.C.Bose, *On the construction of balanced incomplete block designs*, Annals of Eugenics **9** (1939), 353–399.
- [17] L.J.Brant, G.J.Mullen, *A note on isomorphism classes of reduced Latin squares of order 7*, Utilitas Mathematica **27** (1985), 261–263.
- [18] L.J.Brant, G.L.Mullen, *Some results on enumeration and isotopic classification of frequency squares*, Utilitas Mathematica **29** (1986), 231–244.
- [19] A.E.Brouwer, *Some unitals on 28 points and their embeddings in projective planes of order 9*, Geometries and Groups, Proc. Colloq. Berlin 1981, Lecture Notes in Mathematics **893** (1981), 183–188.
- [20] J.W.Brown, *Enumeration of Latin squares with application to order 8*, Journal of Combinatorial Theory **5** (1968), 177–184.
- [21] B.F.Bryant, H.Schneider, *Principal loop-isotopes of quasigroups*, Canadian Journal of Mathematics **18** (1966), 120–125.
- [22] Y.Chang, *A bound for Wilson’s theorem II*, Journal of Combinatorial Designs **4** (1996), 11–26.
- [23] C.J.Colbourn, *A Steiner 2-design with an automorphism fixing exactly $r + 2$ points*, Journal of Combinatorial Designs **7** (1999), 375–380.
- [24] C.J.Colbourn, J.H.Dinitz (eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, 1996.
- [25] C.J.Colbourn, R.C.Read, *Orderly algorithms for generating restricted classes of graphs*, Journal of Graph Theory **3** (1979), 187–195.
- [26] J.Dénes, A.D.Keedwell, *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.
- [27] J.Dénes, A.D.Keedwell, *Latin squares. New developments in the theory and applications*, North-Holland, Amsterdam, 1991.

- [28] J.Dénes, G.L.Mullen, *Enumeration formulas for latin and frequency squares*, Discrete Mathematics **111** (1993), 157–163.
- [29] R.H.F.Denniston, *A Steiner system with a maximal arc*, Ars Combinatoria **9** (1980), 247–248.
- [30] P.C.Denny, *Search and enumeration techniques for incidence structures*, CDMTCS Technical Report **85**, University of Auckland, 1998.
- [31] P.C.Denny, P.B.Gibbons, *Case studies and new results in combinatorial enumeration*, Journal of Combinatorial Designs **8** (2000), 239–260.
- [32] L.Euler, *Recherches sur une nouvelle espèce de quarrés magiques*, St. Petersburg, 1779.
- [33] I.A.Faradžev, *Constructive enumeration of combinatorial objects*, Problèmes combinatoires et théorie des graphes, Colloq. Internat. CNRS **260**, Paris, 1978, pp. 131–135.
- [34] F.Franek, T.S.Griggs, C.C.Lindner, A.Rosa, *Completing the spectrum of 2-chromatic $S(2, 4, v)$* , Discrete Mathematics **247** (2002), 225–228.
- [35] M.Frolov, *Recherches sur les permutations carrées*, J. Math. Spec. de Longchamps **4** (1890), 1–4.
- [36] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3* (2002), <http://www.gap-system.org>.
- [37] A.Geist et al, *PVM: Parallel Virtual Machine. A User's Guide and Tutorial for Networked Parallel Computing*, MIT Press, 1994.
- [38] I.M.Gessel, *Counting latin rectangles*, Bulletin of the American Mathematical Society **16** (1987), 79–82.
- [39] L.A.Goldberg, *Efficient algorithms for listing unlabeled graphs*, Journal of Algorithms **13** (1992), 128–143.
- [40] H.Hanani, *The existence and construction of balanced incomplete block designs*, Annals of Mathematical Statistics **32** (1961), 361–386.
- [41] H.Hanani, *Balanced incomplete block designs and related designs*, Discrete Mathematics **11** (1975), 255–369.
- [42] J.Heitzig, J.Reinhold, *Counting finite lattices*, Algebra Universalis **48** (2002), 43–53.

- [43] S.K.Houghten, L.H.Thiel, J.Janssen, C.W.H.Lam, *There is no (46, 6, 1) block design*, Journal of Combinatorial Designs **9** (2001), 60–71.
- [44] Z.Janko, V.D.Tonchev, *New designs with block size 7*, Journal of Combinatorial Theory A **83** (1998), 152–157.
- [45] W.Johnson, *The diophantine equation $X^2 + 7 = 2^n$* , American Mathematical Monthly **94** (1987), 59–62.
- [46] C.F.Laywine, G.L.Mullen, *Discrete mathematics using Latin squares*, Wiley, 1998.
- [47] P.Kaski, *Isomorph-free exhaustive generation of combinatorial designs*, Laboratory for Theoretical Computer Science Research Reports **70**, Helsinki University of Technology, 2002.
- [48] P.Kaski, *A census of Steiner triple systems and some related combinatorial objects*, Laboratory for Theoretical Computer Science Research Reports **78**, Helsinki University of Technology, 2003.
- [49] P.Kaski, P.R.J.Östergård, *The Steiner triple systems of order 19*, preprint (Mathematics of Computation).
- [50] P.Kaski, P.R.J.Östergård, *Miscellaneous classification results for 2-designs*, Discrete Mathematics **280** (2004), 65–75.
- [51] T.P.Kirkman, *On a problem in combinatorics*, Cambridge and Dublin Mathematical Journal **2** (1847), 191–204.
- [52] W.Kocay, *On writing isomorphism programs*, Computational and Constructive Design Theory, W.D.Wallis (ed.), Kluwer, 1996, pp. 135–175.
- [53] G.Kolesova, C.W.H.Lam, L.Thiel, *On the number of 8×8 Latin squares*, Journal of Combinatorial Theory A **54** (1990), 143–148.
- [54] V.Krčadinac, *Klasifikacija konačnih projektivnih ravnina reda 7 i 8*, diplomski rad, Matematički odjel, Sveučilište u Zagrebu, 1996.
- [55] V.Krčadinac, *Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$* , magistarski rad, Matematički odjel, Sveučilište u Zagrebu, 1999.
- [56] V.Krčadinac, *A new Steiner $S(2, 5, 41)$ design (sažetak)*, 2nd Croatian Congress of Mathematics, Hrvatsko matematičko društvo, 2000.

- [57] V.Krčadinac, *Steiner 2-designs $S(2, 5, 41)$ with automorphisms of order 3*, Journal of Combinatorial Mathematics and Combinatorial Computing **43** (2002), 83-99.
- [58] V.Krčadinac, *Steiner 2-designs $S(2, 4, 28)$ with nontrivial automorphisms*, Glasnik Matematički **37(57)** (2002), 259-268.
- [59] V.Krčadinac, *Constructing block designs by tabu search*, preprint.
- [60] V.Krčadinac, *Some new Steiner 2-designs $S(2, 4, 37)$* , preprint.
- [61] V.Krčadinac, J.Šiftar, *Finite linear spaces consisting of two symmetric configurations*, preprint.
- [62] D.L.Kreher, D.R.Stinson, *Combinatorial algorithms: generation, enumeration and search*, CRC Press, 1999.
- [63] D.L.Kreher, D.R.Stinson, L.Zhu, *On the maximum number of fixed points in automorphisms of prime order of $2-(v, k, 1)$ designs*, Annals of Combinatorics **1** (1997), 227–243.
- [64] J.S.Leon, *An algorithm for computing the automorphism group of a Hadamard matrix*, Journal of Combinatorial Theory A **27** (1979), 289–306.
- [65] J.S.Leon, *Computing automorphism groups of combinatorial objects*, Computational Group Theory, M.D.Atkinson (ed.), Academic Press, 1984, pp. 321–335.
- [66] H.Lüneburg, *Some remarks concerning the Ree groups of type (G_2)* , Journal of Algebra **3** (1966), 256–259.
- [67] R.Mathon, *Computational methods in design theory*, Computational and Constructive Design Theory, W.D.Wallis (ed.), Kluwer, 1996, pp. 29–48.
- [68] R.Mathon, K.T.Phelps, A.Rosa, *Small Steiner triple systems and their properties*, Ars Combinatoria **15** (1983), 3–110.
- [69] B.D.McKay, *Computing automorphisms and canonical labellings of graphs*, Combinatorial Mathematics, D.A.Holton, J.Seberry (ed.), Lecture Notes in Mathematics **686**, Springer–Verlag, 1977, pp. 223–232.
- [70] B.D.McKay, *nauty user's guide (version 1.5)*, Technical Report TR-CS-90-02, Department of Computer Science, Australian National University, 1990.

- [71] B.D.McKay, *Isomorph-free exhaustive generation*, Journal of Algorithms **26** (1998), 306–324.
- [72] B.D.McKay, E.Rogoyski, *Latin squares of order 10*, Electronic Journal of Combinatorics **2** (1995), #N3.
- [73] M.Meringer, *Fast generation of regular graphs and construction of cages*, Journal of Graph Theory **30** (1999), 137–146.
- [74] M.Meszka, A.Rosa, *Embedding Steiner triple systems into Steiner systems $S(2, 4, v)$* , Discrete Mathematics **274** (2004), 199–212.
- [75] W.H.Mills, *BIBDs with $k = 6$ and $\lambda = 1$* , Computational and Constructive Design Theory, W.D.Wallis (ed.), Kluwer, 1996, pp. 189–226.
- [76] L.B.Morales, *Constructing difference families through an optimization approach: six new BIBDs*, Journal of Combinatorial Designs **8** (2000), 261–273.
- [77] L.B.Morales, *Two new 1-rotational $(36, 9, 8)$ and $(40, 10, 9)$ RBIBDs*, Journal of Combinatorial Mathematics and Combinatorial Computing **36** (2001), 119–126.
- [78] L.B.Morales, C.Velarde, *A complete classification of $(12, 4, 3)$ -RBIBDs*, Journal of Combinatorial Designs **9** (2001), 385–400.
- [79] J.R.Nechvatal, *Asymptotic enumeration of generalised Latin rectangles*, Utilitas Mathematica **20** (1981), 273–292.
- [80] H.W.Norton, *The 7×7 squares*, Annals of Eugenics **9** (1939), 269–307.
- [81] P.R.J.Östergård, *Enumeration of 2 - $(12, 3, 2)$ designs*, Australasian Journal of Combinatorics **22** (2000), 227–231.
- [82] T.Pentilla, G.F.Royle, *Sets of type (m, n) in the affine and projective planes of order 9*, Designs, Codes and Cryptography **6** (1995), 229–245.
- [83] C.Pietsch, *On the classification of linear spaces of order 11*, Journal of Combinatorial Designs **3** (1995), 185–193.
- [84] S.Prestwich, *A local search algorithm for balanced incomplete block designs*, International workshop on constraint solving and constraint logic programming, B.O’Sullivan (ed.), Lecture Notes in Computer Science **2627**, Springer, 2003, pp. 132–143.

- [85] R.C.Read, *Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations*, Annals of Discrete Mathematics **2** (1978), 107-120.
- [86] R.C.Read, D.G.Corneil, *The graph isomorphism disease*, Journal of Graph Theory **1** (1977), 339–363.
- [87] H.J.Ryser, *Combinatorial properties of matrices of zeros and ones*, Canadian Journal of Mathematics **9** (1957), 371–377.
- [88] A.Sade, *Enumeration des carrés latins. Applications au 7° ordre. Conjecture pour les ordres supérieurs*, Marseille, 1948.
- [89] A.Sade, *An omission in Norton's list of 7×7 squares*, Annals of Mathematical Statistics **22** (1951), 306-307.
- [90] A. Schinzel, and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arithmetica **4** (1958), 185-208.
- [91] J.Shao, W.Wei, *A formula for the number of Latin squares*, Discrete Mathematics **110** (1992), 293–296.
- [92] E. Spence, *A complete classification of symmetric $(31, 10, 3)$ designs*, Designs, Codes and Cryptography **2** (1992), 127–136.
- [93] E. Spence, *Classification of Hadamard matrices of orders 24 and 28*, Discrete Mathematics **140** (1995), 185–243.
- [94] E. Spence, *The complete classification of Steiner systems $S(2, 4, 25)$* , Journal of Combinatorial Designs **4** (1996), 295–300.
- [95] D.R.Stinson, H.Ferch, *2000000 Steiner triple systems of order 19*, Mathematics of Computation **44** (1985), 533–535.
- [96] J.Steiner, *Combinatorische Aufgabe*, Journal für die Reine und Angewandte Mathematik **45** (1853), 181–182.
- [97] J.Šiftar, *On the automorphism groups of $2-(46, 6, 1)$ and $2-(51, 6, 1)$ designs*, Glasnik Matematički **22(52)** (1987), 3–11.
- [98] J.Šiftar, B.Shita, *On rigidity of $2-(46, 6, 1)$ designs*, Glasnik Matematički **26(46)** (1991), 3–11.
- [99] D.Veljan, *Kombinatorika s teorijom grafova*, Školska knjiga, 1989.
- [100] V.Volenec, *Grupoidi, kvazigrupe i petlje*, Školska knjiga, 1982.

- [101] M.B.Wells, *The number of Latin squares of order eight*, Journal of Combinatorial Theory **3** (1967), 98–99.
- [102] R.M.Wilson, *An existence theory for pairwise balanced designs, III. Proof of the existence conjectures*, Journal of Combinatorial Theory A **18** (1975), 71–79.

Sažetak

U ovoj disertaciji proučavaju se algoritamske tehnike konstrukcije i klasifikacije konačnih matematičkih struktura kao što su blok dizajni, konačni linearni prostori, konfiguracije, latinski i frekvencijski kvadrati te orbitne matrice. Disertacija je podijeljena u tri poglavlja i dodatak.

U prvom poglavlju cilj je potpuno klasificirati promatrane strukture obzirom na neku relaciju ekvivalencije. Dan je općenit opis četiri klasifikacijska algoritma i dokazana je njihova valjanost. Najvažniji rezultati ovog poglavlja su klasifikacija nekih konačnih linearnih prostora, prebrojavanje i klasifikacija frekvencijskih kvadrata reda 7 i 8 i klasifikacija niza orbitnih matrica koje se kasnije koriste za konstrukciju Steinerovih 2-dizajna.

U drugom poglavlju primjenjuje se poznata tehnika konstrukcije blok dizajna sa zadanim grupama automorfizama na Steinerove 2-dizajne. Tehnika se prilagođava jednoj novoj klasi incidencijskih struktura, TSC prostorima (konačnim linearnim prostorima sastavljenim od dvije simetrične konfiguracije). Rezultati o Steinerovim 2-dizajnim su konstrukcija svih $S(2, 4, 28)$ dizajna s netrivialnim automorfizmima, konstrukcija velikog broja novih $S(2, 4, 37)$ dizajna s automorfizmima reda 2, 3 i 11 i još neki rezultati o grupama automorfizama dizajna $S(2, 5, 45)$, $S(2, 6, 61)$, $S(2, 6, 66)$ i $S(2, 7, 85)$. Pomoću diferencijskih familija konstruirani su linearni prostori $TSC(3, k)$ za $k = 5, 6, 7, 8$, a spomenutom tehnikom $TSC(4, 5)$ prostori s automorfizmima reda 3. Za nekoliko drugih parametara dokazano je nepostojanje TSC prostora s određenim automorfizmima. Osim toga dokazana je jedna općenita konstrukcija TSC prostora, zasnovana na konačnim projektivnim ravninama.

U trećem poglavlju pitanje egzistencije blok dizajna i drugih incidencijskih struktura postavlja se kao problem kombinatorne optimizacije i koristi se tabu search algoritam za njegovo rješavanje. Usporedbom s nekoliko sličnih algoritama iz literature pokazuje se da algoritam efikasnije nalazi blok dizajne s $vb \leq 1000$. Rezultati dobiveni pomoću algoritma su poboljšanje 36 donjih ocjena za broj neizomornih blok dizajna i konstrukcija simetrične (34_6) konfiguracije, čija je egzistencija bila nepoznata. Slična tehnika primjenjuje se na jedan drugi kombinatorni problem, pitanje je li svaki $S(2, k, v)$ dizajn s dvostruko više pravaca nego točaka ujedno $TSC(k, k)$ prostor. Dokazano je da tvrdnja vrijedi za sve poznate primjere $S(2, k, v)$ dizajna s $b = 2v$. Pronađeni su primjeri srodnih kombinatornih struktura za koje analogna tvrdnja ne vrijedi.

U dodatku su navedene distribucije klasa izotopije frekvencijskih kvadrata s obzirom na red pune grupe autotopija. Podaci omogućuju usporedbu rezultata klasifikacije s rezultatima prebrojavanja frekvencijskih kvadrata, dobivenih pomoću nezavisnih programa. Rezultati se u cijelosti slažu.

Summary

In this thesis algorithmic construction and classification techniques for finite mathematical structures such as block designs, finite linear spaces, configurations, Latin and frequency squares and orbit matrices are studied. The thesis is divided into three chapters and an appendix.

In the first chapter the goal is complete classification of certain structures with respect to some equivalence relation. Four classification algorithms are described and proved in a general setting. The main results in this chapter are classification of some finite linear spaces, enumeration and classification of frequency squares of order 7 and 8, and classification of various orbit matrices, used in the sequel for the construction of Steiner 2-designs.

In the second chapter the well-known construction technique for block designs with a prescribed automorphism group is applied to Steiner 2-designs. The technique is also adapted to a new class of incidence structures, TSC spaces (finite linear spaces consisting of two symmetric configurations). Results about Steiner 2-designs are construction of all $S(2, 4, 28)$ designs with nontrivial automorphisms, construction of many new $S(2, 4, 37)$ designs with automorphisms of order 2, 3 and 11, and some other results about automorphism groups of $S(2, 5, 45)$, $S(2, 6, 61)$, $S(2, 6, 66)$ and $S(2, 7, 85)$ designs. Linear spaces $TSC(3, k)$, $k = 5, 6, 7, 8$ are obtained from difference families and $TSC(4, 5)$ with automorphisms of order 3 by the aforementioned construction technique. For some other parameters nonexistence of TSC spaces with certain automorphism groups is proved. Furthermore, a general construction of TSC spaces based on finite projective planes is proved.

In the third chapter the existence of block designs and some other incidence structures is formulated as a combinatorial optimization problem and a tabu search algorithm is used to solve it. The algorithm is compared to several similar algorithms from the literature and shown to be more efficient for block designs with $vb \leq 1000$. Results obtained with the algorithm are improvement of 36 lower bounds on the number of nonisomorphic block designs and construction of a symmetric (34_6) configuration, whose existence had previously been unknown. A similar technique is applied to another combinatorial problem, the question whether every $S(2, k, v)$ design with twice as many lines as points is necessarily a $TSC(k, k)$ space. This is shown to be true for all known examples of $S(2, k, v)$ designs with $b = 2v$. Counterexamples are found amongst related combinatorial structures.

In the appendix distributions of isotopy classes of frequency squares by full automorphism group order are given. The data enables comparison of enumeration and classification results about frequency squares, obtained by independent computer programs. The results are consistent with each other.

Životopis

Rođen sam 26. studenog 1973. u Zagrebu. Osnovnu školu sam pohađao u Zagrebu i u Hamburgu, a srednju u Zagrebu (XV. Gimnazija - MIOC). Akademске godine 1992./93. upisao sam studij matematike na Matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Tokom treće i četvrte godine primao sam stipendiju grada Zagreba. Na četvrtoj godini dobio sam Rektorovu nagradu 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.sc. J.Šiftara. Diplomirao sam s odličnim uspjehom u prosincu 1996.

Akademске godine 1996./97. upisao sam poslijediplomski studij na Matematičkom odjelu. Od tada sudjelujem u radu *Seminara za geometriju*. U svibnju i lipnju 1998. pohađao sam tečaj kombinatorne geometrije u Cortoni (predavači prof.dr.sc. G.-C.Rota i prof.dr.sc. A.Beutelspacher), u organizaciji *Scuola Matematica Interuniversitaria*. Zimski semestar akademске godine 1998./99. bio sam na studijskom boravku na University of Glasgow, u posjetu prof.dr.sc. E.Spenceu. Magistrirao sam u listopadu 1999. s radom “Steinerovi 2-dizajni $S(k, 2k^2 - 2k + 1)$ ”, izrađenim pod vodstvom prof.dr.sc. J.Šiftara.

Od travnja 1997. zaposlen sam na Matematičkom odjelu kao znanstveni novak u istraživačkom zvanju mlađi asistent, na projektu *Geometrije i algebarsko-geometrijske strukture*. Od studenog 1999. do srpnja 2000. služio sam vojni rok. U listopadu 2000. izabran sam u istraživačko zvanje asistent. Na Matematičkom odjelu do sada sam vodio vježbe iz kolegija Matematička analiza 1 i 2 za dipl. inž. fizike, Linearna algebra 1 i 2, Matematika 1 i 2 za prof. fizike i politehnike, Uvod u računarstvo, Elementarna matematika 1 i 2, Linearna algebra 2 za dipl. inž. fizike, Uvod u optimizaciju, Kombinatorika, Računarski praktikum 1 i Konveksna analiza s primjenama.

Oženjen sam od prosinca 1997. Supruga Jelena Bekavac Krčadinac također je diplomirala matematiku i radi kao analitičar prodaje u jednoj međunarodnoj tvrtki. U listopadu 2001. dobili smo sina Jakova, a u studenom 2003. kćer Emu.