

Poopćenje i profinjenje nekih algoritama za konstrukciju blokovnih dizajna i istraživanje njihovih podstruktura

Dumičić Danilović, Doris

Doctoral thesis / Disertacija

2014

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:217:134492>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2025-01-03**



Repository / Repozitorij:

[Repository of the Faculty of Science - University of Zagreb](#)





Sveučilište u Zagrebu

PRIRODOSLOVNO-MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Doris Dumičić Danilović

**Poopćenje i profinjenje nekih algoritama za
konstrukciju blokovnih dizajna i istraživanje
njihovih podstruktura**

DOKTORSKI RAD

Zagreb, 2014.



UNIVERSITY OF ZAGREB
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Doris Dumičić Danilović

**Generalization and refinement of some
algorithms for construction and
substructures investigation of block designs**

DOCTORAL THESIS

Zagreb, 2014.



Sveučilište u Zagrebu

PRIRODOSLOVNO-MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Doris Dumičić Danilović

**Poopćenje i profinjenje nekih algoritama za
konstrukciju blokovnih dizajna i istraživanje
njihovih podstruktura**

DOKTORSKI RAD

Voditelji rada:

prof. dr. sc. Dean Crnković
izv. prof. dr. sc. Sanja Rukavina

Zagreb, 2014.



UNIVERSITY OF ZAGREB
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Doris Dumičić Danilović

**Generalization and refinement of some
algorithms for construction and
substructures investigation of block designs**

DOCTORAL THESIS

Supervisors:

Professor Dean Crnković, PhD
Professor Sanja Rukavina, PhD

Zagreb, 2014.

Na ovom mjestu željela bih izraziti zahvalnost prvenstveno mentorima prof. dr. sc. Deanu Crnkoviću i prof. dr. sc. Sanji Rukavini na vođenju i pomoći prilikom izrade ove disertacije, te na brojnim savjetima i usmjeravanju mojih interesa prema ovom zanimljivom području konstrukcija blokovnih dizajna.

Zahvaljujem se članovima povjerenstva doc. dr. sc. Vedrani Mikulić Crnković, prof. dr. sc. Vedranu Krčadincu i prof. dr. sc. Mariu Osvinu Pavčeviću na korisnim savjetima i sugestijama tijekom mojih izlaganja i čitanja ovog rada.

Zahvaljujem se i svim članovima Seminara za konačnu matematiku u Rijeci za korisne sugestije prilikom izlaganja seminara vezanih za disertaciju. Posebnu zahvalu dugujem svojoj obitelji na podršci i strpljenju svih ovih godina mojeg školovanja.

Sadržaj

Predgovor	1
1 Grupe	4
1.1 Uvod u teoriju grupa	4
1.2 Cikličke grupe	7
1.3 Permutacijske grupe	8
1.3.1 Djelovanje grupe na skup	9
1.4 Frobeniusove grupe	15
1.5 Kompozicijski niz grupe	16
2 Incidencijske strukture	19
2.1 Osnovni pojmovi	19
2.2 Uvod u teoriju dizajna	21
2.3 Izomorfizmi blokovnih dizajna	25
2.4 Unitali	30
3 Konstrukcije blokovnih dizajna s pretpostavljenom grupom automorfizama	33
3.1 Metoda taktičke dekompozicije i orbitne matrice	34
3.2 Algoritam za konstrukciju orbitnih matrica	43
3.3 Profinjenje orbitnih matrica	46
3.3.1 Profinjenje primjenom kompozicijskog niza rješive grupe	46
3.3.2 Klasifikacija 2-(45, 12, 3) dizajna s involutornim automorfizmom	49
4 Klasifikacija 2-(45, 5, 1) dizajna s automorfizmom reda šest	51
4.1 Djelovanje automorfizma reda šest na 2-(45, 5, 1) dizajn	52
4.2 Konstrukcija orbitnih matrica i njihovo profinjenje	64
5 Konstrukcija 2-(45, 5, 1) dizajna s grupom automorfizama $G \cong Z_3 \times Z_3$	67
5.1 Djelovanje grupe $G \cong Z_3 \times Z_3$ na 2-(45, 5, 1) dizajn	67
5.2 Konstrukcija orbitnih matrica i njihovo profinjenje	73

6	Konstrukcija 2-(45, 5, 1) dizajna s grupom automorfizama S_3	78
7	Klasifikacija 2-(78, 22, 6) dizajna s grupom automorfizama $Frob_{39} \times Z_2$	88
7.1	Djelovanje grupe $Frob_{39} \times Z_2$ na 2-(78, 22, 6) dizajn	89
7.2	Konstrukcija orbitnih matrica i njihovo profinjenje	96
8	Nepotpuna potraga za dizajnima primjenom genetskog algoritma	103
8.1	Modificirani genetski algoritam (MGU) za traženje unitala u simetričnim dizajnima	104
8.2	Modificirani genetski algoritam (MGPD) za traženje poddizajna u simetričnim dizajnima	111
	Bibliografija	116
	Prilog	121
	Sažetak	126
	Summary	127
	Životopis	128

Predgovor

Teorija dizajna je dio kombinatorne i diskretne matematike koja se bavi egzistencijom, konstrukcijom i klasifikacijom konačnih incidencijskih struktura. Ona doživljava nagli procvat od sredine 20. stoljeća zbog svoje široke primjene, te razvoja računala i programske podrške. Neka od područja primjene teorije dizajna su kriptografija, oblikovanje algoritama, tehnologija umrežavanja, bežična komunikacija, matematička biologija, te brojna druga polja.

Metoda konstrukcije blokovnih dizajna s određenom grupom automorfizama intenzivno se koristi od 80-tih godina 20. stoljeća. Takav je pristup u konstrukciji blokovnih dizajna, u kojoj je ključni pojam taktička dekompozicija konačne incidencijske strukture, među prvima upotrebljavao Z. Janko, a sastoji se od dva koraka: konstrukcije orbitnih matrica za zadane dopustive parametre dizajna $(v, k \text{ i } \lambda)$, te zadanu grupu automorfizama i konstrukcije blokovnih dizajna iz dobivenih orbitnih matrica, tzv. indeksiranje ([32]). V. Čepulić je razvio algoritam za konstrukciju orbitnih matrica za proizvoljne dopustive parametre simetričnih dizajna i proizvoljne distribucije duljina orbita točaka i blokova za djelovanje neke grupe automorfizama na dizajn ([21]). V. Krčadinac je u svojoj doktorskoj disertaciji [37] razvio programske alate za konstrukciju 2 - $(v, k, 1)$ dizajna za dopustive parametre v i k , uz ograničenje da je pripadna grupa automorfizama prostog reda. Postupak indeksiranja orbitnih matrica često traje predugo zbog prevelikog broja mogućnosti za indeksne skupove koje računalni programi trebaju ispitati. Stoga, kako bi se provelo indeksiranje, potrebno je napraviti odgovarajuće profinjenje (dekompoziciju) orbitne matrice, što je moguće realizirati za djelovanje grupe koja nije prostog reda. Profinjenje je do sada napravljeno samo za neke specijalne slučajeve simetričnih dizajna i posebne grupe automorfizama, kao na primjer u [15], [17], [55] i [57]. D. Crnković i S. Rukavina u [18] opisuju primjenu glavnog niza Abelove grupe u svrhu provedbe profinjenja orbitnih matrica blokovnih dizajna na koje djeluje takva grupa, međutim računalni programi koji provode takvo profinjenje, u općenitom slučaju, do sada nisu bili razvijeni.

Heurističke metode (tabu search, hill-climbing, simulated annealing, genetski algoritam) su prikladne za rješavanje niza kombinatoričkih optimizacijskih problema. Primjena heurističkih metoda je prikladnija za veće probleme, kada metode direktne i iscrpne pretrage ne daju rezultate ili ne daju dovoljno rezultata u razumnom vremenu. Nema garancije da će heuristički algoritmi pronaći optimalno rješenje, međutim odlika dobrih

heurističkih algoritama je da često puta pronalaze optimalna rješenja ili njihove dovoljno dobre aproksimacije. Neki od primjera primjene heurističkih metoda prilikom konstrukcije dizajna su opisani u [9],[37],[43],[44] i [48].

Predmet istraživanja ove disertacije je konstrukcija blokovnih dizajna uz pomoć orbitnih matrica, uz pretpostavku djelovanja određene grupe na dizajn. U sklopu ovog rada, razvili smo algoritam za konstrukciju neizomorfničkih točkovnih orbitnih matrica blokovnih dizajna s proizvoljnim dopustivim parametrima na koje djeluje proizvoljna grupa automorfizama, što je zapravo generalizacija algoritma za konstrukciju neizomorfničkih točkovnih orbitnih matrica simetričnih dizajna, opisanog u [21]. Kako bi iz orbitnih matrica konstruirali odgovarajuće dizajne, razvili smo algoritam za profinjenje tih matrica koji se temelji na primjeni kompozicijskog niza rješive grupe automorfizama blokovnih dizajna.

Osim toga, predmet istraživanja ove disertacije je traženje odgovarajućih poddizajna u blokovnim dizajnim, što je provedeno pomoću modificiranih genetskih algoritama. U sklopu ovog rada razvili smo modificirane genetske algoritme za traženje unitala i drugih poddizajna, pretraživanjem matrica incidencije (simetričnih) blokovnih dizajna.

Disertacija je tematski podijeljena na tri dijela. Prvi dio disertacije, koji se proteže na prva tri poglavlja posvećen je prvenstveno opisu, u sklopu ovog rada, razvijenih algoritama za konstrukciju i profinjenje orbitnih matrica blokovnih dizajna na koje djeluje odgovarajuća grupa automorfizama. U poglavlju 1 dan je pregled osnovnih svojstava cikličkih, permutacijskih i Frobeniusovih grupa. U poglavlju 2 dan je uvod u konačne incidencijske strukture, s naglaskom na blokovnim dizajnim, te su definirani unitali u simetričnim dizajnim. U poglavlju 3 opisana je metoda taktičke kompozicije i definirane su orbitne matrice blokovnog dizajna za djelovanje neke grupe automorfizama na taj dizajn. Prikazan je razvijeni algoritam za konstrukciju neizomorfničkih točkovnih orbitnih matrica nekog blokovnog dizajna uz pretpostavku djelovanja proizvoljne grupe na dizajn. Osim toga, opisan je algoritam za profinjenje (dekompoziciju) orbitnih matrica koji se temelji na primjeni kompozicijskog niza rješive grupe automorfizama blokovnih dizajna. Primjenom računalnih programa razvijenih na temelju tih algoritama, napravljena je klasifikacija $2-(45, 12, 3)$ dizajna s involutornim automorfizmom.

Drugi dio disertacije obuhvaća poglavlja od četvrtog do sedmog, a odnosi se na primjenu algoritama, opisanih u poglavlju 3, na konkretne blokovne dizajne i grupe automorfizama tih dizajna. U poglavlju 4 napravljena je klasifikacija $2-(45, 5, 1)$ dizajna na koje djeluje automorfizam reda šest, u poglavlju 5 konstruirani su $2-(45, 5, 1)$ dizajni na koje djeluje grupa automorfizama $Z_3 \times Z_3$, dok su u poglavlju 6 konstruirani $2-(45, 5, 1)$ dizajni na koje djeluje grupa automorfizama S_3 . Niti jedan $2-(45, 5, 1)$ dizajn konstruiran u sklopu ove disertacije nije rastavljiv. Postojanje rastavljivih $2-(45, 5, 1)$ dizajna još je uvijek otvoreno pitanje. U poglavlju 7 napravljena je klasifikacija $2-(78, 22, 6)$ dizajna na koje djeluje grupa $Frob_{39} \times Z_2$, primjenom modificiranog algoritma za profinjenje orbitnih matrica koji se temelji na primjeni glavnog niza konkretne grupe koja djeluje na dizajn.

Dokazali smo da ne postoji $(78, 22, 6)$ diferencijski skup u grupi $Frob_{39} \times Z_2$.

Treći dio disertacije, odnosno poglavlje 8, posvećeno je ispitivanju egzistencije odgovarajućih podstruktura u blokovnim dizajnim. Razvijena su dva modificirana genetska algoritma, jedan za traženje unitala u simetričnim dizajnim, drugi za traženje poddizajna s odgovarajućim parametrima u nekom blokovnom dizajnu. Prikazani su rezultati koji se odnose na traženje unitala u dizajnim s parametrima $2-(66, 26, 10)$ i $2-(36, 15, 6)$, koji su dani u članku [16]. Osim toga, prikazani su i rezultati koji se odnose na traženje $2-(11, 5, 2)$ poddizajna u $2-(66, 26, 10)$ dizajnim.

U prilogu su navedene točkovne orbitne matrice dobivene primjenom programa za profinjenje na odgovarajuće orbitne matrice iz poglavlja 7.

U sklopu ove disertacije razvijeni algoritmi za konstrukciju i profinjenje orbitnih matrica blokovnih dizajna implementirani su u programsku podršku napisanu u programu GAP ([25]), dok su modificirani genetski algoritmi implementirani u programsku podršku napisanu u Matlab-u.

Poglavlje 1

Grupe

U ovom poglavlju ponovit ćemo one pojmove iz teorije konačnih grupa koji su neophodni za razumijevanje nastavka rada. Posebno navodimo neka osnovna svojstva permutacijskih, cikličkih i Frobeniusovih grupa, te definiramo djelovanje grupe na konačni skup jer prilikom konstrukcije blokovnih dizajna pretpostavljamo djelovanje neke permutacijske grupe na skupu njegovih točaka i blokova. Pretpostavljamo da se znaju osnovni pojmovi i definicije teorije konačnih grupa.

1.1 Uvod u teoriju grupa

Svaka podgrupa neke grupe G definira jednu particiju te grupe, stoga ćemo promotriti svojstva particije koju čine susjedne klase neke podgrupe grupe G .

Definicija 1.1. Neka je G grupa, $H \leq G$ i $g \in G$. Skup $gH = \{gh \mid h \in H\}$ naziva se lijeva susjedna klasa podgrupe H određena elementom g . Skup svih lijevih susjednih klasa podgrupe H označavamo sa $G/H = \{gH \mid g \in G\}$. Skup $Hg = \{hg \mid h \in H\}$ naziva se desna susjedna klasa podgrupe H određena elementom g . Skup svih desnih susjednih klasa podgrupe H označavamo sa $H \backslash G = \{Hg \mid g \in G\}$.

Skupovi lijevih i desnih susjednih klasa podgrupe H imaju isti kardinalni broj jer je preslikavanje $\psi : G/H \rightarrow H \backslash G$ definirano sa $\psi(gH) = Hg^{-1}$ bijekcija.

Definicija 1.2. Neka je $H \leq G$. Kardinalni broj skupa G/H naziva se indeks podgrupe H u G i označava sa $[G : H]$.

Teorem 1.1. (*Lagrangeov teorem*) Neka je G konačna grupa i $H \leq G$. Tada je

$$|G| = [G : H]|H|.$$

1.1 Uvod u teoriju grupa

Dokaz. Neka je $g \in G$. Preslikavanje $\pi : H \rightarrow gH$, $\pi(h) = gh$ je bijekcija pa vrijedi $|H| = |gH|$. S obzirom da je G disjunktne unija susjednih klasa g_1H, \dots, g_kH slijedi

$$|G| = \sum_{i=1}^k |g_iH| = \sum_{i=1}^k |H| = k|H|,$$

gdje je k broj različitih susjednih klasa čija unija čini G . Dakle, $k = [G : H]$, što povlači $|G| = [G : H]|H|$. \square

Definicija 1.3. Neka je H podgrupa grupe G i $g \in G$. Grupu gHg^{-1} označavamo sa H^g i kažemo da su grupe H i H^g međusobno konjugirane.

U sljedećoj definiciji navodimo podgrupe kod kojih nema razlike između lijevih i desnih susjednih klasa.

Definicija 1.4. Za podgrupu H grupe G za koju vrijedi

$$H = gHg^{-1} = H^g, \quad \forall g \in G,$$

kažemo da je normalna podgrupa od G (ili normalna u G) i pišemo $H \trianglelefteq G$.

Primjer 1.1. Ako je G komutativna grupa, tada je svaka podgrupa $H \leq G$ normalna jer je $hg = gh$, za svaki $g \in G$ i za svaki $h \in H$. Primijetimo da je trivijalna grupa $\{1\}$ normalna podgrupa svake grupe G .

Grupa G je jednostavna ako nema pravih netrivialnih normalnih podgrupa. Jedine normalne podgrupe jednostavne grupe G su trivijalna grupa $\{1\}$ i cijela grupa G . Posebno, komutativna grupa je jednostavna ako i samo ako je prostog reda.

Prema definiciji 1.4, ako je $H \triangleleft G$, tada su skupovi lijevih i desnih susjednih klasa podgrupe H jednaki, pa ih možemo jednostavno označiti sa G/H . U tom slučaju se na skupu G/H može definirati struktura grupe.

Dokaz sljedećeg teorema može se naći u [53].

Teorem 1.2. Neka je $H \triangleleft G$. Tada je G/H grupa u odnosu na množenje definirano sa $(xH)(yH) = (xy)H$. Preslikavanje $\pi : G \rightarrow G/H$, $\pi(g) = gH$, je epimorfizam i $\text{Ker}(\pi) = H$.

Definicija 1.5. Neka je $H \triangleleft G$. Grupa G/H naziva se kvocijentna grupa, a homomorfizam $\pi : G \rightarrow G/H$, $\pi(g) = gH$, naziva se kanonski homomorfizam ili projekcija sa G na G/H .

Struktura grupe G se odražava na strukturu grupe G/H , pa kvocijentne grupe imaju važnu ulogu u proučavanju strukture grupa.

Pretpostavimo da je G konačna grupa i $H \triangleleft G$. Red kvocijente grupe G/H je $[G : H]$, pa iz teorema 1.1 slijedi sljedeći izraz za red kvocijentne grupe

$$|G/H| = [G : H] = \frac{|G|}{|H|}.$$

Iz postojećih grupa moguće je dobiti novu grupu, kao što je to primjerice kvocijentna grupa. Osim toga, iz familije grupa moguće je dobiti direktne produkte tih grupa. Posebno, za slučaj kada imamo samo dvije grupe pojam direktnog produkta generaliziran je do pojma semidirektnog produkta tih grupa.

Definicija 1.6. Neka su G_i grupe za $i \in \{1, \dots, n\}$. Direktan produkt grupa G_i je skup $G = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i, i = 1, \dots, n\}$ u oznaci $G = G_1 \times G_2 \times \dots \times G_n$. G je grupa s obzirom na operaciju $(g_1, g_2, \dots, g_n)(g'_1, g'_2, \dots, g'_n) = (g_1g'_1, g_2g'_2, \dots, g_ng'_n)$.

Napomena 1.1. Za grupe G i H vrijedi:

- a) $G \times H$ je Abelova ako i samo ako su G i H Abelove grupe,
- b) $|G \times H| = |G||H|$,
- c) $G \cong G \times \{1\} = \{(g, 1) \mid g \in G\} \leq G \times H$ i
 $H \cong \{1\} \times H = \{(1, h) \mid h \in H\} \leq G \times H$,
 stoga, uz identifikaciju $G \equiv G \times \{1\}$ i $H \equiv \{1\} \times H$, podrazumijevamo da je $G, H \leq G \times H$. Štoviše, to su i normalne podgrupe, odnosno $G, H \trianglelefteq G \times H$.

Neka su N i H grupe i neka je zadan homomorfizam

$$\varphi : H \rightarrow \text{Aut}(N), \quad \varphi_h := \varphi(h) \in \text{Aut}(N), \quad h \in H.$$

Neka je $G = \{(n, h) \mid n \in N, h \in H\}$ skup na kojemu je definirana sljedeća operacija

$$(n_1, h_1) * (n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2).$$

Vrijedi da je $(G, *)$ grupa i kažemo da je G semidirektni produkt grupa N i H određen sa φ u oznaci $N \rtimes_{\varphi} H$ ili $N : H$. Jasno, $|G| = |N||H|$.

Uočimo da semidirektni produkt grupe N i H ovisi o homomorfizmu φ te oznakom $N : H$ ne opisujemo grupu jednoznačno.

Primjer 1.2. Ako je φ_h identiteta za svaki $h \in H$, onda je semidirektni produkt grupe N i H zapravo direktan produkt tih grupa.

Neka je G grupa, $N \trianglelefteq G$, $H \leq G$, te neka je $G = NH$ ($G/N \cong H$) i $N \cap H = \{1\}$. Tada je G izomorfna semidirektnom produktu $N : H$ za konjugacijsko djelovanje grupe H na

1.2 Cikličke grupe

grupu N , odnosno $\varphi_h(N) = N^h$, za svaki $h \in H$. Kažemo da je G proširenje cijepanjem grupe N grupom H . Ako H nije podgrupa od G onda je G proširenje grupe N grupom H u oznaci $N.H$.

Obrnuto, ako je $G = N : H$ onda je $N^* = \{(n, 1) \mid n \in N\} \cong N$ normalna podgrupa u G i $H^* = \{(1, h) \mid h \in H\} \cong H$ podgrupa u G , te vrijedi $G = N^*H^*$ i $N^* \cap H^* = \{1\}$.

U nastavku navodimo primjere nekih grupa koje smo koristili prilikom konstrukcije blokovnih dizajna. Naime, za konstrukciju blokovnih dizajna u poglavljima 4, 5, 6 i 7 razmatrali smo djelovanja redom cikličke grupe reda šest, elementarno Abelove grupe reda devet, simetrične grupe $S_3 \cong Z_3 : Z_2$ i direktnog produkta Frobeniusove grupe $Frob_{39}$ i cikličke grupe reda dva na odgovarajuće blokovne dizajne.

1.2 Cikličke grupe

Posebnu ulogu među Abelovim grupama imaju cikličke grupe, odnosno grupe generirane jednim elementom.

Definicija 1.7. Neka je G grupa i $X \subseteq G$. Presjek svih podgrupa od G koje sadrže X naziva se podgrupa generirana sa X i označava sa $\langle X \rangle$.

$\langle X \rangle$ je najmanja podgrupa od G koja sadrži skup X , u smislu da iz $X \subseteq H \leq G$ slijedi da je $\langle X \rangle \leq H$. Ako je $H \leq G$, onda je jasno da je $\langle H \rangle = H$. Ako je X konačan skup, $X = \{x_1, \dots, x_n\}$, pišemo $\langle X \rangle = \langle x_1, \dots, x_n \rangle$.

Propozicija 1.1. Neka je G grupa i X neprazni podskup od G . Tada se $\langle X \rangle$ sastoji od svih konačnih umnožaka $x_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_m^{k_m}$, gdje je $x_i \in X$, $k_i \in \mathbb{Z}$ za svaki $i \in \{1, 2, \dots, m\}$, $m \in \mathbb{N}$.

Dokaz. Neka je $H = \{x_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_m^{k_m} \mid x_i \in X, k_i \in \mathbb{Z}, 1 \leq i \leq m, m \in \mathbb{N}\} \neq \emptyset$. Za $f, g \in H$ slijedi da je $fg^{-1} \in H$. Stoga, H je podgrupa od G koja sadrži X , odnosno vrijedi $\langle X \rangle \leq H$. Grupa $\langle X \rangle$ sadrži sve elemente skupa X , pa se u toj grupi nalaze i svi konačni umnošci oblika $x_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_m^{k_m}$, $x_i \in X, k_i \in \mathbb{Z}$ za svaki $i \in \{1, 2, \dots, m\}$, $m \in \mathbb{N}$, pa je $H \leq \langle X \rangle$. Time je dokazana tvrdnja. \square

Definicija 1.8. Ako je $X \subseteq G$ i $\langle X \rangle = G$, onda kažemo da je X skup generatora grupe G .

Definicija 1.9. Grupa $G = \langle x \rangle$ generirana jednim elementom zove se ciklička grupa. Ako je $|\langle x \rangle| = n$ kažemo da je element x reda n , odnosno ciklička grupa G je reda n i pišemo $|x| = n$.

Svaka ciklička grupa je komutativna s obzirom da je $x^m \cdot x^n = x^n \cdot x^m, \forall m, n \in \mathbb{Z}$.

Dokaz sljedeće propozicije može se naći u [6].

Propozicija 1.2. Ako je $G = \langle x \rangle$ ciklička grupa reda $m \in \mathbb{N}$, onda je $G = \{x^0, \dots, x^{m-1}\}$. Ako je $H = \langle y \rangle$ ciklička grupa reda m , onda je $H \cong G$.

Primjer 1.3. Neka je $m \in \mathbb{N}$ i $\Omega = \{0, 1, \dots, m-1\}$. Nadalje, neka je $\alpha : \Omega \rightarrow \Omega$ preslikavanje takvo da je $\alpha(i) \equiv (i+1) \pmod{m}$, za svaki $i \in \Omega$. Grupa $G \cong \langle \alpha \rangle$ je ciklička grupa reda m .

Primjer 1.4. Neka je $n \in \mathbb{N}$ i Z_n skup ostataka pri dijeljenju elemenata skupa \mathbb{Z} sa n . Z_n je konačna ciklička grupa reda n s obzirom na operaciju zbrajanja modulo n .

Iz propozicije 1.2 i primjera 1.4 slijedi da je svaka ciklička grupa konačnog reda $n \in \mathbb{N}$ izomorfna je s grupom $(Z_n, +)$.

Primjer 1.5. Svaka konačna Abelova grupa je direktni produkt cikličkih grupa. Neka je $n \in \mathbb{N}$, $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, pri čemu su p_1, p_2, \dots, p_m različiti prosti brojevi, te $k_i \in \mathbb{N}$, $1 \leq i \leq m$. Tada je $Z_n \cong Z_{p_1^{k_1}} \times Z_{p_2^{k_2}} \times \dots \times Z_{p_m^{k_m}}$.

Definicija 1.10. Za p prost broj i grupu G kažemo da je p -grupa ako za svaki $g \in G$ vrijedi da je $|g| = p^k$ za neki $k \in \mathbb{N}_0$.

Za p -grupu kažemo da je elementarno Abelova ako je Abelova grupa i za svaki $g \in G$, $g \neq 1$ vrijedi $|g| = p$.

1.3 Permutacijske grupe

Definicija 1.11. Neka je Ω neprazan skup. Svako bijektivno preslikavanje $\sigma : \Omega \rightarrow \Omega$ naziva se permutacija na skupu Ω . Skup svih permutacija skupa Ω označimo sa $S(\Omega)$. Skup $S(\Omega)$ je grupa u odnosu na kompoziciju funkcija i naziva se simetrična grupa skupa Ω . Svaka podgrupa grupe $S(\Omega)$ naziva se permutacijska grupa na Ω .

Ako je $|\Omega| = n$, $n \in \mathbb{N}$, tada je $|S(\Omega)| = n!$. U tom slučaju kažemo da je $S(\Omega)$ simetrična grupa stupnja n i označavamo ju sa S_n . Ako je $G \leq S_n$, tada kažemo da je G permutacijska grupa stupnja n .

Definicija 1.12. Neka je zadan skup $I_n = \{1, 2, \dots, n\}$ i i_1, i_2, \dots, i_r međusobno različiti elementi iz I_n , za $r \leq n$, $n \in \mathbb{N}$. Tada (i_1, i_2, \dots, i_r) označava permutaciju koja preslikava redom $i_1 \mapsto i_2, i_2 \mapsto i_3, \dots, i_{r-1} \mapsto i_r$ i $i_r \mapsto i_1$, dok sve ostale elemente iz I_n fiksira. (i_1, \dots, i_r) nazivamo ciklusom duljine r . Ciklus duljine 2 naziva se transpozicijom.

Svaki ciklus duljine $n \geq 2$ (a_1, a_2, \dots, a_n) može se prikazati kao kompozicija transpozicija, odnosno ciklusa duljine dva $(a_1, a_2, \dots, a_n) = (a_1, a_2)(a_1, a_3) \dots (a_1, a_n)$. Za dva ciklusa (a_1, a_2, \dots, a_n) i (b_1, b_2, \dots, b_n) kažemo da su disjunktna ako je

$$\{a_1, a_2, \dots, a_n\} \cap \{b_1, b_2, \dots, b_n\} = \emptyset.$$

1.3 Permutacijske grupe

Svaki element simetrične grupe S_n može se jednoznačno do poretka prikazati kao kompozicija disjunktih ciklusa. Parna (neparna) permutacija je ona permutacija koja se može prikazati kao kompozicija parnog (neparnog) broja ne nužno disjunktih transpozicija.

Definicija 1.13. Neka je $n \in \mathbb{N}$ i $\alpha, \beta \in S_n$. Kažemo da permutacije α i β imaju istu cikličku strukturu ako je $f_\alpha(d) = f_\beta(d)$, $1 \leq d \leq n$, pri čemu su $f_\alpha(d)$ i $f_\beta(d)$ brojevi ciklusa duljine d u cikličkim zapisima permutacija α i β .

Definicija 1.14. Grupa parnih permutacija na konačnom skupu naziva se alternirajuća grupa. Alternirajuća grupa na skupu $\{1, \dots, n\}$ naziva se alternirajuća grupa stupnja n u oznaci A_n ili $Alt(n)$.

Napomena 1.2. Vrijedi da je $A_n \triangleleft S_n$ za svaki $n \in \mathbb{N}$.

Definicija 1.15. Neka je $G \leq S(\Omega)$ i $g \in G$. Ako za neki $x \in \Omega$ vrijedi $g(x) = x$, onda kažemo da je x fiksna točka permutacije g . Ako je $g(x) = x$ za svaki $g \in G$, tada kažemo da je x fiksna točka grupe G . Ako je $g(A) = A$ za neki $A \subseteq \Omega$, tada kažemo da permutacija g fiksira skup A .

1.3.1 Djelovanje grupe na skup

Proučavanjem djelovanja grupe na skup možemo doznati više o algebarskoj strukturi same grupe. Djelovanje grupe na skup inducira permutacije na tom skupu.

Definicija 1.16. Grupa G djeluje na skup $\Omega \neq \emptyset$ ako postoji preslikavanje $\cdot : G \times \Omega \rightarrow \Omega$ za koje vrijedi:

1. $1.x = x$, $\forall x \in \Omega$,
2. $g.(h.x) = (gh).x$, $\forall g, h \in G$ i $\forall x \in \Omega$.

Skup Ω na kojem je definirano djelovanje grupe G naziva se G -skup.

Sliku djelovanja od $g \in G$ na $x \in \Omega$ u nastavku ovog rada označavat ćemo sa $g.x$.

Definicija 1.17. Kažemo da je djelovanje grupe G na skup Ω poluregularno ako za svaka dva elementa $x, y \in \Omega$ postoji najviše jedan element $g \in G$ za koji je $y = g.x$. Za djelovanje grupe G na skup Ω kažemo da je tranzitivno ako: $(\forall x, y \in \Omega)(\exists g \in G) g.x = y$.

Ako grupa G djeluje poluregularno i tranzitivno na skupu Ω , onda kažemo da djeluje regularno na tom skupu.

Dokaz sljedećeg teorema može se naći u [24].

Teorem 1.3. Grupa G djeluje na skup Ω ako i samo ako postoji homomorfizam $f : G \rightarrow S(\Omega)$, $f(g) = f_g$, gdje je $f_g(x) = g.x$, za svaki $g \in G$ i $x \in \Omega$.

Napomena 1.3. Za svaki homomorfizam $f : G \rightarrow S(\Omega)$ kažemo da je permutacijska reprezentacija grupe G na skupu Ω . Stoga, svako djelovanje grupe G na skup Ω poistovjećujemo s permutacijskom reprezentacijom od G na Ω .

Definicija 1.18. Grupa G djeluje vjerno na skup Ω , odnosno $f : G \rightarrow S(\Omega)$ je vjerna permutacijska reprezentacija, ako je f monomorfizam.

Dokaz sljedećeg teorema može se naći u [31].

Teorem 1.4. (Cayley) *Svaka grupa G je izomorfna podgrupi grupe $S(G)$. Posebno, ako je G konačna grupa reda n , tada je ona izomorfna podgrupi simetrične grupe S_n . Drugim riječima, svaka grupa je izomorfna nekoj permutacijskoj grupi.*

Definicija 1.19. Neka grupe G_1 i G_2 djeluju redom na skupove Ω_1 i Ω_2 . Grupe G_1 i G_2 su permutacijski izomorfne ako postoji izomorfizam $\psi : G_1 \rightarrow G_2$ i bijekcija $\phi : \Omega_1 \rightarrow \Omega_2$ tako da za svaki $g \in G$ sljedeći dijagram komutira

$$\begin{array}{ccc}
 \Omega_1 & \xrightarrow{\phi} & \Omega_2 \\
 \downarrow f_g(x) = g.x & & \downarrow f_{\psi(g)}(x) = \psi(g).x \\
 \Omega_1 & \xrightarrow{\phi} & \Omega_2
 \end{array}$$

Napomena 1.4. Ako su grupe G_1 i G_2 permutacijski izomorfne, onda su one i izomorfne. Obrat ne vrijedi.

Na skupu Ω na koji djeluje grupa G definiramo sljedeću binarnu relaciju (G -povezanost)

$$x \sim y \Leftrightarrow (\exists g \in G) g.x = y. \tag{1.1}$$

Dokaz sljedeće propozicije može se naći u [30].

Propozicija 1.3. *Relacija \sim definirana kao u (1.1) je relacija ekvivalencije na skupu Ω .*

Definicija 1.20. Neka grupa G djeluje na neprazan skup Ω . G -orbita elementa $x \in \Omega$ je klasa ekvivalencije tog elementa s obzirom na relaciju ekvivalencije (1.1) i označavamo je sa $G.x = \{g.x \mid g \in G\}$. Element x naziva se predstavnik orbite $G.x$. Broj elemenata neke G -orbite naziva se duljina te orbite.

Definicija 1.21. Neka grupa G djeluje na neprazan skup Ω i neka je $x \in \Omega$. Skup $G_x = \{g \in G \mid g.x = x\}$ nazivamo stabilizatorom elementa x za djelovanje grupe G na Ω .

1.3 Permutacijske grupe

Lako se može provjeriti da vrijedi $G_x \leq G$, za svaki $x \in \Omega$.

Definicija 1.22. Neka grupa G djeluje na neprazan skup Ω i neka je $X \subseteq \Omega$. Skup $G_X = \{g \in G \mid g.x = x, \forall x \in X\}$ zove se točkovni stabilizator skupa X u grupi G . Skup $G(X) = \{g \in G \mid g.X = X\}$, gdje je $g.X = \{g.x \mid x \in X\}$, naziva se skupovni stabilizator skupa X u grupi G .

Za svaki $X \subseteq \Omega$ vrijedi: $G_X = \bigcap_{x \in X} G_x$, te $G_X, G(X) \leq G$.

Sljedeća propozicija daje vezu između duljine G -orbite elementa $x \in \Omega$ i njegovog stabilizatora u grupi G , a dokaz može se naći u [24].

Propozicija 1.4. Ako grupa G djeluje na neprazan skup Ω , tada za svaki $x \in \Omega$ vrijedi

$$|G.x| = [G : G_x].$$

Korolar 1.1. Neka konačna grupa G djeluje na konačan skup Ω . Tada vrijedi

$$|G.x| = \frac{|G|}{|G_x|}, \forall x \in \Omega.$$

Stoga, u konačnom skupu Ω sve G -orbite su konačni skupovi.

Primjer 1.6. Grupa G djeluje na samu sebe konjugacijom, $g.x = gxg^{-1} = x^g$, za svaki $x, g \in G$ jer vrijedi:

1. $1.x = 1x1^{-1} = x, \forall x \in G$,
2. $g_1.(g_2.x) = g_1(g_2.x)g_1^{-1} = g_1g_2x(g_1g_2)^{-1} = (g_1g_2).x, \forall g_1, g_2, x \in G$.

Napomena 1.5. Orbita za djelovanje konjugacijom grupe G na element $x \in G$ naziva se konjugacijska klasa elementa x u G i označava sa $ccl_G x = \{x^g \mid g \in G\}$.

Primjer 1.7. Pokažimo da grupa G djeluje konjugacijom na skup svojih podgrupa \mathcal{H} . Neka su $1, g_1, g_2 \in G$. Vrijedi:

1. $1.H = H^1 = \{h^1 \mid h \in H\} = H$, za $H \in \mathcal{H}$,
2. $g_1.(g_2.H) = g_1.H^{g_2} = g_1.\{h^{g_2} \mid h \in H\} = \{h^{g_2} \mid h \in H\}^{g_1} = \{(h^{g_2})^{g_1} \mid h \in H\} = (g_1g_2).H$, za $H \in \mathcal{H}$.

Napomena 1.6. Orbita za djelovanje konjugacijom grupe G na podgrupu H naziva se konjugacijska klasa podgrupe H u grupi G i označava sa $ccl_G H$, odnosno $ccl_G H = \{H^g \mid g \in G\}$.

Sljedeća propozicija govori o tome da su stabilizatori elemenata iz iste orbite međusobno konjugirani.

Propozicija 1.5. *Neka je G_x stabilizator elementa $x \in \Omega$ za djelovanje grupe G na neprazan skup Ω . Tada vrijedi $G_{g.x} = G_x^g$ za svaki $g \in G$. Posebno, ako grupa G djeluje tranzitivno na skup Ω , onda su stabilizatori svaka dva elementa iz Ω međusobno konjugirani.*

Dokaz. Vrijedi da je $\bar{g} \in G_{g.x} \Leftrightarrow \bar{g} \cdot (g.x) = g.x \Leftrightarrow (g^{-1}\bar{g}g) \cdot x = x \Leftrightarrow g^{-1}\bar{g}g \in G_x \Leftrightarrow \bar{g} \in gG_xg^{-1} = G_x^g$. Neka grupa G djeluje tranzitivno na skup Ω . Za $x_1, x_2 \in \Omega$ postoji $g \in G$ takav da je $x_2 = g.x_1 \Rightarrow G_{x_2} = G_{g.x_1} = G_{x_1}^g$. \square

Rezultat o broju orbita pri djelovanju grupe na skup daje sljedeća tvrdnja koja je poznata i kao Burnsideova lema.

Lema 1.1. *(Cauchy-Frobenius) Neka konačna grupa G djeluje na konačan skup Ω . Označimo sa t broj orbita za to djelovanje, te neka je $F(g) = \{x \in \Omega \mid g.x = x\}$ skup elemenata iz Ω koje fiksira $g \in G$. Tada vrijedi*

$$t = \frac{1}{|G|} \sum_{g \in G} |F(g)|.$$

Dokaz. Prebrojimo li na dva načina elemente skupa $\{(x, g) \in \Omega \times G \mid g.x = x\}$ dobivamo $\sum_{x \in \Omega} |G_x| = \sum_{g \in G} |F(g)|$. Neka su x_1, x_2, \dots, x_t predstavnici orbita za djelovanje grupe G na skup Ω . Ako je $y \in G.x_i$ i $g \in G$ tako da je $y = g.x_i$, onda je $G_y = gG_{x_i}g^{-1}$, prema propoziciji 1.5. Funkcija $\phi : G_{x_i} \rightarrow gG_{x_i}g^{-1}$ za koju je $\phi(\alpha) = g\alpha g^{-1}$, za $\alpha \in G_{x_i}$ je bijekcija, stoga iz prethodne jednakosti imamo da je $|G_y| = |G_{x_i}|$. Zbog toga vrijedi

$$\sum_{g \in G} |F(g)| = \sum_{i=1}^t |G.x_i| |G_{x_i}| = \sum_{i=1}^t |G| = t|G|,$$

čime je tvrdnja dokazana. \square

Ako grupa G djeluje tranzitivno na skupu Ω , onda postoji samo jedna G -orbita u Ω i vrijedi $|\Omega| = [G : G_x]$ za svaki $x \in \Omega$. Ako je Ω konačan skup na kojem G djeluje tranzitivno, onda iz tvrdnje leme 1.1 slijedi da je $|G| = \sum_{g \in G} |F(g)|$.

Definicija 1.23. Neka je G grupa, A podskup od G i $x \in G$. Stabilizator za djelovanje konjugacijom grupe G na element x , $C_G(x) = \{g \in G \mid x^g = x\}$, naziva se centralizator od x u G , dok skup

$$C_G(A) = \{g \mid g \in G, a^g = a, \forall a \in A\}$$

zovemo centralizatorom skupa A u grupi G .

Definicija 1.24. Neka je G grupa, A podskup od G . Stabilizator za djelovanje konjugacijom grupe G na skup A

$$N_G(A) = \{g \mid g \in G, A^g = A\}$$

1.3 Permutacijske grupe

zovemo normalizatorom skupa A u grupi G .

Napomena 1.7. Centralizator $C_G(A)$ i normalizator $N_G(A)$ su podgrupe grupe G .

Napomena 1.8. Ako je $g \in C_G(A)$, pri čemu je A podskup od G , onda je $gag^{-1} = a$ za svaki $a \in A$, što implicira $gAg^{-1} = A$, odnosno $g \in N_G(A)$, pa vrijedi $C_G(A) \leq N_G(A)$.

Napomena 1.9. Konjugacijske klase elemenata konačne grupe G u grupi G čine particiju te grupe, pa vrijedi klasna jednadžba

$$|G| = \sum_{i=1}^n [G : C_G(x_i)],$$

pri čemu su x_1, \dots, x_n predstavnici konjugacijskih klasa.

Teorem 1.5. *Neka grupa G djeluje na skup Ω i neka je $x \in \Omega$. Nadalje, neka G djeluje na $G_x \backslash G$ tako da $g.(G_x g') = G_x g' g^{-1}$, za svaki $g, g' \in G$. Djelovanje grupe G na $G_x \backslash G$ je permutacijski izomorfno djelovanju grupe G na $G_{x'} \backslash G$, za $x' \in G.x$.*

Dokaz. Lako je pokazati da je djelovanje grupe G na $G_x \backslash G$ dobro definirano. Iz propozicije 1.5 slijedi da je $G_{x'} = G_{\bar{g}.x} = G_{\bar{g}.x}$, za neki $\bar{g} \in G$. Definiramo preslikavanje $\alpha : G_x \backslash G \rightarrow G_{x'} \backslash G$ tako da je $\alpha(G_x g) = G_{x'} \bar{g} g$, za svaki $g \in G$. Preslikavanje α je bijekcija. Za svaki $G_x g' \in G_x \backslash G$ i svaki $g \in G$ vrijedi

$$g.\alpha(G_x g') = g.[G_{x'} \bar{g} g'] = G_{x'} \bar{g} g' g^{-1} = \alpha(G_x g' g^{-1}) = \alpha[g.(G_x g')].$$

Time je tvrdnja dokazana. □

Teorem 1.6. *Neka grupa G djeluje na skup Ω , te neka G djeluje na $G_x \backslash G$ kao u prethodnom teoremu, za neki $x \in \Omega$. Tada je djelovanje grupe G na G -orbitu $G.x$ permutacijski izomorfno djelovanju grupe G na $G_x \backslash G$.*

Dokaz. Definiramo preslikavanje $\alpha : G.x \rightarrow G_x \backslash G$ tako da je $\alpha(g.x) = G_x g^{-1}$, za svaki $g \in G$. Preslikavanje α je bijekcija. Za svaki $g'.x \in G.x$ i svaki $g \in G$ vrijedi

$$g.[\alpha(g'.x)] = g.(G_x g'^{-1}) = G_x g'^{-1} g^{-1} = G_x (gg')^{-1} = \alpha[(gg').x].$$

Time je tvrdnja dokazana. □

Rezultat iz sljedećeg teorema i korolara koristimo za redukciju broja izomorfnih struktura prilikom konstrukcije blokovnih dizajna.

Teorem 1.7. *Neka grupa G djeluje na konačan skup Ω , neka su $x_1, x_2 \in \Omega$ i $G_{x_2}^{\bar{g}} = G_{x_1}$ za neki $\bar{g} \in G$. Tada postoji bijekcija $\alpha : G.x_1 \rightarrow G.x_2$ takva da*

$$g.\alpha(x) = \alpha(g.x), \quad \forall g \in G, \quad x \in G.x_1.$$

Dokaz. Definiramo preslikavanje $\alpha : G.x_1 \rightarrow G.x_2$ na sljedeći način:

$$\alpha(x) = \alpha(g'.x_1) = (g'\bar{g}).x_2, \quad \forall x \in G.x_1.$$

Takvo preslikavanje je dobro definirano jer iz jednakosti $g'.x_1 = g''.x_1 \Rightarrow g''^{-1}g' \in G_{x_1} \Rightarrow g''^{-1}g' \in G_{x_2}^{\bar{g}} \Rightarrow \bar{g}^{-1}g''^{-1}g'\bar{g} \in G_{x_2} \Rightarrow (\bar{g}^{-1}g''^{-1}g'\bar{g}).x_2 = x_2 \Rightarrow (g'\bar{g}).x_2 = (g''\bar{g}).x_2$.

Bijektivnost preslikavanja α lako je pokazati. Osim toga, za sve $g \in G$, $x \in G.x_1$ vrijedi

$$g.\alpha(x) = g.[\alpha(g'.x_1)] = (gg'\bar{g}).x_2 = \alpha[(gg').x_1] = \alpha(g.x).$$

Time je dokazana tvrdnja. □

Korolar 1.2. Neka je Ω konačan skup, $G \leq S(\Omega)$, $x_1, x_2 \in \Omega$ i $G_{x_2}^{\bar{g}} = G_{x_1}$ za neki $\bar{g} \in G$. Tada postoji permutacija $\alpha \in C_{S(\Omega)}(G)$ takva da je

$$\alpha(G.x_1) = G.x_2.$$

Dokaz. Definiramo preslikavanje $\alpha : \Omega \rightarrow \Omega$ tako da je

$$\alpha(x) = \begin{cases} \alpha(g'.x_1) = (g'\bar{g}).x_2, & x \in G.x_1 \\ \alpha[(g'\bar{g}).x_2] = g'.x_1, & x \in G.x_2 \\ x, & \text{inače.} \end{cases}$$

Očito je da vrijedi $\alpha \in S(\Omega)$. Iz definicije preslikavanja α slijedi da je $\alpha(G.x_1) \subseteq G.x_2$.

Iz dokaza teorema 1.7 jasno je da vrijedi $\alpha(G.x_1) = G.x_2$.

Pokažimo da je $\alpha \in C_{S(\Omega)}(G)$. Ako je $x \in \Omega - (G.x_1 \cup G.x_2)$, onda je $\alpha(g.x) = g.x = g.\alpha(x)$, za svaki $g \in G$. Za $x \in G.x_1$ također vrijedi $\alpha(g.x) = g.\alpha(x)$, za svaki $g \in G$, prema tvrdnji teorema 1.7. Ako je $x \in G.x_2$, onda iz činjenice da je $G_{x_2} = G_{x_1}^{\bar{g}^{-1}}$ i teorema 1.7 također slijedi da je $\alpha(g.x) = g.\alpha(x)$, za svaki $g \in G$.

Time je dokazana tvrdnja korolara. □

Normalne podgrupe mogu se karakterizirati kao one podgrupe $H \leq G$ čiji je normalizator cijela grupa G , $N_G(H) = G$.

Napomena 1.10. Podskup A grupe G ne mora biti sadržan u $N_G(A)$. Međutim, ako je A podgrupa od G , tada za svaki $g \in A$ vrijedi $gAg^{-1} = A$, odakle slijedi da je $A \subseteq N_G(A)$. Isto vrijedi i za svaki $g \in N_G(A)$, stoga vrijedi $A \trianglelefteq N_G(A)$.

Neka grupa G djeluje na neprazan skup Ω i neka je $H \trianglelefteq G$, te $[G : H] = k \in \mathbb{N}$. Onda je grupa G disjunktna unija lijevih susjednih klasa podgrupe H , odnosno vrijedi

1.4 Frobeniusove grupe

$G = \bigsqcup_{i=1}^k g_i H$ za neke $g_i \in G$. Neka je $x \in \Omega$, tada je

$$G.x = \bigsqcup_{i=1}^k (g_i H).x = \bigsqcup_{i=1}^k H.(g_i.x),$$

što znači da se G -orbite u skupu Ω sastoje od H -orbita.

Teorem 1.8. *Neka konačna grupa G djeluje na konačan skup Ω i $H \triangleleft G$. Neka su $x, y \in \Omega$ elementi iste G -orbite. Tada vrijedi $|H.x| = |H.y|$.*

Dokaz. Za elemente $x, y \in \Omega$ iz iste G -orbite postoji $g \in G$ takav da je $y = g.x$.

$$|H.y| = |H \cap G_y| = |H \cap G_{g.x}| = |H \cap G_x^g| = |H^g \cap G_x^g| = |(H \cap G_x)^g| = |H \cap G_x| = |H.x|.$$

Stoga, vrijedi

$$|H.y| = \frac{|H|}{|H_y|} = \frac{|H|}{|H_x|} = |H.x|.$$

□

Na temelju tvrdnje prethodnog teorema vrijedi da se svaka G -orbita sastoji od H -orbita iste duljine, za $H \triangleleft G$.

Teorem 1.9. *Neka grupa G djeluje na konačan skup Ω , $H \triangleleft G$ i za $x \in \Omega$ neka je $G.x = \bigsqcup_{i=1}^h H.x_i$, tada grupa G/H djeluje tranzitivno na skupu $\{H.x_i \mid i = 1, 2, \dots, h\}$.*

Dokaz. Iz $H \triangleleft G$ slijedi da je $g.(H.x) = H.(g.x)$ za svaki $x \in \Omega$ i $g \in G$. Vrijedi jednakost $gH.(H.x_i) = H.(g.x_i)$, što znači da G/H djeluje na skup $\{H.x_i \mid i = 1, 2, \dots, h\}$.

Još treba pokazati tranzitivnost djelovanja. Neka su $H.x_i$ i $H.x_j$ dvije različite H -orbite u G -orbiti $G.x$. Postoji $g \in G$ takav da je $x_j = g.x_i$, odakle slijedi da je $(gH).(H.x_i) = H.(g.x_i) = H.x_j$. Time je dokazana tvrdnja. □

Tvrdnje iz teorema 1.8 i teorema 1.9 koristimo prilikom konstrukcije blokovnih dizajna, odnosno u algoritmu za profinjene orbitnih matrica blokovnih dizajna na koje djeluje odgovarajuća grupa.

1.4 Frobeniusove grupe

Dokaze sljedeća tri teorema moguće je pronaći u [53].

Teorem 1.10. *(Frobenius) Neka je G konačna grupa i $\{1\} < H < G$ takva da je $H \cap H^g = \{1\}$ za svaki $g \in G - H$. Tada je $N = G - \bigcup_{g \in G} (H \setminus \{1\})^g$ normalna podgrupa grupe G takva da je $G = NH$ i $H \cap N = \{1\}$.*

Grupa G koja zadovoljava pretpostavku iz prethodnog teorema naziva se Frobeniusova grupa. Podgrupa N zove se Frobeniusova jezgra, a podgrupa H Frobeniusov komplement. Frobeniusova grupa G je semidirektni produkt grupa N i H .

Sada navodimo karakterizaciju Frobeniusove grupe kao permutacijske grupe.

Teorem 1.11. *Neka je G Frobeniusova grupa s komplementom H . Djelovanje grupe G na skup G/H je vjerno, tranzitivno i neregularno takvo da svaki element $g \in G$, $g \neq 1$, fiksira najviše jednu susjednu klasu.*

Teorem 1.12. *Neka grupa G djeluje tranzitivno i neregularno na skup X pri čemu svaki element $g \in G$, $g \neq 1$, fiksira najviše jedan element skupa X . Nadalje, neka je H stabilizator nekog elementa iz skupa X , a N unija skupa permutacija bez fiksnih elemenata i skupa $\{1\}$. Tada je G Frobeniusova grupa za H , a N je Frobeniusova jezgra grupe G . Grupa N djeluje regularno na skup X .*

Lako se može pokazati da vrijedi tvrdnja sljedećeg teorema.

Teorem 1.13. *Neka je G Frobeniusova grupa za H i N Frobeniusova jezgra od G . Tada $|H|$ dijeli $[G : H] - 1$.*

H.E. Rose u [54] ističe da svaka konačna Frobeniusova grupa reda pq , za $p \neq 2$ i q različite proste brojeve, ima prezentaciju:

$$\langle a, b \mid a^p = b^q = 1, b^{-1}ab = a^r \rangle,$$

pri čemu vrijedi $(p, q(r-1)) = 1$, $0 \leq r < p$ i $r^q \equiv 1 \pmod{p}$. Takve grupe označavamo sa $Frob_{pq}$ ili $Frob_{pq,r}$ ako za fiksne p i q postoji nekoliko vrijednosti za r , odnosno nekoliko neizomorfnih grupa.

Primjer 1.8. Alternirajuća grupa A_4 je Frobeniusova grupa. $S_3 \cong Z_3 : Z_2$ je Frobeniusova grupa.

1.5 Kompozicijski niz grupe

Algoritam za profinjenje orbitnih matrica blokovnih dizajna opisan u Poglavlju 3.3.1 temelji se na primjeni kompozicijskog niza rješive grupe čije djelovanje promatramo na zadanom dizajnu.

Definicija 1.25. Neka je G grupa. Subnormalan niz podgrupa u grupi G je niz

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G. \tag{1.2}$$

1.5 Kompozicijski niz grupe

Za broj $n \in \mathbb{N}$ kažemo da je duljina subnormalnog niza.

Definicija 1.26. Za subnormalan niz (1.2) kažemo da je normalan niz ako vrijedi da je $G_i \trianglelefteq G$, za svaki $i \in \{0, \dots, n\}$, $n \in \mathbb{N}$.

Definicija 1.27. Za (sub)normalan niz kažemo da je pravi niz ako su sve kvocijentne grupe G_{i+1}/G_i netrivialne, $0 \leq i \leq n-1$, $n \in \mathbb{N}$.

Definicija 1.28. Za subnormalan niz podgrupa u grupi G , (1.2), kažemo da je kompozicijski niz ako su sve kvocijentne grupe G_{i+1}/G_i netrivialne jednostavne grupe, za $0 \leq i \leq n-1$, $n \in \mathbb{N}$. Kažemo da je kompozicijska duljina grupe G duljina njenog kompozicijskog niza. Kvocijentne grupe G_{i+1}/G_i kompozicijskog niza podgrupa u grupi G nazivamo kompozicijski faktori.

Definicija 1.29. Za normalnu podgrupu $N \triangleleft G$ kažemo da je maksimalna normalna podgrupa grupe G ako ne postoji normalna podgrupa H od G takva da $N < H < G$.

Definicija 1.30. Za normalan niz podgrupa u grupi G kažemo da je glavni niz ako za svaku grupu $G_{i-1} \trianglelefteq G_i$ vrijedi da je maksimalna među normalnim podgrupama od G koja je sadržana u grupi G_i , za $1 \leq i \leq n$, $n \in \mathbb{N}$.

Definicija 1.31. Za dva kompozicijska niza grupe G

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G \text{ i } \{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_m = G, \quad m, n \in \mathbb{N},$$

kažemo da su ekvivalentna je $m = n$ i ako su im pripadni kompozicijski faktori jednaki do na izomorfizam i permutaciju.

Primjer 1.9.

- a) Grupa S_5 ima kompozicijski niz $\{1\} \triangleleft A_5 \triangleleft S_5$, pri čemu su kompozicijski faktori izomorfni sa $Z_2 (\cong S_5/A_5)$ i A_5 .
- b) Kompozicijski nizovi cikličke grupe $Z_6 \cong \langle \rho \rangle$ su $\{1\} \triangleleft \langle \rho^3 \rangle \triangleleft Z_6$ i $\{1\} \triangleleft \langle \rho^2 \rangle \triangleleft Z_6$.
- c) Kompozicijski niz cikličke grupe $Z_{105} \cong \langle a \rangle$ je $\{1\} \triangleleft Z_5 \cong \langle a^{21} \rangle \triangleleft Z_{15} \cong \langle a^7 \rangle \triangleleft Z_{105}$.
- d) Kompozicijski niz grupe $G \cong \text{Frob}_{39} \times Z_2$ je $\{1\} \triangleleft Z_{13} \triangleleft \text{Frob}_{39} \triangleleft G$.

Lako se pokaže da vrijedi sljedeća tvrdnja.

Lema 1.2. *Neka je $K \triangleleft G$. Kvocijentna grupa G/K je jednostavna ako i samo ako je K maksimalna normalna podgrupa od G .*

Dokaze sljedeća tri teorema moguće je pronaći u [54].

Teorem 1.14. *Svaka konačna grupa ima kompozicijski niz.*

Teorem 1.15. *(Jordan-Hölderov teorem) Svaka dva kompozicijska niza grupe G su ekvivalentna.*

Definicija 1.32. Za grupu G kažemo da je rješiva ako ima subnormalan niz čije su sve kvocijentne grupe komutativne. Takav niz nazivamo rješivim nizom.

Teorem 1.16. *Neka je G konačna grupa. G je rješiva ako i samo ako ima kompozicijski niz čiji su kompozicijski faktori cikličke grupe prostog reda.*

Primjer 1.10. Konačna komutativna grupa je rješiva. Konačna p -grupa je rješiva.

Poglavlje 2

Incidencijske strukture

U ovom poglavlju opisat ćemo osnovna svojstva konačnih incidencijskih struktura i dati uvod u osnove teorije dizajna. Definirat ćemo blokovne dizajne i navesti neka njihova osnovna svojstva. Osim toga, definirat ćemo izomorfizam blokovnih dizajna i posebno G -izomorfizam. Na kraju poglavlja promotrit ćemo osnovna svojstva unitala u simetričnim dizajnimima.

2.1 Osnovni pojmovi

Definicija 2.1. Incidencijska struktura \mathcal{D} je uređena trojka $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, gdje su \mathcal{P} i \mathcal{B} neprazni disjunktni skupovi, dok je $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. Elemente skupa \mathcal{P} nazivamo točke, elemente skupa \mathcal{B} blokovi, a relaciju \mathcal{I} nazivamo relacijom incidencije. Kažemo da je incidencijska struktura konačna ako su skupovi \mathcal{P} i \mathcal{B} konačni.

Definicija 2.2. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura, te neka je $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{B}' \subseteq \mathcal{B}$ i $\mathcal{I}' = (\mathcal{P}' \times \mathcal{B}') \cap \mathcal{I}$. Incidencijsku strukturu $\mathcal{D}' = (\mathcal{P}', \mathcal{B}', \mathcal{I}')$ nazivamo podstruktura strukture \mathcal{D} . Ako je $\mathcal{P}' \subset \mathcal{P}$ kažemo da je \mathcal{D}' prava podstruktura od \mathcal{D} .

Definicija 2.3. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura. Struktur $\mathcal{D}' = (\mathcal{P}, \mathcal{B}, \mathcal{I}')$, pri čemu je $\mathcal{I}' = (\mathcal{P} \times \mathcal{B}) \setminus \mathcal{I}$ nazivamo komplementarna struktura strukture \mathcal{D} .

Definicija 2.4. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura. Struktur $\mathcal{D}^* = (\mathcal{P}^*, \mathcal{B}^*, \mathcal{I}^*)$, gdje je $\mathcal{P}^* = \mathcal{B}$, $\mathcal{B}^* = \mathcal{P}$, $\mathcal{I}^* = \{(x, P) | (P, x) \in \mathcal{I}\}$ nazivamo dualna struktura strukture \mathcal{D} .

Broj blokova koji su incidentni s točkom $P \in \mathcal{P}$ nazivamo stupanj točke P , dok broj točaka koje su incidentne s blokom $x \in \mathcal{B}$ nazivamo stupanj bloka x .

Propozicija 2.1. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura s v točaka i b blokova,

te neka su stupnjevi točaka r_1, \dots, r_v i stupnjevi blokova k_1, \dots, k_b . Tada vrijedi

$$\sum_{i=1}^v r_i = \sum_{i=1}^b k_i.$$

Dokaz. Prebrojavanjem na dva načina elemenata skupa $\{(P, x) \in \mathcal{P} \times \mathcal{B} \mid (P, x) \in \mathcal{I}\}$. \square

Korolar 2.1. Za incidencijsku strukturu u kojoj je svaka od v točaka stupnja r i svaki od b blokova stupnja k vrijedi $vr = bk$.

Svakoj konačnoj incidencijskoj strukturi možemo pridružiti matricu incidencije, koju uvodimo u sljedećoj definiciji.

Definicija 2.5. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ konačna incidencijska struktura s v točaka i b blokova. Označimo točke sa P_1, \dots, P_v , a blokove sa x_1, \dots, x_b . Matrica incidencije incidencijske strukture \mathcal{D} je $v \times b$ matrica $M = [m_{i,j}]$, gdje je

$$m_{i,j} = \begin{cases} 1, & (P_i, x_j) \in \mathcal{I} \\ 0, & (P_i, x_j) \notin \mathcal{I} \end{cases}$$

Napomena 2.1. Neka je M matrica incidencije strukture \mathcal{D} . Matrica incidencije komplementarne strukture \mathcal{D}' je $J - M$, pri čemu je J matrica čiji su svi elementi 1, a matrica incidencije dualne strukture \mathcal{D}^* je matrica M^T .

Definicija 2.6. Linearni prostor je konačna incidencijska struktura čije su svake dvije točke sadržane u jedinstvenom bloku, a svaki blok sadrži barem dvije točke.

U radu [5] dan je pregled teorije konačnih linearnih prostora. V. Krčadinac u svojoj disertaciji [37] daje klasifikaciju nekih linearnih prostora. Linearni prostori se javljaju u poglavlju 4, kao fiksne strukture automorfizma reda dva koji djeluje na 2-(45, 5, 1) dizajn.

Definicija 2.7. Neka su $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, \mathcal{I}_1)$ i $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2, \mathcal{I}_2)$ incidencijske strukture. Za bijektivno preslikavanje $f : \mathcal{P}_1 \cup \mathcal{B}_1 \rightarrow \mathcal{P}_2 \cup \mathcal{B}_2$ kažemo da je izomorfizam iz \mathcal{D}_1 u \mathcal{D}_2 ako vrijedi:

1. f preslikava \mathcal{P}_1 na \mathcal{P}_2 i \mathcal{B}_1 na \mathcal{B}_2 ,
2. $(P, x) \in \mathcal{I}_1 \Leftrightarrow (f(P), f(x)) \in \mathcal{I}_2, \quad P \in \mathcal{P}_1 \text{ i } x \in \mathcal{B}_1.$

Ako je $\mathcal{D}_1 = \mathcal{D}_2$, onda kažemo da je preslikavanje f automorfizam incidencijske strukture $\mathcal{D} = \mathcal{D}_1 = \mathcal{D}_2$.

Skup svih automorfizama incidencijske strukture \mathcal{D} je grupa s obzirom na kompoziciju funkcija i naziva se puna grupa automorfizama strukture \mathcal{D} koju označavamo sa $Aut(\mathcal{D})$.

Grupa automorfizama incidencijske strukture \mathcal{D} je svaka podgrupa pune grupe automorfizama te strukture.

Često se izomorfizam incidencijskih struktura $\mathcal{D}_1 = (\mathcal{P}, \mathcal{B}, \mathcal{I}_1)$ i $\mathcal{D}_2 = (\mathcal{P}, \mathcal{B}, \mathcal{I}_2)$ zapisuje kao uređeni par permutacija elemenata skupa \mathcal{P} i elemenata skupa \mathcal{B} .

Definicija 2.8. Incidencijska struktura $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ je samodualna ako je izomorfna svojoj dualnoj strukturi.

2.2 Uvod u teoriju dizajna

Definicija 2.9. Konačna incidencijska struktura $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ je t - (v, k, λ) dizajn ako vrijedi:

1. $|\mathcal{P}| = v$,
2. svaki element skupa \mathcal{B} incidentan je s točno k elemenata skupa \mathcal{P} ,
3. svakih t elemenata skupa \mathcal{P} incidentno je s točno λ elemenata skupa \mathcal{B} .

Dizajn s parametrima t - (v, k, λ) nazivat ćemo kraće t -dizajn. Nenegativne cijele brojeve t, v, k i λ zovemo parametrima dizajna. Broj blokova dizajna \mathcal{D} označit ćemo sa b .

Definicija 2.10. Za podstrukturu dizajna kažemo da je poddizajn ako je i sama dizajn.

Kažemo da je t -dizajn jednostavan ako ne sadrži ponovljene blokove. Svaki blok u takvom dizajnu možemo identificirati sa skupom točaka koje su s njim incidentne.

Napomena 2.2. Kako bismo izbjegli trivijalne slučajeve, zahtijevamo da za parametre dizajna vrijedi $0 \leq t \leq k < v$. Potpun dizajn je onaj dizajn čiji su blokovi svi k -člani podskupovi skupa točaka, a relacija incidencije je inducirana relacijom pripadnosti podskupu. Broj blokova potpunog t - (v, k, λ) dizajna jednak je $\binom{v}{k}$. Dizajn za koji je broj blokova $b < \binom{v}{k}$ kažemo da je nepotpun dizajn. Dizajni se najviše proučavaju u slučajevima kada je $t = 2$ ili $\lambda = 1$.

Dizajn s parametrima 2 - (v, k, λ) naziva se blokovni dizajn.

U ovom radu baviti ćemo se isključivo jednostavnim blokovnim dizajnim.

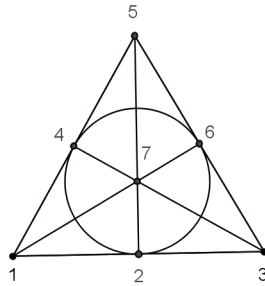
Definicija 2.11. Ako je $t \geq 2$ i $\lambda = 1$, tada t - (v, k, λ) dizajn nazivamo Steinerov sustav ili Steinerov t -dizajn i parametre označavamo $S(t, k, v)$.

Napomena 2.3. U Steinerovom 2 -dizajnu blokovi se često nazivaju pravcima, s obzirom da svake dvije točke određuju jedinstveni blok.

Lema 2.1. *Svaka dva bloka u $2-(v, k, 1)$ dizajnu sijeku se u jednoj točki ili se ne sijeku.*

Dokaz. Ako pretpostavimo da postoje dva bloka koja se sijeku u dvije točke, tada su te dvije točke incidentne s barem dva različita bloka, što je nemoguće iz razloga jer $\lambda = 1$. Dakle, slijedi tvrdnja leme. \square

Primjer 2.1. Neka je $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\}$ i $\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\}$. Tada je $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ $2-(7, 3, 1)$ dizajn. Ovaj je dizajn ujedno i projektivna ravnina reda dva, $PG(2, 2)$, koju još nazivamo i Fanovom ravninom, te ju obično grafički prikazujemo kao na sljedećoj slici.



Slika 2.1: Fanova ravnina

Sljedeći teorem govori o tome da je svaki t -dizajn ujedno i s -dizajn za $s < t$.

Teorem 2.1. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ $t-(v, k, \lambda)$ dizajn. Tada je, za svaki cijeli broj s za koji vrijedi $0 \leq s < t$, broj blokova incidentnih sa s različitih točaka neovisan o izboru tih s točaka, i jednak je*

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

\mathcal{D} je $s-(v, k, \lambda_s)$ dizajn za svaki $s \in \{1, \dots, t\}$.

Dokaz. Neka je $S \subset \mathcal{P}, |S| = s$. Tvrdnju teorema dobivamo prebrojavanjem na dva načina elemenata skupa $\{(T, B) \mid S \subset T \subseteq B, |T| = t, B \in \mathcal{B}\}$. \square

Za $s = 0$ dobivamo broj blokova koji sadrže prazan skup, dakle ukupan broj blokova u t -dizajnu, dok za $s = 1$ dobivamo broj blokova t -dizajna incidentnih s jednom njegovom točkom.

Korolar 2.2. *Za svaku točku $P \in \mathcal{P}$ t -dizajna \mathcal{D} , broj blokova incidentnih s tom točkom jednak je*

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

2.2 Uvod u teoriju dizajna

Ukupan broj blokova b dizajna \mathcal{D} jednak je

$$b = \lambda_0 = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Iz teorema 2.1 slijedi rekurzija za parametre λ_s

$$\lambda_s = \frac{v-s}{k-s} \lambda_{s+1}. \quad (2.1)$$

Kažemo da je uređena četvorka (t, v, k, λ) dopustiva, ako je svaki $\lambda_s = \lambda \binom{v-s}{t-s} / \binom{k-s}{t-s}$ prirodni broj, za $s = 0, \dots, t$. Kažemo da je uređena četvorka (t, v, k, λ) ostvariva ako postoji dizajn s tim parametrima. Dopustivost ne implicira ostvarivost. Na primjer, uređena četvorka $(3, 8, 4, 1)$ je i dopustiva i ostvariva. Uređena četvorka $(2, 43, 7, 1)$ je dopustiva, ali nije ostvariva. Uređena četvorka $(3, 16, 7, 5)$ je dopustiva, ali ne zna se da li je ostvariva.

Definicija 2.12. Neka je \mathcal{D} t -dizajn za $t \geq 2$. Red dizajna \mathcal{D} je $n = \lambda_1 - \lambda_2$, odnosno za blokovni dizajn $n = r - \lambda$.

Dokaze sljedeća dva teorema može se naći u [60].

Teorem 2.2. Neka je M $(0, 1)$ -matrica dimenzije $v \times b$. Matrica M je matrica incidencije 2 - (v, k, λ) dizajna ako i samo ako vrijedi:

1. $MM^T = \lambda J_v + (r - \lambda)I_v$,
2. $u_v M = k u_b$,

gdje je I_v jedinična matrica reda v , J_v matrica reda v čiji su svi elementi jednaki 1, u_v (u_b) je vektor duljine v (b) čiji su svi elementi jednaki 1.

Teorem 2.3. Neka su $M = [m_{i,j}]$ i $M' = [m'_{i,j}]$ matrice incidencije dva blokovna dizajna \mathcal{D} i \mathcal{D}' . Dizajni \mathcal{D} i \mathcal{D}' su izomorfni ako i samo ako postoje permutacija α skupa $\{1, \dots, v\}$ i permutacija β skupa $\{1, \dots, b\}$ takve da je $m_{i,j} = m'_{\alpha(i),\beta(j)}$ za sve $1 \leq i \leq v$, $1 \leq j \leq b$.

Teorem 2.4. Neka je \mathcal{D} 2 - (v, k, λ) dizajn reda n i neka je M njegova matrica incidencije. Ako \mathcal{D} nije trivijalan, tada je rang matrice M nad poljem racionalnih brojeva \mathbb{Q} jednak v .

Dokaz. Znamo da za $b \times v$ matricu incidencije M vrijedi $M^T M = \lambda J_v + (r - \lambda)I_v$, pa je $\det(M^T M) = rkn^{v-1}$. Kako je $\text{rang}(M) \geq \text{rang}(M^T M)$ i $M^T M$ je kvadratna matrica reda v , njezin rang je jednak v ako i samo ako joj je determinanta različita od nule. Znamo da je $\det(M^T M) = rkn^{v-1}$ i $k, r \neq 0$. Ako je $n = 0$, tada $r = \lambda(v-1)/(k-1) = \lambda$ daje $v = k$, što je u kontradikciji s pretpostavkom da \mathcal{D} nije trivijalan. \square

Korolar 2.3. (*Fisherova nejednakost*) Ako postoji $2-(v, k, \lambda)$ dizajn, onda je $b \geq v$.

Definicija 2.13. Za nepotpuni $t-(v, k, \lambda)$ dizajn kažemo da je simetričan ako vrijedi $b = v$.

Iz definicije simetričnog dizajna slijedi da je $1 < k < v - 1$. Osim toga, s obzirom da za $t-(v, k, \lambda)$ dizajn vrijedi $vr = bk$, slijedi da za simetričan dizajn vrijedi $r = k$.

Propozicija 2.2. Ako je $t-(v, k, \lambda)$ dizajn simetričan, tada je $t \leq 2$.

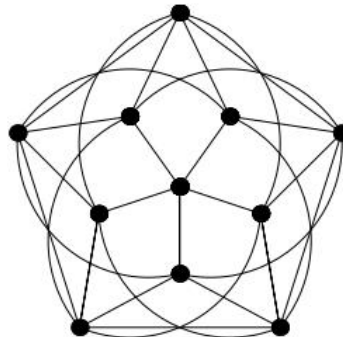
Dokaz. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ simetričan $t-(v, k, \lambda)$ dizajn i neka je $t \geq 3$. Prema teoremu 2.1, postoji λ' takav da je \mathcal{D} također i $3-(v, k, \lambda')$ dizajn. Za točku $P \in \mathcal{P}$ definiramo dizajn $\mathcal{D}' = (\mathcal{P}', \mathcal{B}', \mathcal{I}')$, pri čemu je $\mathcal{P}' = \mathcal{P} - \{P\}$ i $\mathcal{B}' = \{x - \{P\} \mid x \in \mathcal{B}, P \in x\}$. \mathcal{D}' je $2-(v - 1, k - 1, \lambda')$ dizajn sa r blokova. Iz Fisherove nejednakosti slijedi $r \geq v - 1$. S druge strane, s obzirom da je \mathcal{D} simetričan dizajn, vrijedi $r = k$, pa slijedi $k \geq v - 1$. Stoga, \mathcal{D} je potpun $(v - 1)-(v, v - 1, 1)$ dizajn, što je u kontradikciji s pretpostavkom da je simetričan dizajn. \square

Komplementarna incidencijska struktura t -dizajna također je t -dizajn, ([63]). Komplementaran dizajn $2-(v, k, \lambda)$ dizajna \mathcal{D} je dizajn s parametrima $2-(v, v - k, b - 2r + \lambda)$. Ako je \mathcal{D} simetričan blokovni dizajn, tada je i njegov komplement simetričan dizajn.

Definicija 2.14. Projektivna ravnina reda n je simetrični blokovni dizajn s parametrima $2-(n^2 + n + 1, n + 1, 1)$.

Definicija 2.15. Simetričan dizajn s parametrima $2-(v, k, 2)$ naziva se dvoravnina.

Poznate su dvoravnine $2-(v, k, 2)$ samo za parametre $k = 4, 5, 6, 9, 11, 13$, prema napomeni 6.14 u [12]. Do na izomorfizam, postoji jedna dvoravnina s parametrima $2-(11, 5, 2)$, tzv. Paleyjeva dvoravnina, prikazana na slici 2.2. Pretraživanjem matrice incidencije simetričnih $2-(66, 26, 10)$ dizajna tražimo $2-(11, 5, 2)$ dizajne kao poddizajne početnih dizajna, primjenom modificiranog genetskog algoritma, opisanog u poglavlju 8.2.



Slika 2.2: Dvoravnina s parametrima $2-(11, 5, 2)$

Dokaz sljedećeg teorema može se naći u [60].

2.3 Izomorfizmi blokovnih dizajna

Teorem 2.5. *U simetričnom $2-(v, k, \lambda)$ dizajnu svaka dva bloka su incidentna s točno λ zajedničkih točaka.*

Sljedeći rezultat ističe da je dual simetričnog dizajna također simetričan dizajn, što je direktna posljedica tvrdnje teorema 2.5.

Korolar 2.4. *Neka je M matrica incidencije simetričnog $2-(v, k, \lambda)$ dizajna. Tada je M^T također matrica incidencije simetričnog $2-(v, k, \lambda)$ dizajna.*

Dokaz sljedećeg teorema može se naći u [58].

Teorem 2.6. *Neka je zadan skup $\mathcal{P} = \{P_1, \dots, P_v\}$ i neka se skup \mathcal{B} sastoji od v k -članih podskupova skupa \mathcal{P} takvih da svaka dva različita podskupa imaju točno λ zajedničkih elemenata. Tada je $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ simetričan blokovni dizajn, pri čemu je \mathcal{I} relacija pripadnosti.*

Definicija 2.16. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ $2-(v, k, \lambda)$ dizajn. Paralelna klasa u \mathcal{D} je skup koji se sastoji od disjunktne blokova iz \mathcal{B} čija unija je \mathcal{P} .

Paralelna klasa sadrži $\frac{v}{k}$ blokova i dizajn \mathcal{D} može imati paralelnu klasu jedino ako je $v \equiv 0 \pmod{k}$.

Definicija 2.17. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn. Particija od \mathcal{B} na r paralelnih klasa naziva se rezolucija, a za \mathcal{D} kažemo da je rastavljiv dizajn ako \mathcal{B} ima barem jednu rezoluciju.

2.3 Izomorfizmi blokovnih dizajna

Izomorfizam blokovnih dizajna \mathcal{D}_1 i \mathcal{D}_2 je izomorfizam tih dizajna kao incidencijskih struktura. Automorfizam blokovnog dizajna je izomorfizam tog dizajna na samog sebe. Ukoliko želimo ustanoviti egzistenciju $2-(v, k, \lambda)$ dizajna na kojem djeluje odgovarajuća grupa automorfizama, od velike je pomoći ispitivanje egzistencije takozvane fiksne strukture te grupe.

Definicija 2.18. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn, $G \leq \text{Aut}(\mathcal{D})$, te $g \in G$. Točku $P \in \mathcal{P}$ nazivamo fiksnom točkom automorfizma g ako vrijedi $g.P = P$. Točku P nazivamo fiksnom točkom grupe automorfizama G , ako je $g.P = P$ za svaki $g \in G$. Analogno definiramo fiksni blok automorfizma, odnosno grupe automorfizama G .

Napomena 2.4. Uočimo da su fiksni blokovi za djelovanje grupe G na dizajn zapravo disjunktne unije G -orbita točaka. Analogno vrijedi za fiksne točke pri djelovanju grupe G na dizajn.

Definicija 2.19. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn i $G \leq \text{Aut}(\mathcal{D})$. Neka je $\mathcal{P}' \subseteq \mathcal{P}$ skup fiksnih točaka grupe G , a $\mathcal{B}' \subseteq \mathcal{B}$ skup fiksnih blokova grupe G . Fiksna struktura grupe G je struktura $(\mathcal{P}', \mathcal{B}', \mathcal{I}')$, pri čemu je relacija $\mathcal{I}' = \mathcal{I} \cap (\mathcal{P}' \times \mathcal{B}')$.

Istaknimo sljedećih nekoliko svojstava koja vrijede za Steinerove 2-dizajne.

Lema 2.2. Neka je α automorfizam 2- $(v, k, 1)$ dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. Ako α fiksira dvije točke, tada su one sadržane u fiksnom bloku. Ako α fiksira dva bloka koji se sijeku, njihov presjek je fiksna točka.

Dokaz. Neka su zadane dvije fiksne točke $P_1, P_2 \in \mathcal{P}, P_1 \neq P_2$, te $B \in \mathcal{B}$ jedinstven blok koji sadrži te točke. Blok $\alpha.B \in \mathcal{B}$ sadrži točke $\alpha.P_1 = P_1$ i $\alpha.P_2 = P_2$, pa iz činjenice $\lambda = 1$ slijedi da je $\alpha.B = B$. Analogno bi se dokazala druga tvrdnja. \square

Direktna posljedica leme 2.2 je sljedeća tvrdnja.

Korolar 2.5. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ 2- $(v, k, 1)$ dizajn i automorfizam $\alpha \in \text{Aut}(\mathcal{D})$ prostog reda p . Označimo sa f_B broj fiksnih točaka automorfizma α u bloku $B \in \mathcal{B}$. Ako blok B sadrži barem dvije fiksne točke, tada vrijedi $f_B \equiv k \pmod{p}$.

Dokaz sljedećeg teorema o gornjoj granici za broj fiksnih točaka 2- $(v, k, 1)$ dizajna uz djelovanje automorfizma prostog reda može se naći u [40].

Teorem 2.7. Neka je α automorfizam prostog reda p koji djeluje na 2- $(v, k, 1)$ dizajn. Ako α fiksira f točaka, tada vrijedi

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

V. Čepulić 1994. godine u [21] uvodi koncept G -izomorfizma dvaju blokovnih dizajna koji ima jako važnu ulogu u algoritmima za konstrukciju blokovnih dizajna napravljenim u sklopu ovog rada.

Definicija 2.20. Neka su $\mathcal{D}_1 = (\mathcal{P}, \mathcal{B}, \mathcal{I}_1)$ i $\mathcal{D}_2 = (\mathcal{P}, \mathcal{B}, \mathcal{I}_2)$ blokovni dizajni i $G \leq \text{Aut}(\mathcal{D}_1) \cap \text{Aut}(\mathcal{D}_2) \leq S = S(\mathcal{P}) \times S(\mathcal{B})$. Za preslikavanje $\alpha \in S$ kažemo da je G -izomorfizam iz \mathcal{D}_1 na \mathcal{D}_2 ako vrijedi:

1. $\alpha : \mathcal{D}_1 \rightarrow \mathcal{D}_2$ je izomorfizam,
2. postoji automorfizam $\tau : G \rightarrow G$ takav da za sve $P, Q \in \mathcal{P}$ i $\forall g \in G$ vrijedi:

$$(\tau g).(\alpha.P) = \alpha.Q \Leftrightarrow g.P = Q.$$

2.3 Izomorfizmi blokovnih dizajna

U tom slučaju kažemo da su dizajni \mathcal{D}_1 i \mathcal{D}_2 G -izomorfni. Ako $\mathcal{I}_1 = \mathcal{I}_2$, tada kažemo da je α G -automorfizam dizajna \mathcal{D} , pri čemu je $\mathcal{D} = \mathcal{D}_1 = \mathcal{D}_2$.

Napomena 2.5. Neka je α G -izomorfizam iz \mathcal{D}_1 na \mathcal{D}_2 . Točke P i Q su u istoj G -orbiti ako i samo ako su točke $\alpha.P$ i $\alpha.Q$ u istoj G -orbiti. Analogno vrijedi za blokove.

Lema 2.3. *Neka su $\mathcal{D}_1 = (\mathcal{P}, \mathcal{B}, \mathcal{I}_1)$ i $\mathcal{D}_2 = (\mathcal{P}, \mathcal{B}, \mathcal{I}_2)$ blokovni dizajni, $G \leq \text{Aut}(\mathcal{D}_1) \cap \text{Aut}(\mathcal{D}_2) \leq S = S(\mathcal{P}) \times S(\mathcal{B})$. Za $\alpha \in S$ vrijedi da je G -izomorfizam iz \mathcal{D}_1 na \mathcal{D}_2 ako i samo ako je α izomorfizam iz \mathcal{D}_1 na \mathcal{D}_2 i sadržana je u normalizatoru $N_S(G)$.*

Dokaz. Neka je α G -izomorfizam iz \mathcal{D}_1 na \mathcal{D}_2 , te $g \in G, P \in \mathcal{P}$ i $g.P = Q$. Prema definiciji G -izomorfizma postoji $\tau \in \text{Aut}(G)$ takav da vrijedi $(\tau g).(\alpha.P) = \alpha.Q$, odnosno $(\tau g).(\alpha.P) = \alpha.(g.P)$. Ova jednakost vrijedi za svaku točku $P \in \mathcal{P}$, pa vrijedi da je $(\tau g)\alpha = \alpha g$, odakle slijedi da je $\tau g = \alpha g \alpha^{-1}$. Jasno, $\alpha \in N_S(G)$ jer je $\alpha G \alpha^{-1} = \tau G = G$. S druge strane, neka je $\alpha \in N_S(G)$, odnosno $\alpha G \alpha^{-1} = G$ i neka je zadan automorfizam grupe G , $\tau : G \rightarrow G, \tau g = \alpha g \alpha^{-1}$. Slijedi da je $(\tau g)\alpha = \alpha g$ i za točku P vrijedi $(\tau g).(\alpha.P) = \alpha.Q \Leftrightarrow g.P = Q$. Time je dokazana tvrdnja. \square

Direktna posljedica definicije G -izomorfizma i prethodne leme je sljedeća tvrdnja.

Propozicija 2.3. *Neka je G grupa automorfizama blokovnog dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, $S = S(\mathcal{P}) \times S(\mathcal{B})$ i $\alpha \in N_S(G)$. Tada je α G -izomorfizam iz \mathcal{D} na $\mathcal{D}_\alpha = (\mathcal{P}, \mathcal{B}, \mathcal{I}_\alpha)$, pri čemu je $(P_\alpha, x_\alpha) \in \mathcal{I}_\alpha \Leftrightarrow (P, x) \in \mathcal{I}$.*

Kako bismo u razvijenim algoritmima za konstrukciju blokovnih dizajna reducirali broj orbitnih matrica iz kojih će se konstruirati izomorfni dizajni i time znatno smanjili vrijeme potrebno za izvođenje algoritama, bitno je odrediti elemente iz normalizatora $N_S(G)$.

Sada promotrimo automorfizme simetričnih dizajna. Općenito, izomorfizmi simetričnih blokovnih dizajna određeni su svojim djelovanjem na skupu točaka ili blokova. Zbog toga se često opisuje samo djelovanje izomorfizma na skupu točaka.

Propozicija 2.4. *Automorfizam simetričnog blokovnog dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ fiksira jednaki broj točaka i blokova.*

Dokaz. Neka je $\alpha \in \text{Aut}(\mathcal{D})$ koji fiksira F_1 točaka i F_2 blokova. Prebrojavanjem na dva načina elementa skupa $\{(P, \alpha.P, x) \mid P \in \mathcal{P}, (P, x) \in \mathcal{I}, (\alpha.P, x) \in \mathcal{I}\}$ dobivamo jednakost

$$F_1 k + (v - F_1)\lambda = F_2 k + (v - F_2)\lambda,$$

odakle slijedi $(F_1 - F_2)k = (F_1 - F_2)\lambda$. Ako je $F_1 \neq F_2$, onda vrijedi da je $k = \lambda$, što je nemoguće zbog definicije simetričnih dizajna. \square

Dokaz sljedeće propozicije može se pronaći u [41].

Propozicija 2.5. *Neka je α automorfizam simetričnog blokovnog dizajna $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, te neka je $\alpha = (\pi_1, \pi_2) \in S(\mathcal{P}) \times S(\mathcal{B})$. Tada permutacije π_1 i π_2 imaju jednaku cikličku strukturu.*

Propozicija 2.6. *Ako je G grupa automorfizama simetričnog blokovnog dizajna, tada G ima jednak broj orbita na skupu točaka i skupu blokova.*

Dokaz. Označimo sa t_1 i t_2 broj orbita na skupu točaka, odnosno blokova. Vrijedi

$$t_1 = \frac{1}{|G|} \sum_{g \in G} F_1(g) = \frac{1}{|G|} \sum_{g \in G} F_2(g) = t_2,$$

pri čemu su $F_1(g)$ i $F_2(g)$ broj fiksnih točaka odnosno blokova automorfizma $g \in G$. \square

Napomena 2.6. Grupa automorfizama simetričnog blokovnog dizajna djeluje tranzitivno na skupu točaka ako i samo ako djeluje tranzitivno na skupu blokova. Također vrijedi da grupa automorfizama djeluje regularno na skupu točaka ako i samo ako djeluje regularno na skupu blokova.

Simetrične dizajne na koje regularno djeluje neka grupa automorfizama moguće je konstruirati iz diferencijskog skupa u toj grupi.

Definicija 2.21. Neka je G konačna grupa reda $v \in \mathbb{N}$. Neka su $k, \lambda \in \mathbb{N}$ takvi da je $2 \leq k < v$. (v, k, λ) diferencijski skup u grupi G je podskup $D \subseteq G$ za koji vrijede sljedeća svojstva:

1. $|D| = k$,
2. multiskup $\{xy^{-1} \mid x, y \in D, x \neq y\}$ sadrži svaki element iz $G \setminus \{1\}$ točno λ puta.

Nužan uvjet za egzistenciju (v, k, λ) diferencijskog skupa u grupi G je $\lambda(v-1) = k(k-1)$.

Primjer 2.2. Skup $D = \{0, 1, 6, 8, 18\}$ je $(21, 5, 1)$ diferencijski skup u grupi $(\mathbb{Z}_{21}, +)$.

Definicija 2.22. Neka je D (v, k, λ) diferencijski skup u grupi G . Za svaki $g \in G$ definiramo skup

$$Dg = \{xg \mid x \in D\},$$

kojeg nazivamo translat od D (u aditivnom zapisu $D + g$). Kolekciju svih translata od D označimo sa

$$\text{Dev}(D) = \{Dg \mid g \in G\}.$$

Skup $\text{Dev}(D)$ nazivamo razvoj od D .

Dokaz sljedećeg teorema može se pronaći u [35].

2.3 Izomorfizmi blokovnih dizajna

Teorem 2.8. *Postoji (v, k, λ) diferencijski skup u grupi G ako i samo ako postoji simetričan 2 - (v, k, λ) dizajn na koji regularno djeluje grupa G kao grupa automorfizama.*

Dokaz tvrdnji sljedećih propozicija može se pronaći u [41].

Propozicija 2.7. *Neka je $\alpha \neq 1$ automorfizam simetričnog 2 - (v, k, λ) dizajna. Ako α fiksira F točaka, onda vrijedi $F \leq v - 2n$ i $F \leq \frac{\lambda}{k - \sqrt{n}}v$. Ako u nekoj od tih nejednakosti vrijedi jednakost, onda α mora biti involucija i svaki nefiksni blok sadrži točno λ fiksnih točaka.*

Napomena 2.7. U literaturi se često pojavljuje nejednakost $F \leq k + \sqrt{n}$. Ta je nejednakost ekvivalentna nejednakosti $F \leq \frac{\lambda}{k - \sqrt{n}}v$ iz prethodne propozicije.

Definicija 2.23. Kažemo da grupa automorfizama G djeluje polustandardno na simetričnom blokovnom dizajnu ako su multiskupovi duljina orbita točaka i blokova jednaki. Ako su svi elementi multiskupa duljina orbita točaka jednaki 1 ili $|G|$, onda kažemo da grupa G djeluje standardno na simetričnom blokovnom dizajnu.

Napomena 2.8. Neka je $G = \langle g \rangle$ ciklička grupa automorfizama simetričnog blokovnog dizajna \mathcal{D} . Iz propozicije 2.5 slijedi da G djeluje polustandardno na \mathcal{D} . Ako je $|g|$ prost broj, tada G djeluje standardno na \mathcal{D} i vrijedi

1. $v = F + |g| \cdot (t - F)$,

2. $F \equiv v \pmod{|g|}$,

pri čemu je t broj orbita točaka.

Propozicija 2.8. *Neka grupa automorfizama G djeluje polustandardno na simetričnom 2 - (v, k, λ) dizajnu. Tada je red tog dizajna $n = k - \lambda$ kvadrat cijelog broja ili je broj G -orbita na skupu točaka neparan broj.*

Propozicija 2.9. *Neka je \mathcal{D} simetričan 2 - (v, k, λ) dizajn i neka je $\alpha \in \text{Aut}(\mathcal{D})$. Ako je α involucija koja fiksira $F \neq 0$ točaka, onda je*

$$F \geq \begin{cases} 1 + \frac{k}{\lambda}, & \text{za } k, \lambda \text{ parne brojeve,} \\ 1 + \frac{k-1}{\lambda}, & \text{inače.} \end{cases}$$

Dokaz sljedeće propozicije može se pronaći u [1].

Propozicija 2.10. *Ako je α automorfizam prostog reda simetričnog 2 - (v, k, λ) dizajna, tada $|\alpha|$ dijeli v ili $|\alpha| \leq k$.*

2.4 Unitali

Sam naziv unital proizlazi iz činjenice da su prvi primjeri unitala, odnosno dizajni s parametrima $2-(q^3 + 1, q + 1, 1)$, konstruirani iz skupa apsolutnih točaka i neapsolutnih pravaca unitarnog polariteta konačne projektivne ravnine reda q^2 , za q potenciju prostog broja.

Definicija 2.24. Neka je $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ projektivna ravnina. Bijekciju $\rho : \mathcal{P} \cup \mathcal{L} \rightarrow \mathcal{P} \cup \mathcal{L}$ takva da vrijedi $\rho(\mathcal{P}) = \mathcal{L}$, $\rho(\mathcal{L}) = \mathcal{P}$, te $(P, m) \in \mathcal{I} \iff (\rho(m), \rho(P)) \in \mathcal{I}$, $\forall P \in \mathcal{P}$ i $\forall m \in \mathcal{L}$, nazivamo korelacija projektivne ravnine. Polaritet ρ je involutorna korelacija, odnosno vrijedi $\rho^2 = id$.

Definicija 2.25. Neka je ρ polaritet projektivne ravnine $(\mathcal{P}, \mathcal{L}, \mathcal{I})$. Točke i blokove zovemo apsolutnim ako su incidentni sa svojom ρ -slikom. Inače ih zovemo neapsolutnim točkama, odnosno blokovima.

Dokazi tvrdnji sljedećih teorema nalaze se u [29].

Teorem 2.9. Neka je ρ polaritet projektivne ravnine reda $n = m^2$. Tada vrijedi $n + 1 \leq a(\rho) \leq m^3 + 1$, gdje je $a(\rho)$ broj apsolutnih točaka polariteta ρ .

Definicija 2.26. Neka je dana projektivna ravnina reda $n = m^2$. Polaritete čiji je broj apsolutnih točaka maksimalan, odnosno jednak $m^3 + 1$, nazivamo unitarni polariteti.

Teorem 2.10. Neka je ρ unitarni polaritet projektivne ravnine reda $n = m^2$. Skup apsolutnih točaka i neapsolutnih pravaca od ρ čine unital, odnosno $2-(m^3 + 1, m + 1, 1)$ dizajn.

Klasična projektivna ravnina reda q^2 , gdje je q potencija prostog broja, ima unitarni polaritet. Unital, odnosno $2-(q^3 + 1, q + 1, 1)$ dizajn, dobiven iz tog unitarnog polariteta nazivamo klasični ili Hermitski unital. Rezultati o unitalima i unitarnim polaritetima projektivne ravnine mogu se pronaći u [4], [22] i [29].

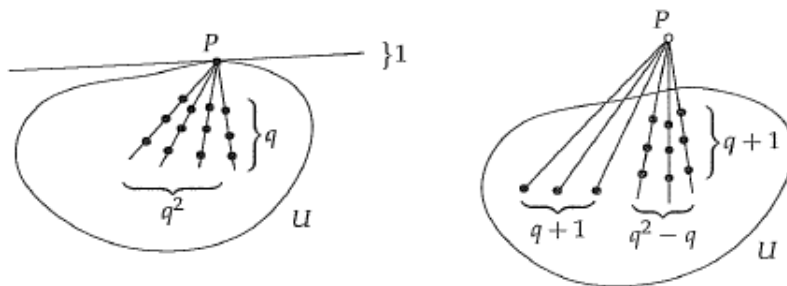
Iz kombinatoričkog gledišta, unital u projektivnoj ravnini \mathcal{A} reda $n = q^2$ je skup \mathcal{U} koji se sastoji od $q^3 + 1$ točaka i ima sljedeće svojstvo:

- kroz svaku točku $P \in \mathcal{U}$ prolazi točno jedan pravac (tangenta) iz \mathcal{A} koji presijeca \mathcal{U} u točki P , te postoji q^2 pravaca (sekanti) iz \mathcal{A} koji presijecaju \mathcal{U} u $q + 1$ točaka.

Stoga, unital uložen u projektivnu ravninu možemo definirati pomoću ovog svojstva, bez da promatramo unitarni polaritet.

Osim toga, vrijedi da kroz svaku točku $P \in \mathcal{A} \setminus \mathcal{U}$ prolazi $q + 1$ tangenti i $q^2 - q$ sekanti koje presijecaju \mathcal{U} u $q + 1$ točaka, što je ilustrirano na slici 2.3.

Unitali se također definiraju kao $2-(s^3 + 1, s + 1, 1)$ dizajni za $s > 1$. Stoga, unital ne mora nužno biti dobiven iz unitarnog polariteta, niti uložen u projektivnu ravninu, što je


 Slika 2.3: Broj tangenti i sekanti kroz točku $P \in U$ i $P \in A \setminus U$

pokazano u [10]. Prvi unital, s blokom veličine 7, za kojeg nije poznato može li se uložiti u projektivnu ravninu reda 36 konstruirali su neovisno jedan o drugome S. Bagchi i B. Bagchi ([3]), te Mathon ([45]).

Pojam unitala uloženog u projektivnu ravninu proširen je do pojma unitala uloženog u simetričan dizajn. Prvi put takve se strukture, pod drugačijim nazivom, M. J. de Resmini promatra u radu [52].

Definicija 2.27. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ simetričan 2 - (v, k, λ) dizajn. Neka je $\mathcal{U} \subseteq \mathcal{P}$ sa svojstvom da je svaka točka $P \in \mathcal{U}$ incidentna sa $k - 1$ blokova iz \mathcal{B} koji sijeku \mathcal{U} u α točaka i s točno jednim blokom koji presijeca \mathcal{U} u točki P .

Podskup \mathcal{U} nazivamo unital. Blokove iz \mathcal{B} koji \mathcal{U} sijeku u α točaka nazivamo sekante, dok blokove koji ga presijecaju u jednoj točki nazivamo tangente.

U sljedećim lemeta navodimo nekoliko osnovnih svojstava unitala u simetričnim blokovnim dizajnama. Dokaze sljedećih lema moguće je pronaći u [52].

Lema 2.4. Neka je \mathcal{U} podskup skupa točaka simetričnog 2 - (v, k, λ) dizajna \mathcal{D} koji ima svojstvo iz prethodne definicije. Tada vrijedi:

- (i) $n = k - \lambda$ je kvadrat,
- (ii) $\alpha = \sqrt{n} + 1$,
- (iii) $|\mathcal{U}| = 1 + (k - 1)\sqrt{n}/\lambda$, posebno $1 + (k - 1)\sqrt{n}/\lambda \in \mathbb{N}$,
- (iv) Točke od \mathcal{U} i njegove sekante čine 2 - $(1 + (k - 1)\sqrt{n}/\lambda, \sqrt{n} + 1, \lambda)$ dizajn.

Također i dizajn dobiven iz \mathcal{U} i pripadnih sekanti nazivamo unital.

Sljedeće dvije leme daju karakterizaciju unitala.

Lema 2.5. Neka je \mathcal{U} skup od $u = 1 + (k - 1)\sqrt{n}/\lambda$ točaka simetričnog 2 - (v, k, λ) dizajna \mathcal{D} . Pretpostavimo da svaki blok iz \mathcal{D} presijeca \mathcal{U} u 1 ili $\sqrt{n} + 1$ točaka. Tada je \mathcal{U} unital.

Lema 2.6. *Neka je \mathcal{U} unital u simetričnom $2-(v, k, \lambda)$ dizajnu \mathcal{D} i neka točka P nije element iz \mathcal{U} . Tada kroz tu točku prolazi $(\sqrt{n} + 1)$ tangenti i $(k - \sqrt{n} - 1)$ sekanti.*

Napomena 2.9. Dual unitala \mathcal{U} uloženog u projektivnu ravninu \mathcal{P} reda m^2 je unital s oznakom \mathcal{U}^* , koji ima iste parametre kao \mathcal{U} i uložen je u projektivnu ravninu \mathcal{P}^* , ([4]). Analogno tome, vrijedi da ako simetričan blokovni dizajn \mathcal{D} sadrži unital, isto tako će unital sadržavati i njegov dual \mathcal{D}^* .

R. Mathon i T. van Trung u članku [46] navode sljedeća dva primjera unitala u simetričnim dizajnim.

Primjer 2.3. Simetričan $2-(36, 15, 6)$ dizajn \mathcal{D} (konstruiran u [14]) s punom grupom automorfizama reda 42 koja je izomorfna s grupom $Frob_{21} \times Z_2$, sadrži barem tri unitala, odnosno tri rastavljiva blokovna dizajna s parametrima $2-(8, 4, 6)$. Naime, označimo točke dizajna \mathcal{D} sa $\mathcal{P} = \{\infty, i_0, i_1, i_2, i_3, i_4, i_5, i_6, \mid i = 1, \dots, 5\}$ i automorfizam ρ tog dizajna koji djeluje na skup točaka na sljedeći način $\rho = (\infty)(i_0, i_1, i_2, i_3, i_4, i_5, i_6), i = 1, \dots, 5$. Predstavnicu orbita blokova za djelovanje automorfizma ρ :

$\infty 1_0 1_1 1_2 1_3 1_4 1_5 1_6 2_0 2_1 2_2 2_3 2_4 2_5 2_6,$
 $\infty 1_0 1_1 1_2 1_4 2_0 3_1 3_2 3_4 4_3 4_6 4_5 5_1 5_2 5_4,$
 $\infty 2_0 2_1 2_2 2_4 1_0 4_1 4_2 4_4 3_3 3_6 3_5 5_1 5_2 5_4,$
 $1_1 1_2 1_4 2_3 2_6 2_5 3_0 3_3 3_6 3_5 4_0 5_0 5_1 5_2 5_4,$
 $2_1 2_2 2_4 1_3 1_6 1_5 4_0 4_3 4_6 4_5 3_0 5_0 5_1 5_2 5_4,$
 $1_1 1_2 1_4 2_1 2_2 2_4 3_0 3_1 3_2 3_4 4_0 4_1 4_2 4_4 5_0.$

Lako je provjeriti da su skupovi točaka $\{\infty, 3_0, 3_1, 3_2, 3_3, 3_4, 3_5, 3_6\}$, $\{\infty, 4_0, 4_1, 4_2, 4_3, 4_4, 4_5, 4_6\}$, i $\{\infty, 5_0, 5_1, 5_2, 5_3, 5_4, 5_5, 5_6\}$ unitali u dizajnu \mathcal{D} za djelovanje automorfizma ρ .

Primjer 2.4. T. van Trung u [64] konstruirao prvi simetričan $2-(66, 26, 10)$ dizajn kojeg označimo sa \mathcal{D}' . Taj dizajn sadrži barem šest unitala, odnosno blokovnih dizajna s parametrima $2-(11, 5, 10)$. Naime, označimo točke dizajna \mathcal{D}' sa $\mathcal{P}' = \{1_i, \dots, 6_i \mid i = 0, 1, \dots, 10\}$ i neka su automorfizmi ρ i σ tog dizajna koji djeluju na skupu točaka $\rho = (I_0, I_1, \dots, I_{10}), I = 1, 2, \dots, 6$ i $\sigma = (1_i, 2_i, 3_i, 4_i, 5_i)(6_i), i = 0, 1, \dots, 10$. Predstavnicu orbita blokova za djelovanje automorfizama ρ i σ :

$1_1 1_3 1_4 1_5 1_9 2_2 2_6 2_7 2_8 2_{10} 3_2 3_6 3_7 3_8 3_{10} 4_1 4_3 4_4 4_5 4_9 5_0 6_1 6_3 6_4 6_5 6_9$
 $1_2 1_6 1_7 1_8 1_{10} 2_2 2_6 2_7 2_8 2_{10} 3_2 3_6 3_7 3_8 3_{10} 4_2 4_6 4_7 4_8 4_{10} 5_2 5_6 5_7 5_8 5_{10} 6_0$

Lako je provjeriti da svaka od šest $\langle \rho \rangle$ -orbita točaka čini unital.

Poglavlje 3

Konstrukcije blokovnih dizajna s pretpostavljenom grupom automorfizama

Kramer-Mesnerova metoda opisana u [36] i metoda taktičke dekompozicije opisana u [34] poznate su metode za konstrukciju dizajna s pretpostavljenom grupom automorfizama. U ovom poglavlju opisat ćemo metodu taktičke dekompozicije za konstrukciju blokovnih dizajna. Z. Janko je razvio način konstrukcije blokovnih dizajna s pretpostavkom djelovanja neke grupe automorfizama na dizajn, čime se pojednostavljuje konstrukcija, ali se u većini slučajeva ne konstruiraju svi dizajni sa zadanim parametrima ([32]). Ta se konstrukcija sastoji od dva osnovna koraka koje ćemo opisati u ovom poglavlju. Definirat ćemo točkovne orbitne matrice blokovnih dizajna i uvesti poredak u skupu blokovnih dizajna s istom orbitnom matricom, po uzoru na to kako je radio V. Čepulić pri konstrukciji blokovnih orbitnih matrica simetričnih dizajna ([21]).

U ovom poglavlju ćemo opisati, u sklopu ovog rada, razvijen algoritam za konstrukciju neizomorfnih točkovnih orbitnih matrica nekog blokovnog dizajna uz pretpostavku djelovanja proizvoljne grupe automorfizama na taj dizajn. Taj je algoritam generalizacija algoritma za konstrukciju neizomorfnih blokovnih orbitnih matrica simetričnih dizajna, opisanog u [21]. Osim toga, opisat ćemo algoritam za profinjenje (dekompoziciju) orbitnih matrica koji se temelji na primjeni kompozicijskog niza rješive grupe automorfizama blokovnih dizajna. U oba algoritma koristimo elemente normalizatora grupe za koju pretpostavljamo da djeluje na blokovni dizajn. Time reduciramo broj orbitnih matrica iz kojih će se konstruirati izomorfni dizajni i skraćujemo vrijeme potrebno za izvođenje programa napisanih na temelju spomenutih algoritama. Indeksiranje se provodi kao specijalni slučaj profinjenja. Implementacija spomenutih algoritama napravljena je u obliku računalnih programa napisanih za program GAP, ([25]).

3.1 Metoda taktičke dekompozicije i orbitne matrice

P. Dembowski prvi uvodi ideju korištenja taktičke dekompozicije blokovnih dizajna ([23]). Metoda taktičke dekompozicije je metoda za konstrukciju blokovnih dizajna s pretpostavljenom konačnom grupom automorfizama. Ovu metodu koristio je Z. Janko za konstrukciju raznih primjera simetričnih blokovnih dizajna ([33], [34]). Osim toga, postoji još niz rezultata dobivenih ovom metodom, kao na primjer u [19], [28], [38] i [61].

Najprije ćemo razmotriti dekompozicije matrice, koje je uveo Block u radu [8].

Neka je M $v \times b$ matrica. Dekompozicija od M je particija $\mathcal{P}_1, \dots, \mathcal{P}_m$ redaka od M i particija $\mathcal{B}_1, \dots, \mathcal{B}_n$ stupaca od M . Označimo sa $\nu_i = |\mathcal{P}_i|$ i sa $\beta_j = |\mathcal{B}_j|$, $1 \leq i \leq m, 1 \leq j \leq n$, te označimo sa $M_{i,j}$ $\nu_i \times \beta_j$ matricu koja se sastoji od elemenata iz presjeka redaka iz \mathcal{P}_i i stupaca iz \mathcal{B}_j .

Definicija 3.1. Ako je za $i = 1, \dots, m$ i $j = 1, \dots, n$ suma elemenata u svakom retku matrice $M_{i,j}$ konstantna, kažemo da je dekompozicija taktička po retcima. Ako je za $i = 1, \dots, m$ i $j = 1, \dots, n$ suma elemenata u svakom stupcu matrice $M_{i,j}$ konstantna, kažemo da je dekompozicija taktička po stupcima. Za dekompoziciju matrice kažemo da je taktička ako je taktička po retcima i po stupcima.

Dokaz sljedeće propozicije može se naći u [7].

Propozicija 3.1. *Neka je M $v \times b$ matrica i $\text{rang}(M) = v$. Za taktičku dekompoziciju matrice M vrijedi $0 \leq n - m \leq b - v$.*

Definicija 3.2. Particija skupa točaka i blokova dizajna \mathcal{D} naziva se taktička po točkama, taktička po blokovima ili taktička dekompozicija od \mathcal{D} ako odgovara taktičkoj po retcima, taktičkoj po stupcima ili taktičkoj dekompoziciji njegove matrice incidencije.

Propozicija 3.2. *Neka su $\mathcal{P}_1, \dots, \mathcal{P}_m$ i $\mathcal{B}_1, \dots, \mathcal{B}_n$ particije skupa točaka i skupa blokova dizajna \mathcal{D} . Tada je dekompozicija dizajna*

- 1) *taktička po točkama ako i samo ako je svaka točka iz \mathcal{P}_i incidentna s konstantnim brojem blokova iz $\mathcal{B}_j, i = 1, \dots, m, j = 1, \dots, n$,*
- 2) *taktička po blokovima ako i samo ako je svaki blok iz \mathcal{B}_j incidentan s konstantnim brojem točaka iz $\mathcal{P}_i, i = 1, \dots, m, j = 1, \dots, n$.*

Dokaz. 1) Neka je M $v \times b$ matrica incidencije dizajna \mathcal{D} . Prema definiciji, dekompozicija dizajna \mathcal{D} je taktička po točkama ako i samo ako je suma elemenata u svakom retku matrice $M_{i,j}$ konstantna i označimo je sa $a_{i,j}$, za $i = 1, \dots, m, j = 1, \dots, n$. S obzirom da je M 0-1 matrica, slijedi da matrica $M_{i,j}$ u svakom retku ima $a_{i,j}$ jedinica, što odgovara

3.1 Metoda taktičke dekompozicije i orbitne matrice

broju blokova iz klase \mathcal{B}_j incidentnih s točkom iz klase \mathcal{P}_i . Analogno bi se dokazala tvrdnja 2). \square

Postoje dvije trivijalne taktičke dekompozicije dizajna, to je dekompozicija u kojoj je svaka klasa točaka i blokova jednočlana i dekompozicija koja se sastoji od samo jedne klase točaka i jedne klase blokova. Osim trivijalnih postoje i netrivialne taktičke dekompozicije dizajna.

Sljedeća propozicija daje važan primjer taktičke dekompozicije.

Propozicija 3.3. *Neka grupa G djeluje na dizajn $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. Tada G -orbite točaka i blokova daju taktičku dekompoziciju dizajna \mathcal{D} .*

Dokaz. Kako bi pokazali da je dekompozicija taktička po točkama, dovoljno je dokazati da su dvije proizvoljne točke iz neke G -orbite točaka \mathcal{P}_i , incidentne s istim brojem blokova iz G -orbite blokova \mathcal{B}_j . Neka su $P, Q \in \mathcal{P}_i$, $P \neq Q$, te označimo sa $x_1, \dots, x_k \in \mathcal{B}_j$ blokove incidentne s točkom P . Postoji $g \in G$ tako da je $g.P = Q$. Tada su $g.x_1, \dots, g.x_k$ blokovi iz \mathcal{B}_j incidentni s točkom Q . Analogno se polaže da je dekompozicija taktička po blokovima. \square

Dokaz sljedećeg teorema slijedi iz teorema 2.4, propozicije 3.1 i propozicije 3.3.

Teorem 3.1. *Neka je \mathcal{D} 2- (v, k, λ) dizajn. Ako $G \leq \text{Aut}(\mathcal{D})$ ima m orbita točaka i n orbita blokova, tada vrijedi $0 \leq n - m \leq b - v$.*

Tranzitivno djelovanje grupe G na skupu blokova dizajna povlači tranzitivno djelovanje i na skupu njegovih točaka, prema teoremu 3.1.

Posljedica teorema 3.1 je činjenica da u simetričnom blokovnom dizajnu broj G -orbita točaka je jednak broju G -orbita blokova, što je ujedno i tvrdnja propozicije 2.6.

U nastavku označavamo sa $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ 2- (v, k, λ) dizajn i $G \leq \text{Aut}(\mathcal{D})$. Označimo G -orbite točaka sa $\mathcal{P}_1, \dots, \mathcal{P}_m$ i G -orbite blokova sa $\mathcal{B}_1, \dots, \mathcal{B}_n$, te neka je

$$\nu_i = |\mathcal{P}_i|, \quad 1 \leq i \leq m,$$

$$\beta_j = |\mathcal{B}_j|, \quad 1 \leq j \leq n.$$

Očito je da vrijedi

$$\sum_{i=1}^m \nu_i = v, \quad \sum_{j=1}^n \beta_j = b, \quad b = |\mathcal{B}|.$$

Za blok $x \in \mathcal{B}$ i točku $P \in \mathcal{P}$ označimo

$$\langle x \rangle = \{Q \in \mathcal{P} \mid (Q, x) \in \mathcal{I}\},$$

$$\langle P \rangle = \{y \in \mathcal{B} \mid (P, y) \in \mathcal{I}\}.$$

S obzirom da G -orbite točaka i blokova daju taktičku dekompoziciju dizajna \mathcal{D} , za $P \in \mathcal{P}_i$ i $x \in \mathcal{B}_j$ označimo sa

$$a_{i,j} = |\langle P \rangle \cap \mathcal{B}_j|,$$

$$b_{i,j} = |\langle x \rangle \cap \mathcal{P}_i|.$$

Kako je $a_{i,j}$ broj blokova iz orbite blokova \mathcal{B}_j incidentnih s točkom iz orbite točaka \mathcal{P}_i , vrijedi

$$\sum_{j=1}^n a_{i,j} = r, \quad \forall i \in \{1, \dots, m\}.$$

Slično, vrijedi

$$\sum_{i=1}^m b_{i,j} = k, \quad \forall j \in \{1, \dots, n\}.$$

Osim toga, za $a_{i,j}$ i $b_{i,j}$ vrijede jednakosti iz sljedeće leme.

Lema 3.1. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn, $G \leq \text{Aut}(\mathcal{D})$, te kao ranije definirani ν_i , β_j , $a_{i,j}$ i $b_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n$. Vrijede sljedeće jednakosti:*

$$1) \nu_i a_{i,j} = \beta_j b_{i,j},$$

$$2) \sum_{j=1}^n a_{s,j} b_{t,j} = \lambda \nu_t + \delta_{st}(r - \lambda), \text{ gdje je } \delta_{st} \text{ Kroneckerov delta simbol,}$$

$$s, t \in \{1, \dots, m\}.$$

Dokaz. 1) Traženu jednakost dobit ćemo prebrojavanjem na dva načina elemenata skupa $\{(P, x) \mid (P, x) \in \mathcal{I}, P \in \mathcal{P}_i, x \in \mathcal{B}_j\}$.

2) Neka je $P \in \mathcal{P}_s$. Prebrojavanjem na dva načina elemenata skupa $\{(Q, x) \in \mathcal{P}_t \times \mathcal{B} \mid P, Q \in x\}$ dobivamo

$$\sum_{j=1}^n a_{s,j} b_{t,j} = \sum_{Q \in \mathcal{P}_t} |\langle P \rangle \cap \langle Q \rangle|.$$

Vrijedi

$$\sum_{j=1}^n a_{s,j} b_{t,j} = \sum_{Q \in \mathcal{P}_t} |\langle P \rangle \cap \langle Q \rangle| = \begin{cases} \lambda \nu_t, & s \neq t \\ \lambda(\nu_t - 1) + r = \lambda \nu_t + r - \lambda, & s = t \end{cases}$$

□

Iz svega navedenog slijedi tvrdnja sljedeće propozicije.

Propozicija 3.4. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn, $G \leq \text{Aut}(\mathcal{D})$ te neka su $a_{i,j}$, $b_{i,j}$, ν_i i β_j definirani kao ranije. Vrijede sljedeće jednakosti:*

$$1) \sum_{j=1}^n a_{i,j} = r,$$

3.1 Metoda taktičke dekompozicije i orbitne matrice

$$2) \sum_{j=1}^n \frac{\nu_t}{\beta_j} a_{s,j} a_{t,j} = \lambda \nu_t + \delta_{st}(r - \lambda).$$

Na temelju svega navedenog definiramo točkovnu i blokovnu orbitnu matricu, pri čemu pretpostavljamo da su parametri v, b, r, k, λ dopustivi.

Definicija 3.3. Točkovna orbitna matrica za parametre (v, k, λ) i distribuciju duljina orbita točaka $\nu = (\nu_1, \dots, \nu_m)$, odnosno blokova $\beta = (\beta_1, \dots, \beta_n)$ je svaka $m \times n$ matrica $A = [a_{i,j}]$ s elementima iz \mathbb{N}_0 za koju vrijedi:

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

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

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

$$4) \sum_{j=1}^n \frac{\nu_t}{\beta_j} a_{s,j} a_{t,j} = \begin{cases} \lambda \nu_t, & s \neq t, \\ \lambda(\nu_t - 1) + r, & s = t. \end{cases}$$

Pritom vrijedi $\sum_{i=1}^m \nu_i = v$, $\sum_{j=1}^n \beta_j = b$, $r = \frac{v-1}{k-1} \lambda$ i $b = \frac{vr}{k}$.

Definicija 3.4. Parcijalna točkovna orbitna matrica je $l \times n$ matrica $A(l) = [a_{i,j}]$, za $1 \leq l \leq m$ s elementima iz \mathbb{N}_0 , koja ima svojstva 1, 2 i 4 iz definicije 3.3 i sljedeće svojstvo

$$3') \sum_{i=1}^l \frac{\nu_i}{\beta_j} a_{i,j} \leq k, \quad 1 \leq j \leq n.$$

Definicija 3.5. Blokovna orbitna matrica za parametre (v, k, λ) i distribuciju duljina orbita točaka $\nu = (\nu_1, \dots, \nu_m)$, odnosno blokova $\beta = (\beta_1, \dots, \beta_n)$ je svaka $m \times n$ matrica $B = [b_{i,j}]$ s elementima iz \mathbb{N}_0 koja zadovoljava:

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

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

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

$$4) \sum_{j=1}^n \frac{\beta_j}{\nu_s} b_{s,j} b_{t,j} = \begin{cases} \lambda \nu_t, & s \neq t, \\ \lambda(\nu_t - 1) + r, & s = t. \end{cases}$$

Pritom vrijedi $\sum_{i=1}^m \nu_i = v$, $\sum_{j=1}^n \beta_j = b$, $r = \frac{v-1}{k-1} \lambda$ i $b = \frac{vr}{k}$.

Orbitne matrice jednoznačno su određene do poretka redaka i stupaca.

U ovom radu, za konstrukciju blokovnih dizajna koristimo isključivo točkovne orbitne matrice.

Za simetrične dizajne vrijedi da su svaka dva bloka incidentna sa λ zajedničkih točaka, prema tvrdnji teorema 2.5. Stoga, slijedi tvrdnja sljedeće propozicije.

Propozicija 3.5. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ simetričan blokovni dizajn, $G \leq \text{Aut}(\mathcal{D})$ te neka su $a_{i,j}$, $b_{i,j}$, ν_i i β_j definirani kao ranije. Za elemente točkovne orbitne matrice $A = [a_{i,j}]$ dizajna \mathcal{D} na koji djeluje grupa G vrijede sljedeće jednakosti:*

$$1) \sum_{j=1}^n a_{i,j} = r,$$

$$2) \sum_{i=1}^m \frac{\nu_i}{\beta_s} a_{i,s} a_{i,t} = \lambda \beta_t + \delta_{st}(r - \lambda).$$

Dokaz. 2) Neka je $x_s \in \mathcal{B}_s$. Prebrojavanjem na dva načina elementa skupa $\{(Q, x) \in \mathcal{P} \times \mathcal{B}_t \mid Q \in \langle x \rangle \cap \langle x_s \rangle\}$ dobivamo

$$\sum_{i=1}^m b_{i,s} a_{i,t} = \sum_{x \in \mathcal{B}_t} |\langle x_s \rangle \cap \langle x \rangle|.$$

Vrijedi

$$\sum_{i=1}^m b_{i,s} a_{i,t} = \sum_{x \in \mathcal{B}_t} |\langle x_s \rangle \cap \langle x \rangle| = \begin{cases} \lambda \beta_t, & s \neq t \\ \lambda(\beta_t - 1) + r = \lambda \beta_t + r - \lambda, & s = t. \end{cases}$$

Iz tvrdnje 1) u lemi 3.1 slijedi jednakost. □

Za blokovni dizajn \mathcal{D} i $\rho \in \text{Aut}(\mathcal{D})$ označimo sa \mathcal{F}_p , odnosno sa \mathcal{F}_b , skup ρ -fiksnihi točaka, odnosno ρ -fiksnihi blokova. Neka je A točkovna orbitna matrica dizajna \mathcal{D} na koji djeluje $\langle \rho \rangle$. Skup redaka od A koji se odnosi na ρ -fiksne točke sadržane u i fiksnih blokova označimo sa N_i , te skup redaka koji se odnosi na ρ -nefiksne točke sadržane u j fiksnih blokova označimo sa M_j . Označimo sa $n_i = |N_i|$, $m_j = |M_j|$, $F_p = |\mathcal{F}_p|$ i $F_b = |\mathcal{F}_b|$. Isto tako, skup stupaca od A koji se odnosi na ρ -fiksne blokove koji sadrže g fiksnih točaka označimo sa N'_g , te skup stupaca koji se odnosi na ρ -nefiksne blokove koji sadrže h fiksnih točaka označimo sa M'_h , te neka je $n'_g = |N'_g|$ i $m'_h = |M'_h|$. Za uvedene parametre vrijede svojstva iz sljedeće leme ([42]).

Lema 3.2. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ 2 -(v, k, λ) dizajn, $\rho \in \text{Aut}(\mathcal{D})$, $|\rho| = p$, gdje je p prost broj. Neka su $F_p, F_b, n_i, n'_g, m_j, m'_h$ definirani kao ranije. Tada vrijede sljedeća svojstva*

$$\sum_i n_i = F_p, \quad p \sum_j m_j = v - F_p, \tag{3.1}$$

$$\sum_g n'_g = F_b, \quad p \sum_h m'_h = b - F_b, \quad (3.2)$$

$$\sum_i in_i + p \sum_j jm_j = F_b k, \quad (3.3)$$

$$\sum_g gn'_g + p \sum_h hm'_h = F_p r, \quad (3.4)$$

$$\sum_g \binom{g}{2} n'_g + p \sum_h \binom{h}{2} m'_h = \binom{F_p}{2} \lambda. \quad (3.5)$$

Ako je \mathcal{D} simetričan dizajn, tada vrijedi i

$$\sum_i \binom{i}{2} n_i + p \sum_j \binom{j}{2} m_j = \binom{F_b}{2} \lambda. \quad (3.6)$$

Dokaz. Jednakosti (3.1) se odnose na broj ρ -fiksnih, odnosno ρ -nefiksnih točaka, dok se jednakosti (3.2) odnose na broj ρ -fiksnih, odnosno ρ -nefiksnih blokova.

Tražena jednakost (3.3) dobije se prebrojavanjem na dva načina elemenata skupa $\{(P, x) \mid P \in \mathcal{P}, x \in \mathcal{F}_b, (P, x) \in \mathcal{I}\}$. Na analogan način može se pokazati da vrijedi jednakost (3.4) za skupove N'_g, M'_h i njihove kardinalne brojeve.

Tražena jednakost (3.5) dobije se prebrojavanjem na dva načina elemenata skupa $\{P, Q, x\}$, pri čemu su $P, Q \in \mathcal{F}_p, P \neq Q, x \in \mathcal{B}$, te $(P, x), (Q, x) \in \mathcal{I}$. Za simetričan dizajn na analogan način može se pokazati da vrijedi jednakost (3.6). \square

Pokazalo se da primjena rezultata iz prethodne leme u programu za konstrukciju točkovnih orbitnih matrica blokovnih dizajna, u slučaju kada pretpostavimo djelovanje grupe automorfizama prostog reda na dizajn, znatno smanjuje broj konstruiranih izomorfnih parcijalnih orbitnih matrica i time znatno skraćuje vrijeme potrebno za izvođenje programa.

Prema definiciji blokovnog dizajna \mathcal{D} , za točke $P, Q \in \mathcal{P}$ vrijedi $P \neq Q$ ako i samo ako $\langle P \rangle \neq \langle Q \rangle$, stoga možemo identificirati točke sa skupom blokova koji sadrže tu točku. Označimo elemente G -orbite blokova $\mathcal{B}_j = G.x_j$ blokovnog dizajna \mathcal{D} sa $x_j = x_{j_0}, x_{j_1}, \dots, x_{j_{\beta_j-1}}$ ili kraće $j_0, j_1, \dots, j_{\beta_j-1}$. Svaka permutacija $g \in G \leq \text{Aut}(\mathcal{D})$ inducira permutaciju skupa blokova G -orbite \mathcal{B}_j koju možemo promatrati kao permutaciju skupa indeksa $\{0, 1, \dots, \beta_j - 1\}$.

Definiramo poredak u skupu blokovnih dizajna na koji zadana grupa automorfizama djeluje s istom točkovnom orbitnom matricom, na isti način kako je to definirao V. Čepulić u radu [21]. Najprije uvodimo pojam kanonskog oblika za točke i dizajne.

Definicija 3.6. Neka je zadan poredak u skupu orbita blokova $\mathcal{B}_1, \dots, \mathcal{B}_n$. Za točku $P \in \mathcal{P}$ vrijedi

$$\langle P \rangle = \bigsqcup_{j=1}^n (\langle P \rangle \cap \mathcal{B}_j).$$

Tada postoji jedinstveni niz blokova \tilde{P} duljine r za koji vrijedi

1. $\tilde{P}(j) \in \langle P \rangle$, $1 \leq j \leq r$, $\tilde{P}(s) \neq \tilde{P}(t)$ za $s \neq t$, $1 \leq s, t \leq r$,
2. ako je $\tilde{P}(i) \in \mathcal{B}_s$, $\tilde{P}(j) \in \mathcal{B}_t$, $s < t$, onda je $i < j$,
3. ako su $\tilde{P}(i), \tilde{P}(j) \in \mathcal{B}_s$, $\tilde{P}(i) = x_{sa}$, $\tilde{P}(j) = x_{sb}$, $a < b$, tada je $i < j$.

Niz \tilde{P} nazivamo kanonski oblik točke P .

S obzirom da je točka P jednoznačno određena nizom \tilde{P} , možemo ih poistovjetiti.

Definicija 3.7. Ako za točke $P, Q \in \mathcal{P}$ vrijedi $|\langle P \rangle \cap \mathcal{B}_j| = |\langle Q \rangle \cap \mathcal{B}_j|$, za sve $j \in \{1, \dots, n\}$, kažemo da točke P i Q imaju jednake orbitne strukture.

Definicija 3.8. Neka su P i Q točke koje imaju jednake orbitne strukture i neka su \tilde{P} i \tilde{Q} njihovi kanonski oblici. Kažemo da \tilde{P} kanonski strogo prethodi \tilde{Q} ako postoji j , $1 \leq j \leq r$, takav da vrijedi

1. $\tilde{P}(i) = \tilde{Q}(i)$, $i < j$,
2. $\tilde{P}(j) = x_{sa}$, $\tilde{Q}(j) = x_{sb}$, $1 \leq s \leq n$, $a < b$.

Definicija 3.9. Neka je zadan poredak u skupu G -orbita točaka i blokova dizajna \mathcal{D} . Niz $\tilde{\mathcal{D}}$ koji se sastoji od m točaka u kanonskom obliku $\tilde{\mathcal{D}}(i)$ za koji vrijedi:

1. $\tilde{\mathcal{D}}(i) \in \mathcal{P}_i$, $1 \leq i \leq m$,
2. $\tilde{\mathcal{D}}(i)$ kanonski strogo prethodi ostalim točkama iz \mathcal{P}_i ,

nazivamo kanonski oblik dizajna \mathcal{D} s obzirom na grupu G i skupove $\{\mathcal{P}_1, \dots, \mathcal{P}_m\}$ i $\{\mathcal{B}_1, \dots, \mathcal{B}_n\}$. Takav niz je jedinstven.

S obzirom da je $\mathcal{P}_i = G \cdot \tilde{\mathcal{D}}(i)$, dizajn \mathcal{D} poistovjećujemo s nizom $\tilde{\mathcal{D}}$.

Neka su \mathcal{D}_1 i \mathcal{D}_2 dizajni s parametrima $2-(v, k, \lambda)$. Ako vrijedi da $\tilde{\mathcal{D}}_1(i)$ i $\tilde{\mathcal{D}}_2(i)$ imaju jednake orbitne strukture za sve $1 \leq i \leq m$, tada kažemo da dizajni \mathcal{D}_1 i \mathcal{D}_2 imaju jednake orbitne matrice.

Definicija 3.10. Neka su \mathcal{D}_1 i \mathcal{D}_2 dizajni s parametrima $2-(v, k, \lambda)$ koji imaju jednake orbitne matrice. Dizajn \mathcal{D}_1 kanonski strogo prethodi dizajnu \mathcal{D}_2 ako postoji j , $1 \leq j \leq m$ za koji vrijedi

1. $\tilde{\mathcal{D}}_1(i) = \tilde{\mathcal{D}}_2(i)$, $i < j$,
2. $\tilde{\mathcal{D}}_1(j)$ kanonski strogo prethodi $\tilde{\mathcal{D}}_2(j)$.

3.1 Metoda taktičke dekompozicije i orbitne matrice

Točkovne orbitne matrice koristimo za konstrukciju blokovnih dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ na koje djeluje grupa $G \leq \text{Aut}(\mathcal{D})$.

Konstrukcija blokovnih dizajna na koje djeluje odgovarajuća grupa automorfizama sastoji se od dva osnovna koraka ([32]):

1. konstrukcije orbitnih matrica blokovnih dizajna za djelovanje zadane grupe,
2. konstrukcije blokovnih dizajna za dobivene orbitne matrice iz prethodnog koraka, odnosno indeksiranja orbitnih matrica.

Prije konstrukcije orbitnih matrica, potrebno je provjeriti jesu li parametri blokovnog dizajna v, k i λ dopustivi. Zatim, osim strukture grupe G moramo znati na koji način ona djeluje na skupu točaka i blokova dizajna \mathcal{D} . Potrebno je odrediti sve distribucije duljina G -orbita točaka $\nu = (\nu_1, \dots, \nu_m)$ i blokova $\beta = (\beta_1, \dots, \beta_n)$ dizajna \mathcal{D} za koje vrijedi

$$\sum_{i=1}^m \nu_i = v, \quad \sum_{j=1}^n \beta_j = b,$$

gdje su $m, n \in \mathbb{N}$. Duljina G -orbite jednaka je indeksu neke podgrupe u grupi G , prema tvrdnji korolara 1.1. Osim toga, pri određivanju distribucija duljina G -orbita točaka i blokova, važnu ulogu može imati poznavanje fiksnih struktura podgrupa grupe G .

Također, prije konstrukcije orbitnih matrica potrebno je odrediti vektor $\kappa\nu$, odnosno vektor $\kappa\beta$, s informacijom o konjugiranosti stabilizatora predstavnika G -orbita točaka, odnosno G -orbita blokova. Neka za vektor $\kappa\nu = (\kappa\nu_1, \dots, \kappa\nu_m)$ vrijedi da je $\kappa\nu_i = \kappa\nu_j$ ako i samo ako predstavnici G -orbita točaka \mathcal{P}_i i \mathcal{P}_j imaju konjugirane stabilizatore, gdje je $|\mathcal{P}_i| = \nu_i$ i $|\mathcal{P}_j| = \nu_j$ za $1 \leq i, j \leq m$. Analogno definiramo vektor $\kappa\beta$.

U nastavku navodimo objašnjenje potrebe za uvođenjem vektora $\kappa\nu$ i $\kappa\beta$.

Kako bi se smanjio broj konstruiranih izomorfnih blokovnih dizajna, koristimo elemente normalizatora grupe automorfizama koja djeluje na taj dizajn i time znatno ubrzavamo proces konstrukcije dizajna. Taj se postupak naziva eliminacija ili redukcija. Redukcija započinje konstrukcijom neizomorfnih (parcijalnih) točkovnih orbitnih matrica, a provodimo je na temelju tvrdnje sljedećeg teorema.

Teorem 3.2. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn, $G \leq \text{Aut}(\mathcal{D})$ i $m \times n$ točkovna orbitna matrica A dobivena djelovanjem grupe G na dizajn \mathcal{D} . Neka je $g = (\alpha, \beta) \in S = S_m \times S_n$ sa sljedećim svojstvima:*

1. ako $\alpha(s) = t$, tada je stabilizator $G_{\mathcal{P}_s}$ konjugat od $G_{\mathcal{P}_t}$, gdje su $\mathcal{P}_s, \mathcal{P}_t \in \mathcal{P}$, $\mathcal{P}_s = G \cdot \mathcal{P}_s$ i $\mathcal{P}_t = G \cdot \mathcal{P}_t$,
2. ako $\beta(i) = j$, tada je G_{x_i} konjugat od G_{x_j} , gdje su $x_i, x_j \in \mathcal{B}$, $\mathcal{B}_i = G \cdot x_i$ i $\mathcal{B}_j = G \cdot x_j$.

Tada postoji $g^* \in C_{S(\mathcal{P}) \times S(\mathcal{B})}(G)$ takav da

$$\begin{aligned}\alpha(s) = t & \text{ ako i samo ako vrijedi } g^*(\mathcal{P}_s) = \mathcal{P}_t \text{ i} \\ \beta(i) = j & \text{ ako i samo ako vrijedi } g^*(\mathcal{B}_i) = \mathcal{B}_j.\end{aligned}$$

Dokaz. Ako su α i β identitete, onda je i g^* identiteta. Permutacije α i β koje nisu identitete možemo zapisati $\alpha = \alpha_1 \dots \alpha_{m_1}$, $\beta = \beta_1 \dots \beta_{n_1}$, $m_1, n_1 \in \mathbb{N}$, pri čemu su $\alpha_1, \dots, \alpha_{m_1}, \beta_1, \dots, \beta_{n_1}$ transpozicije. Iz korolara 1.2 slijedi da za svaki α_k , $1 \leq k \leq m_1$, postoji $\alpha_k^* \in C_{S(\mathcal{P})}(G)$, pri čemu vrijedi

$$\alpha_k(s) = t \Leftrightarrow \alpha_k^*(\mathcal{P}_s) = \mathcal{P}_t, \quad 1 \leq k \leq m_1.$$

Nadalje, za svaku permutaciju β_l , $1 \leq l \leq n_1$, postoji $\beta_l^* \in C_{S(\mathcal{B})}(G)$, pri čemu vrijedi

$$\beta_l(i) = j \Leftrightarrow \beta_l^*(\mathcal{B}_i) = \mathcal{B}_j, \quad 1 \leq l \leq n_1.$$

Ako definiramo preslikavanja α^* i β^* na sljedeći način

$$\alpha^* = \alpha_1^* \dots \alpha_{m_1}^*, \quad \beta^* = \beta_1^* \dots \beta_{n_1}^*,$$

tada preslikavanje $g^* = (\alpha^*, \beta^*)$ ima traženo svojstvo. □

Definicija 3.11. Neka je $\Delta = [\delta_{i,j}]$ $m \times n$ matrica i $g = (\alpha, \beta) \in S_m \times S_n$. Matrica $\Delta' = g \cdot \Delta = [\delta'_{i,j}]$ je $m \times n$ matrica, gdje je $\delta'_{\alpha(i), \beta(j)} = \delta_{i,j}$. Za g kažemo da je izomorfizam sa Δ na Δ' , dok za pripadne matrice kažemo da su izomorfne. Ako je $g \cdot \Delta = \Delta$, g se naziva automorfizam matrice Δ . Svi automorfizmi matrice Δ čine punu grupu automorfizama od Δ , u oznaci $Aut(\Delta)$.

Na temelju teorema 3.2, definiramo točkovne orbitne matrice za djelovanje grupe na dizajn na sljedeći način.

Definicija 3.12. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn, $G \leq Aut(\mathcal{D})$, te $\nu = (\nu_1, \dots, \nu_m)$ i $\beta = (\beta_1, \dots, \beta_n)$ distribucije duljina G -orbita točaka i blokova, gdje su $m, n \in \mathbb{N}$. Za $m \times n$ točkovnu orbitnu matricu $A = [a_{i,j}]$ sa svojstvima iz definicije 3.3 kažemo da je orbitna matrica za djelovanje grupe G na dizajn \mathcal{D} ako su određeni vektori s informacijom o konjugiranosti stabilizatora predstavnika G -orbita točaka $\kappa\nu = (\kappa\nu_1, \dots, \kappa\nu_m)$ i G -orbita blokova $\kappa\beta = (\kappa\beta_1, \dots, \kappa\beta_n)$.

Izomorfizam orbitnih matrica iz definicije 3.12 definiramo na sljedeći način.

Definicija 3.13. Neka su A i B dvije $m \times n$ točkovne orbitne matrice 2 - (ν, k, λ) dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ na koji djeluje grupa $G \leq Aut(\mathcal{D})$. Neka su ν_s i β_i duljine G -orbite točaka

3.2 Algoritam za konstrukciju orbitnih matrica

\mathcal{P}_s i orbite blokova \mathcal{B}_i za $1 \leq s \leq m$, $1 \leq i \leq n$.

Za preslikavanje $g = (\alpha, \beta) \in S_m \times S_n$ kažemo da je izomorfizam orbitnih matrica A i B ako vrijede sljedeća svojstva:

1. g je izomorfizam tih matrica,
2. ako je $\alpha(s) = t$, tada je G_{P_s} konjugat od G_{P_t} , gdje su $\mathcal{P}_s = G.P_s$ i $\mathcal{P}_t = G.P_t$,
3. ako je $\beta(i) = j$, tada je G_{x_i} konjugat od G_{x_j} , gdje su $\mathcal{B}_i = G.x_i$, $\mathcal{B}_j = G.x_j$.

U tom slučaju kažemo da su orbitne matrice A i B izomorfne. Ako vrijedi $A = B$ tada za preslikavanje g kažemo da je automorfizam orbitne matrice A . Svi automorfizmi orbitne matrice A čine punu grupu automorfizama od A , u oznaci $Aut(A)$.

U drugom koraku konstrukcije blokovnih dizajna provodi se postupak indeksiranja za svaku konstruiranu točkovnu orbitnu matricu ([32]). Tim postupkom konstruiraju se matrice incidencije svih dizajna na koje djeluje odgovarajuća grupa automorfizama G , ako takvi postoje. Prilikom indeksiranja identificiraju se blokovi iz orbite \mathcal{B}_j koji su incidentni s pojedinim točkama iz orbite \mathcal{P}_i , gdje su $1 \leq i \leq m$ i $1 \leq j \leq n$, za $m, n \in \mathbb{N}$. Dovoljno je odrediti po jednu točku iz svake orbite točaka, odnosno predstavnika te orbite točaka. Preostalih $|\mathcal{P}_i| - 1$ točaka može se dobiti djelovanjem grupe G na predstavnika te G -orbite točaka.

Definicija 3.14. Indeksni skup za element $a_{i,j}$ točkovne orbitne matrice A je skup indeksa blokova orbite \mathcal{B}_j koji označavaju koji su blokovi iz te orbite incidentni s predstavnikom orbite točaka \mathcal{P}_i , gdje su $1 \leq i \leq m$ i $1 \leq j \leq n$, za $m, n \in \mathbb{N}$.

Zbog prevelikog broja mogućnosti, često se koriste računala i razvijaju algoritmi kako bi se provela oba spomenuta koraka konstrukcije.

3.2 Algoritam za konstrukciju orbitnih matrica

Prije konstrukcije 2 - (v, k, λ) dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ potrebno je provjeriti zadovoljavaju li parametri v, k, λ ranije navedene nužne uvjete za egzistenciju dizajna s tim parametrima. Zatim odabiremo grupu G za koju pretpostavljamo da može biti grupa automorfizama tog dizajna i određujemo sve moguće distribucije duljina G -orbita točaka $\nu = (\nu_1, \dots, \nu_m)$ i G -orbita blokova $\beta = (\beta_1, \dots, \beta_n)$ u nepadajućem poretku. Osim toga, G -orbite točaka (blokova) čiji predstavnici imaju konjugirane stabilizatore poredane su jedna do druge.

Primjenom programa napisanog na temelju razvijenog algoritma za konstrukciju orbitnih matrica konstruiraju se sve, do na izomorfizam, točkovne orbitne matrice dizajna \mathcal{D} na koji djeluje grupa automorfizama $G \leq S = S(\mathcal{P}) \times S(\mathcal{B})$.

Iz definicije 3.3, za retke $i = 1, \dots, m$ orbitne matrice $A = [a_{i,j}]$ vrijedi

1. $\sum_{j=1}^n a_{i,j} = r,$
2. $\sum_{j=1}^n \frac{\nu_i}{\beta_j} a_{i,j}^2 = \lambda \nu_i + r - \lambda.$

Nenegativna cjelobrojna rješenja tih dviju jednadžbi $(a_{i,j})_i$, pri čemu je vanjski indeks stalan, nazivamo točkovne orbitne strukture i -te orbite točaka. Za dvije točkovne orbitne strukture $(a'_{s,j})_s$ i $(a''_{t,j})_t$ kažemo da su istog tipa ako postoji $\alpha \in N_S(G)$ takav da je $\alpha \mathcal{P}_s = \mathcal{P}_t$ i $a'_{s,j} = a''_{t,\alpha j}$, pri čemu je $\alpha \mathcal{B}_j = \mathcal{B}_{\alpha j}$ za $j = 1, \dots, n$, pritom je $\mathcal{B}_{\alpha j}$ orbita blokova čiji je predstavnik blok $B_{\alpha j}$.

Definicija 3.15. Neka su $(a'_{s,j})_s$ i $(a''_{s,j})_s$ dvije točkovne orbitne strukture s -te orbite točaka koje su istog tipa. Ako postoji $i, 1 \leq i \leq n$ takav da je

1. $a'_{s,j} = a''_{s,j}, \quad j < i,$
2. $a'_{s,i} > a''_{s,i}$

tada kažemo da $(a'_{s,j})_s$ strogo prethodi $(a''_{s,j})_s$.

Za predstavnika tipa uzimamo orbitnu strukturu koja je prva s obzirom na uvedeni poredak. Poredak između tipova uvodimo kao poredak između njihovih predstavnika na istom principu kao i poredak točkovnih orbitnih struktura unutar tipa.

Kad odredimo sve tipove točkovnih orbitnih struktura, prelazimo na izgradnju parcijalnih točkovnih orbitnih matrica iz definicije 3.4, te, u konačnici orbitnih matrica iz definicije 3.3.

Definicija 3.16. Neka su $A'(j) = [a'_{s,i}]$ i $A''(j) = [a''_{s,i}]$ parcijalne točkovne orbitne matrice do j -tog retka, odnosno točkovne orbitne matrice ako je $j = m$. Ako postoji $l, l \leq j$ takav da je

1. $(a'_{s,i})_s = (a''_{s,i})_s, \quad s < l,$
2. tip od $(a'_{l,i})_l$ strogo prethodi tipu od $(a''_{l,i})_l$ ili su te točkovne orbitne strukture istog tipa ali $(a'_{l,i})_l$ strogo prethodi $(a''_{l,i})_l$ kao točkovna orbitna struktura,

tada kažemo da $A'(j)$ strogo prethodi $A''(j)$ i pišemo $A'(j) \prec A''(j)$.

Primjer 3.1. Neka su A i B parcijalne točkovne orbitne matrice za djelovanje odgovarajuće grupe automorfizama na neki blokovni dizajn, pri čemu je $\nu = (1, 1, 1, 2, 2, 2, 3, 3)$, $\beta = \nu$, uz pretpostavku da su stabilizatori predstavnika orbita točaka (blokova) istih duljina međusobno konjugirani. Retci matrice A odgovaraju orbitnim strukturama koje su istoga tipa, pri čemu prvi redak strogo prethodi drugome. Retci matrice B odgovaraju orbitnim strukturama koje nisu istoga tipa, pri čemu tip prvog retka strogo prethodi tipu drugog retka.

3.2 Algoritam za konstrukciju orbitnih matrica

A	1	1	1	2	2	2	3	3
1	1	0	1	2	0	1	1	0
1	1	0	1	1	2	0	0	1

B	1	1	1	2	2	2	3	3
1	0	1	1	0	2	2	1	1
1	0	1	1	1	2	0	1	1

Označimo sa $A^{(j)}$, $1 \leq j \leq m$ skup svih konstruiranih parcijalnih točkovnih orbitnih matrica do j -tog retka. Orbitne matrice konstruiramo na sljedeći način:

1. $A^{(1)}$ se sastoji od svih predstavnika tipova prve orbite točaka.
2. $A^{(j)}$ konstruiramo iz $A^{(j-1)}$ tako da svakoj konstruiranoj parcijalnoj orbitnoj matrici $A^{(j-1)}$ dodamo sve točkovne orbitne strukture j -te orbite točaka za koje je dobivena matrica $A^{(j)}$ parcijalna točkovna orbitna matrica. Matricu $A^{(j)}$ uključujemo u skup $A^{(j)}$ ako ne postoji $\alpha \in N_S(G)$ takva da je $\alpha.A^{(j)} \prec A^{(j)}$. Pri tome za $A^{(j)} = [a_{s,i}]$ i $\alpha \in N_S(G)$ vrijedi $\alpha.P_s = P_{\alpha s}$, $\alpha.B_i = B_{\alpha i}$, što inducira djelovanje od α na način da je $\alpha.A^{(j)} = [a'_{s,i}]$ gdje je $a'_{\alpha s, \alpha i} = a_{s,i}$. Na taj način za neku orbitnu matricu A eliminiramo dizajne koje bi konstruirali iz orbitne matrice $\alpha.A$, za $\alpha \in N_S(G)$. Ti su dizajni G -izomorfni s dizajnim konstruiranim iz A . Primjenom te eliminacije, u $A^{(j)}$ uključujemo samo one matrice koje su prve s obzirom na uvedeni poredak. Time se tijekom konstrukcije eliminiraju orbitne matrice koje se djelovanjem takvih permutacija mogu prevesti u matrice koje im prethode s obzirom na uvedeni poredak.
3. U skupu $A^{(m)}$ su sve orbitne matrice $2-(v, k, \lambda)$ dizajna \mathcal{D} za zadanu distribuciju duljina G -orbita točaka ν i blokova β , te vektore $\kappa\nu$ i $\kappa\beta$, koje nismo mogli eliminirati G -izomorfizmima.

Prilikom konstrukcije orbitnih matrica, za redukciju broja izomorfnih orbitnih matrica koristimo permutacije iz $S_m \times S_n$ koje imaju svojstva iz teorema 3.2, dok je prilikom profinjavanja orbitne matrice moguće upotrijebiti samo automorfizme te orbitne matrice.

Primjer 3.2. Poznato je da, do na izomorfizam, postoji 591 orbitnih matrica simetričnog $2-(45, 12, 3)$ dizajna na koji djeluje grupa automorfizama reda 3 ([20]). Na isti problem primijenili smo, u sklopu ovo rada, razvijeni program za konstrukciju točkovnih orbitnih matrica. Prema napomeni 2.8, grupa automorfizama prostog reda djeluje standardno na simetričnom dizajnu, stoga je dovoljno odrediti samo distribuciju duljina orbita točaka. Jasno je da će predstavnici orbita točaka, odnosno blokova, iste duljine imati konjugirane stabilizatore. Za broj fiksnih točaka F automorfizma reda 3 koji djeluje na dizajn \mathcal{D} , prema propoziciji 2.7 i napomeni 2.8, vrijedi $F \in \{0, 3, 6, 9, 12\}$.

Primjenom razvijenog programa za konstrukciju točkovnih orbitnih matrica dobiveni su podaci prikazani u tablici 3.1, čime je ponovljen rezultat iz [20].

# fiksnih točaka	0	3	6	9	12
# orbitnih matrica	293	245	49	4	0

Tablica 3.1: Broj orbitnih matrica 2-(45, 12, 3) dizajna za djelovanje grupe automorfizama reda 3

3.3 Profinjenje orbitnih matrica

Postupak indeksiranja orbitnih matrica često traje predugo zbog prevelikog broja mogućnosti za indeksne skupove koje računalni program treba ispitati. Stoga, kako bi se provelo indeksiranje, potrebno je napraviti odgovarajuće profinjenje (dekompoziciju) orbitne matrice, što je do sada napravljeno samo za specijalne slučajeve simetričnih dizajna i neke posebne grupe automorfizama, kao na primjer u [15], [17], [55], [56] i [57].

D. Crnković i S. Rukavina u [18] opisuju primjenu glavnog niza Abelove grupe u svrhu provedbe profinjenja orbitnih matrica blokovnih dizajna na koje djeluje takva grupa automorfizama. Iako je u tom članku opisan način konstrukcije blokovnih dizajna s Abelovim grupama automorfizama, računalni programi kojima se takva konstrukcija provodi u općenitom slučaju dosad nisu bili razvijeni.

U sklopu ovog rada razvijen je algoritam i u skladu s njim napisan program za profinjenje točkovnih orbitnih matrica blokovnih dizajna na koje djeluje rješiva grupa. Prednost ovog algoritma je njegova primjena za konstrukciju blokovnih dizajna na koje djeluje širi spektar grupa (rješive grupe) u usporedbi s konstrukcijom opisanom u [18], dok je nedostatak gubitak u brzini izvođenja algoritma. U ovom poglavlju ćemo opisati taj algoritam.

3.3.1 Profinjenje primjenom kompozicijskog niza rješive grupe

Prema tvrdnji teorema 1.8, za grupu $H \triangleleft G \leq \text{Aut}(\mathcal{D})$ svaka G -orbita točaka i blokova blokovnog dizajna \mathcal{D} profinjuje se na jednu ili više H -orbita iste duljine. Osim toga, kvocijentna grupa G/H djeluje kao tranzitivna grupa na skupu H -orbita točaka (blokova) dobivenih iz neke G -orbite točaka (blokova), prema tvrdnji teorema 1.9. Primjenom tih činjenica, orbitne matrice za djelovanje grupe G profinjuju se do orbitnih matrica za djelovanje normalne podgrupe H na dizajn \mathcal{D} .

Prema tvrdnji teorema 1.16, svaka konačna rješiva grupa G ima kompozicijski niz

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_n = G, \tag{3.7}$$

čiji su kompozicijski faktori cikličke grupe prostog reda, odnosno $H_{n-i+1}/H_{n-i} \cong Z_{p_{n-i+1}}$, gdje je p_{n-i+1} prost broj, $1 \leq i \leq n$, $n \in \mathbb{N}$.

Neka je \mathcal{S} skup neizomorfni točkovnih orbitnih matrica 2-(v, k, λ) dizajna \mathcal{D} na kojeg

3.3 Profinjenje orbitnih matrica

djeluje grupa $G \leq \text{Aut}(\mathcal{D})$, dobivenih primjenom razvijenog programa za konstrukciju orbitnih matrica blokovnih dizajna.

Nakon prve primjene programa za profinjenje orbitnih matrica, iz skupa \mathcal{S} konstruiraju se orbitne matrice dizajna \mathcal{D} za djelovanje normalne podgrupe $H_{n-1} \triangleleft G$ iz kompozicijskog niza (3.7), uz pretpostavku djelovanja kvocijentne grupe $G/H_{n-1} \cong Z_{p_n}$ na H_{n-1} -orbite.

Kako bi se provela eliminacija izomorfnih blokovnih dizajna za vrijeme profinjenja orbitnih matrica iz skupa \mathcal{S} , koristimo automorfizme tih matrica, odnosno permutacije redaka i stupaca tih matrica koje imaju svojstva iz definicije 3.13. Naime, prema tvrdnji teorema 3.2, svaki automorfizam orbitne matrice za neki blokovni dizajn \mathcal{D} na koji djeluje grupa $G \leq \text{Aut}(\mathcal{D})$ određuje po jedan element grupe $C_S(G)$, gdje je $S = S(\mathcal{P}) \times S(\mathcal{B})$. U sklopu ovog rada razvijen je program koji određuje sve automorfizme orbitne matrice na temelju pripadnih vektora $\kappa\nu$ i $\kappa\beta$ s informacijom o konjugiranosti stabilizatora orbita točaka i blokova.

Osim toga, za eliminaciju izomorfnih blokovnih dizajna koristimo izomorfizme (parcijalnih) točkovnih orbitnih matrica konstruiranih pomoću programa za profinjenje, koji se nalaze u normalizatoru grupe G/H_{n-1} u grupi S . To zapravo znači da se primjenjuju izomorfizmi tih orbitnih matrica, čime se eliminiraju one (parcijalne) orbitne matrice iz kojih će se konstruirati G -izomorfni dizajni, prema tvrdnji propozicije 2.3. Eliminiraju se one (parcijalne) orbitne matrice koje se djelovanjem spomenutih permutacija mogu prevesti u matrice koje im prethode s obzirom na uvedeni poredak.

Skup orbitnih matrica dizajna \mathcal{D} za djelovanje normalne podgrupe H_{n-1} , koje su konstruirane primjenom programa za profinjenje, označimo sa \mathcal{S}' .

Program za profinjenje moguće je ponovno primijeniti na konstruiranim orbitnim matricama iz skupa \mathcal{S}' , ako je grupa $H_{n-1} \neq \{1\}$, pri čemu više ne vodimo računa o djelovanju grupe $H_n = G$. Taj se postupak ponavlja za svaki element kompozicijskog niza, odnosno u i -tom koraku konstruiraju se točkovne orbitne matrice dizajna \mathcal{D} za djelovanje grupe H_{n-i} , gdje je $H_{n-i} \triangleleft H_{n-i+1} \leq \text{Aut}(\mathcal{D})$ uz pretpostavku djelovanja kvocijentne grupe $H_{n-i+1}/H_{n-i} \cong Z_{p_{n-i+1}}$ na H_{n-i} -orbite.

Kao zadnji, n -ti korak u profinjenju orbitnih matrica dizajna \mathcal{D} , provodi se indeksiranje, odnosno konstrukcija $v \times b$ matrica incidencije blokovnih dizajna iz dobivenih orbitnih matrica za djelovanje grupe $H_1 \leq \text{Aut}(\mathcal{D})$, $H_1 \cong Z_{p_1}$, iz kompozicijskog niza (3.7).

Napomena 3.1. Prije svake sljedeće primjene programa za profinjenje, potrebno je redefinirati vektore koji predstavljaju distribucije duljina orbita točaka ν i blokova β , te pripadne vektore $\kappa\nu$ i $\kappa\beta$. Osim toga, u slučaju kada postoje barem dva kompozicijska faktora iz niza (3.7) koji su istog prostog reda p , potrebno je definirati još dva 0-1 vektora koje označimo sa $\eta\nu$ i $\eta\beta$. U i -toj iteraciji primjene programa za profinjenje, u kojem se neke H_{n-i+1} -orbite profinjuju na nekoliko H_{n-i} -orbita, vektor $\eta\nu$ ima vrijednost 1 na pozicijama koje odgovaraju onim H_{n-i+1} -orbitama točaka za čije predstavnike vrijedi da

im je stabilizator podgrupa grupe H_{n-i} . Stoga, takve se H_{n-i+1} -orbite profinjaju u i -toj primjeni programa za profinjavanje, za neki $i \in \{1, \dots, n\}$. Analogno se za orbite blokova definira vektor $\eta\beta$.

Jasno je da se u nekoj i -toj iteraciji primjene programa za profinjavanje orbitnih matrica može se dogoditi da se za p_{n-i+1} prost broj takav da je $|H_{n-i+1}/H_{n-i}| = p_{n-i+1}$ radi profinjavanje samo nekih orbita iz skupa orbita točkaka (blokova) čija je duljina djeljiva sa p_{n-i+1} , pri čemu je $i \in \{1, \dots, n\}$.

Označimo sa A točkovnu orbitnu matricu dobivenu djelovanjem rješive grupe G na blokovni dizajn \mathcal{D} . Neka je u l -tom koraku primjene programa za profinjavanje konstruirana (parcijalna) točkovna orbitna matrica A_l dizajna \mathcal{D} dobivena profinjavanjem (parcijalne) točkovne orbitne matrice A_{l-1} . Označimo sa r neku H_{n-l+1} -orbitu točkaka (blokova) koja se profinjuje u l -tom koraku profinjavanja na p H_{n-l} -orbita koje označimo sa r_0, \dots, r_{p-1} , za p prost broj. Tih p H_{n-l} -orbita vezano je djelovanjem kvocijentne grupe $H_{n-l+1}/H_{n-l} \cong \langle \alpha \rangle \cong Z_p$ u polaznu orbitu r . Bez smanjenja općenitosti, to djelovanje definiramo na sljedeći način

$$\alpha(r_i) = r_j, \quad \text{gdje je } j \equiv (i+1)(\text{mod } p). \quad (3.8)$$

Za eliminaciju G -izomorfni dizajna u l -toj primjeni programa za profinjavanje koristimo G -izomorfizme σ_k , $1 \leq k \leq m$, za neki $m \in \mathbb{N}$, koji se nalaze u normalizatoru grupe $Z_p \cong H_{n-l+1}/H_{n-l}$ u simetričnoj grupi S_p , za p prost broj.

Ako pritom za neki $k \in \{1, \dots, m\}$ vrijedi da σ_k nije element centralizatora grupe $Z_p \cong H_{n-l+1}/H_{n-l}$ u S_p , onda σ_k mora djelovati na svim orbitama r_0, \dots, r_{p-1} koje su dobivene profinjavanjem neke orbite r , zbog očuvanja djelovanja kvocijentne grupe definiranog u (3.8). Za $\sigma_k \in C_{S_p}(Z_p)$ definiramo djelovanje

$$\sigma_k(s_i) = \begin{cases} s_i & s \neq r \\ s_{\sigma_k i}, & \text{inače} \end{cases}$$

za svaku orbitu r početne matrice koja se profinjuje u l -toj primjeni programa za profinjavanje, pri čemu $i \in \{0, \dots, p-1\}$.

Opisani način djelovanja permutacija σ_k , za $1 \leq k \leq m$, implementirali smo u program za profinjavanje orbitnih matrica, što zajedno s primjenom automorfizama tih matrica značajno doprinosi u eliminaciji G -izomorfni dizajna.

Nakon što opisanim postupkom konstruiramo blokovne dizajne, potrebno je još provjeriti jesu li neki od njih međusobno izomorfni, što činimo pomoću GAP paketa Design, ([59]). Osim toga, isti paket koristimo za određivanje strukture pune grupe automorfizama konstruiranih dizajna.

3.3.2 Klasifikacija 2-(45, 12, 3) dizajna s involutornim automorfizmom

U primjeru 3.2 konstruirane su sve orbitne matrice simetričnih 2-(45, 12, 3) dizajna s automorfizmom reda tri. Ovdje najprije konstruiramo orbitne matrice 2-(45, 12, 3) dizajna uz pretpostavku djelovanja grupe automorfizama reda dva, a potom, primjenom programa za profinjenje, provodimo indeksiranje dobivenih orbitnih matrica.

Teorem 3.3. *Do na izomorfizam, postoje 682 orbitne matrice za djelovanje involutornog automorfizma na 2-(45, 12, 3) dizajn.*

Dokaz. Prema napomeni 2.8, grupa automorfizama prostog reda djeluje standardno na simetričnom dizajnu, stoga je dovoljno odrediti samo distribuciju duljina orbita točaka. Jasno je da će predstavnici orbita istih duljina imati konjugirane stabilizatore.

Za broj fiksnih točaka F involutornog automorfizma koji djeluje na simetrični 2-(45, 12, 3) dizajn \mathcal{D} vrijedi $5 \leq F \leq 15$, $F \equiv 1 \pmod{2}$, odnosno $F \in \{5, 7, 9, 11, 13, 15\}$, prema propoziciji 2.7, napomeni 2.8 i propoziciji 2.9.

Primjenom programa za konstrukciju točkovnih orbitnih matrica dobiju se 682 orbitne matrice dizajna \mathcal{D} s involutornim automorfizmom, što je prikazano u tablici 3.2.

# fiksnih točaka	5	7	9	11	13	15
# orbitnih matrica	233	397	32	4	11	5

Tablica 3.2: Broj orbitnih matrica 2-(45, 12, 3) dizajna za djelovanje involutornog automorfizma

Indeksiranje je provedeno programom za profinjenje koji se temelji na algoritmu opisanom u poglavlju 3.3.1, a rezultati su prikazani u tablici 3.3. □

# fiksnih točaka	5	7	9	11	13	15
# dizajna	603	1898	524	0	225	28

Tablica 3.3: 2-(45,12,3) dizajni na koje djeluje involutorni automorfizam

Nakon dodatne eliminacije izomorfni dizajna pomoću paketa Design, dobiveno je 2987 neizomorfni dizajna. Time je dokazana tvrdnja sljedećeg teorema.

Teorem 3.4. *Do na izomorfizam, postoji 2987 simetričnih 2-(45, 12, 3) dizajna na koji djeluje involutorni automorfizam.*

Podaci o konstruiranim dizajnima iz prethodnog teorema prikazani su u tablici 3.4.

$ \text{Aut}(D) $	Struktura grupe $\text{Aut}(D)$	# dizajna	$ \text{Aut}(D) $	Struktura grupe $\text{Aut}(D)$	# dizajna
51840	$PSp(4, 3) : Z_2$	1	48	$(Z_3 \times Q_8) : Z_2$	3
19440	$(E_{81} : SL(2, 5)) : Z_2$	1	48	$(Z_4 \times Z_4) : Z_3$	1
1296	$E_{27} : (S_4 \times Z_2)$	1	48	$Z_2 \times S_4$	1
486	$E_{81} : Z_6$	1	36	$S_3 \times S_3$	4
486	$E_{81} : S_3$	1	36	$E_9 : Z_4$	1
432	$((S_3 \times S_3) : Z_2) \times S_3$	2	36	$Z_2 \times (E_9 : Z_2)$	1
360	$(Z_{15} \times Z_3) : Z_8$	1	32	$Z_4 : Q_8$	1
324	$(E_{27} : Z_3) : E_4$	1	30	$Z_5 \times S_3$	1
324	$(E_{27} : Z_3) : E_4$	1	24	$Z_3 \times Q_8$	1
216	$(Z_3 \times S_3 \times S_3) : Z_2$	3	20	$Z_5 : Z_4$	1
216	$(E_9 : Z_4) \times S_3$	2	20	$Z_5 : Z_4$	1
216	$S_3 \times S_3 \times S_3$	2	18	$Z_3 \times S_3$	87
192	$(E_4 \times Q_8) : S_3$	2	18	$Z_6 \times Z_3$	4
162	$E_{27} : Z_6$	8	18	$E_9 : Z_2$	4
162	$E_{27} : S_3$	5	16	QD_{16}	7
162	$E_{27} : S_3$	1	16	$Z_2 \times D_8$	2
162	$S_3 \times (E_9 : Z_3)$	1	16	$(Z_4 \times Z_2) : Z_2$	1
144	$(E_9 : Z_8) : Z_2$	2	12	D_{12}	65
108	$S_3 \times (E_9 : Z_2)$	4	8	D_8	12
108	$E_{27} : Z_4$	2	8	Q_8	7
108	$E_{27} : E_4$	1	8	Z_8	4
108	$Z_3 \times S_3 \times S_3$	1	8	E_8	2
64	$(E_4.(Z_4 \times Z_2)) : Z_2$	1	8	$Z_4 \times Z_2$	2
64	$((Z_2 \times Q_8) : Z_2) : Z_2$	1	6	S_3	446
54	$E_{27} : Z_2$	24	6	Z_6	104
54	$E_{27} : Z_2$	9	4	E_4	128
54	$(Z_9 : Z_3) : Z_2$	6	4	Z_4	71
54	$E_9 \times S_3$	6	2	Z_2	1931
54	$E_9 : Z_6$	3			

Tablica 3.4: 2-(45,12,3) dizajni na koje djeluje involutorni automorfizam

Poglavlje 4

Klasifikacija $2-(45, 5, 1)$ dizajna s automorfizmom reda šest

Zanimljivu klasu blokovnih dizajna čine $2-(v, k, 1)$ dizajni, odnosno Steinerovi 2-dizajni koje obično zapisujemo u obliku $S(2, k, v)$. H. Hanani je 1975. u radu [27] dokazao da je $v \equiv 1, 5 \pmod{20}$ nužan i dovoljan uvjet za egzistenciju $S(2, 5, v)$ dizajna. Prema tablici I.1.28 u [12], postoje barem 16 dizajna (do na izomorfizam) s parametrima $2-(45, 5, 1)$ i poznato je da se dizajn s takvim parametrima može konstruirati pomoću diferencijske familije nad grupom $Z_3^2 \times Z_5$. C. J. Colbourn je 1998. godine prikazao konstrukciju $2-(45, 5, 1)$ dizajna s automorfizmom reda dva koji fiksira maksimalan broj točaka ([11]). Redovi punih grupa automorfizama dizajna dobivenih takvom konstrukcijom su dva i osam. V. Krčadinac u svojoj doktorskoj disertaciji [37] radi klasifikaciju $2-(45, 5, 1)$ dizajna na koje djeluje automorfizam reda pet i konstruira tri dizajna s redom pune grupe automorfizama 40, 160 i 360.

U ovom poglavlju određene su sve moguće distribucije duljina orbita točaka i blokova za djelovanje automorfizma reda šest na $2-(45, 5, 1)$ dizajn. Konstruirane su sve, do na izomorfizam, orbitne matrice za dobivene distribucije uz primjenu programa za konstrukciju orbitnih matrica blokovnog dizajna. Napravljena je klasifikacija $2-(45, 5, 1)$ dizajna uz pretpostavku djelovanja automorfizma reda šest. Postoje točno tri, do na izomorfizam, $2-(45, 5, 1)$ dizajna na koje djeluje automorfizam reda šest, a red njihove pune grupe automorfizama je 24. Pretpostavljamo da ti dizajni nisu poznati od ranije.

Niti jedan $2-(45, 5, 1)$ dizajn konstruiran u sklopu ove disertacije nije rastavljiv, što je provjereno pomoću paketa Design ([59]). Postojanje rastavljivih $2-(45, 5, 1)$ dizajna još je uvijek otvoreno pitanje.

4.1 Djelovanje automorfizma reda šest na 2-(45, 5, 1) dizajn

U prvom koraku konstrukcije 2-(45, 5, 1) dizajna potrebno je odrediti sve moguće distribucije duljina orbita točaka i blokova tog dizajna uz pretpostavku djelovanja automorfizma reda šest.

Označimo sa \mathcal{D} 2-(45, 5, 1) dizajn, te sa $G = \langle \alpha \mid \alpha^6 = 1 \rangle \cong Z_6 \cong Z_2 \times Z_3$ grupu automorfizama tog dizajna.

Promotrimo najprije djelovanje involutornog automorfizma na dizajn \mathcal{D} .

Lema 4.1. *Svaka fiksna točka involutornog automorfizma 2-(45, 5, 1) dizajna \mathcal{D} je sadržana u neparnom broju fiksnih blokova.*

Dokaz. Involutorni automorfizam fiksira barem jednu točku (blok) dizajna \mathcal{D} . Stupanj svake točke dizajna \mathcal{D} je neparan broj, odnosno iznosi $r = \frac{v-1}{k-1}\lambda = 11$. Svaka fiksna točka je sadržana u parnom broju nefiksnih blokova. Stoga, svaka fiksna točka je incidentna s neparnim brojem fiksnih blokova. \square

Lema 4.2. *Niti jedna nefiksna točka involutornog automorfizma 2-(45, 5, 1) dizajna \mathcal{D} nije sadržana u oba bloka iz neke orbite blokova duljine dva. Osim toga, niti jedan nefiksni blok ne sadrži obje točke iz neke orbite točaka duljine dva.*

Dokaz. Za djelovanje involutornog automorfizma na dizajn \mathcal{D} postoje barem dvije nefiksne točke i barem dva nefiksna bloka. Ako za točku P iz neke orbite točaka i duljine dva, $i \in \{1, \dots, m\}$, vrijedi da je sadržana u oba bloka iz neke orbite blokova j duljine dva, $j \in \{1, \dots, n\}$, tada je i preostala točka P' iz orbite točaka i sadržana u oba bloka iz orbite blokova j , što znači da postoje dvije točke P i P' koje su sadržane u dva bloka, što je nemoguće jer $\lambda = 1$. Tvrdnja za blokove direktna je posljedica tvrdnje leme 2.1. \square

Korolar 4.1. *Ako na 2-(45, 5, 1) dizajn \mathcal{D} djeluje involutorni automorfizam, tada su točke iz iste orbite točaka duljine dva sadržane u jedinstvenom fiksnom bloku.*

Dokaz. Involutorni automorfizam fiksira barem jedan blok i ne fiksira barem dvije točke 2-(45, 5, 1) dizajna \mathcal{D} . Dio orbitne matrice dizajna \mathcal{D} za djelovanje involutornog automorfizma koji se odnosi na orbite točaka i blokova duljine dva može sadržavati samo vrijednosti 0 ili 1, prema lemi 4.2. Stoga, točke iz orbite točaka duljine dva ne mogu biti sadržane u jedinstvenom nefiksnom bloku. \square

Promotrimo dalje fiksnu strukturu za djelovanje involutornog automorfizma na 2-(45, 5, 1) dizajn \mathcal{D} .

Propozicija 4.1. *Involutori automorfizam 2-(45, 5, 1) dizajna \mathcal{D} fiksira jedan od sljedećih skupova točaka i blokova:*

- (a) *Jednu točku i 11 blokova incidentnih s njom.*
- (b) *Tri točke bloka i još 10 blokova koji sadrže neke od fiksnih točaka. Mogući rasporedi tih 10 blokova: $10+0+0$, $8+2+0$, $6+4+0$, $6+2+2$, $4+4+2$, pri čemu $a_1+a_2+a_3$ znači da je a_i fiksnih blokova incidentno s i -tom fiksnom točkom, $1 \leq i \leq 3$.*
- (c) *Pet točaka bloka i još 10 blokova koji sadrže neke od fiksnih točaka. Mogući rasporedi tih 10 blokova: $10+0+0+0+0$, $8+2+0+0+0$, $6+4+0+0+0$, $6+2+2+0+0$, $4+4+2+0+0$, $4+2+2+2+0$, $2+2+2+2+2$.*
- (d) *Sedam točaka i sedam blokova koji čine projektivnu ravninu reda dva, te još šest blokova koji sadrže neke od fiksnih točaka. Mogući rasporedi tih blokova: $6+0+0+0+0+0+0$, $4+2+0+0+0+0+0$, $2+2+2+0+0+0+0$.*
- (e) *Linearni prostor s 13 točaka, 19 blokova, od kojih su tri bloka incidentna s pet točaka, a preostalih 16 s tri točke.*

Fiksne strukture od (a) do (d) prikazane su na slici 4.1, dok je linearni prostor u slučaju fiksne strukture (e) prikazan pomoću matrice incidencije u dokazu koji slijedi.

Dokaz. Koristimo oznake F_2 i f_2 redom za broj fiksnih točaka i fiksnih blokova involutornog automorfizma dizajna \mathcal{D} . Broj orbita točaka i orbita blokova duljine dva označimo redom sa M_2 i m_2 . Prema teoremu 2.7 za broj fiksnih točaka F_2 vrijedi nejednakost $F_2 \leq 13$. Na temelju uvedenih oznaka, možemo izraziti broj točaka, odnosno blokova dizajna \mathcal{D} :

$$45 = F_2 + 2M_2, \quad 99 = f_2 + 2m_2.$$

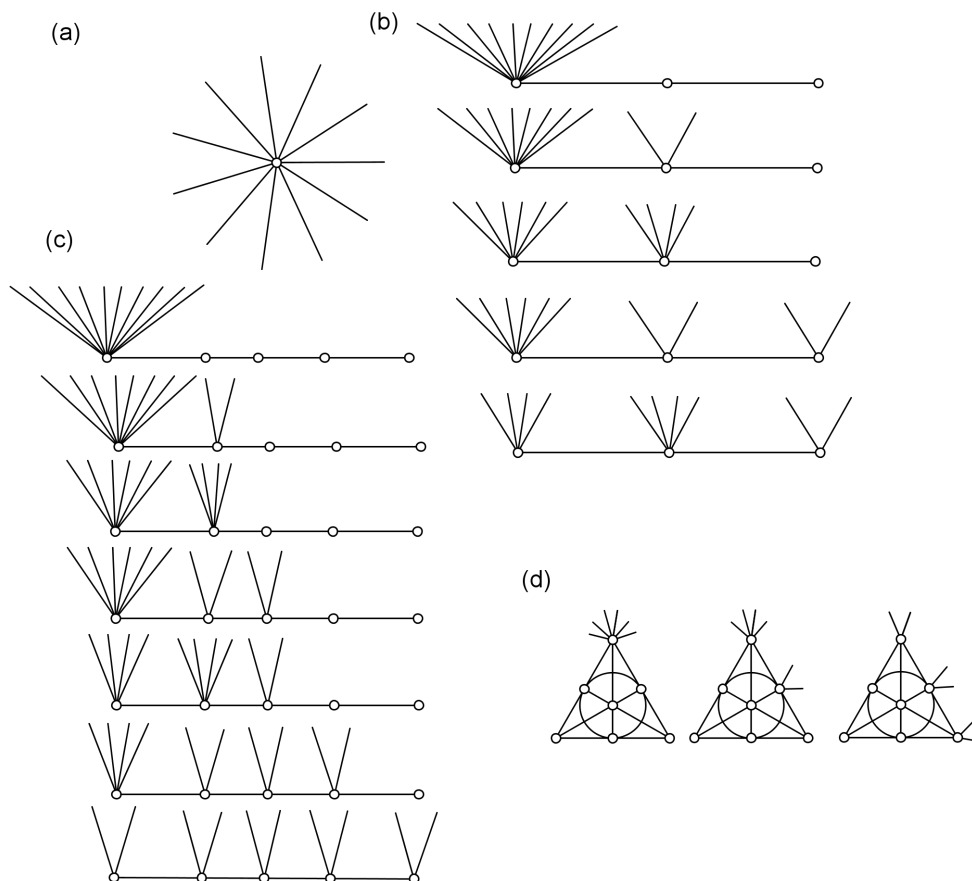
Neka je \mathcal{B}_i skup blokova incidentnih sa i fiksnih točaka i $b_i = |\mathcal{B}_i|$, za $i = 0, \dots, 5$. Skupovi \mathcal{B}_2 i \mathcal{B}_4 očito su prazni. Blokovi u \mathcal{B}_0 nisu fiksni, jer u protivnom, prema korolaru 4.1, stupanj fiksnog bloka iz \mathcal{B}_0 bio bi paran broj što je nemoguće jer je svaki blok stupnja pet. Blokovi u \mathcal{B}_3 i \mathcal{B}_5 su fiksni, što vrijedi prema tvrdnji leme 2.2, dok blokovi u \mathcal{B}_1 mogu biti fiksni ili nefiksni. Označimo sa \mathcal{B}'_1 skup svih fiksnih, a \mathcal{B}''_1 skup svih nefiksnih blokova iz \mathcal{B}_1 , te sa $b'_1 = |\mathcal{B}'_1|$ i $b''_1 = |\mathcal{B}''_1|$. Ukupan broj blokova i broj fiksnih blokova možemo izraziti na sljedeći način

$$b_0 + b'_1 + b''_1 + b_3 + b_5 = 99, \tag{4.1}$$

$$b'_1 + b_3 + b_5 = 99 - 2m_2. \tag{4.2}$$

Blokovi iz skupa \mathcal{B}'_1 sadrže dvije, a blokovi iz \mathcal{B}_3 jednu orbitu točaka duljine dva, pa prema tvrdnji leme 4.1 vrijedi jednakost

$$2b'_1 + b_3 = M_2, \tag{4.3}$$



Slika 4.1: Fiksne strukture involutornog automorfizma 2-(45, 5, 1) dizajna

što znači da je svaka nefiksna točka sadržana u nekom fiksnom bloku. Sljedeće dvije jednačbe dobivamo prebrojavanjem parova fiksnih točaka i parova nefiksnih točaka

$$3b_3 + 10b_5 = \binom{F_2}{2} = (45 - 2M_2)(22 - M_2) \quad (4.4)$$

$$10b_0 + 6b'_1 + 6b''_1 + b_3 = \binom{2M_2}{2} = M_2(2M_2 - 1). \quad (4.5)$$

Sustav jednačbi (4.1)-(4.5) ima jedinstveno rješenje za zadane vrijednosti M_2 i m_2 i možemo ih izraziti na sljedeći način:

$$\begin{aligned} b_0 &= 20M_2 - 8m_2 \\ b'_1 &= \frac{M_2(M_2 - 41)}{2} + 5m_2 \\ b''_1 &= -20M_2 + 10m_2 \\ b_3 &= M_2(42 - M_2) - 10m_2 \\ b_5 &= \frac{M_2(M_2 - 43)}{2} + 3m_2 + 99. \end{aligned}$$

4.1 Djelovanje automorfizma reda šest na 2-(45, 5, 1) dizajn

Nenegativni cijeli brojevi b_i , $i = 0, 3, 5$, te b'_1 i b''_1 se dobiju za devet parova $(M_2, m_2) \in \{16, \dots, 22\} \times \{1, \dots, 49\}$ navedenih u tablici 4.1.

Redni broj	F_2	f_2	M_2	m_2	b_0	b'_1	b''_1	b_3	b_5
1	1	11	22	44	88	11	0	0	0
2	3	11	21	44	68	10	20	1	0
3	5	11	20	44	48	10	40	0	1
4	7	13	19	43	36	6	50	7	0
5	9	13	18	43	16	8	70	2	3
6	9	15	18	42	24	3	60	12	0
7	11	15	17	42	4	6	80	5	4
8	11	17	17	41	12	1	70	15	1
9	13	19	16	40	0	0	80	16	3

Tablica 4.1: Rješenja sustava jednadžbi (4.1)-(4.5)

Prva četiri retka tablice 4.1 odgovaraju fiksnim strukturama (a), (b), (c) i (d).

Retci od petog do osmog opisuju nemoguće fiksne strukture. Fiksna struktura opisana petim retkom ima tri bloka iz skupa \mathcal{B}_5 , za što treba barem 12 fiksnih točaka, a ima ih devet. Fiksna struktura opisana sedmim retkom ima četiri bloka iz skupa \mathcal{B}_5 , za što treba barem 12 fiksnih točaka, a ima ih 11.

Šesti redak isto tako opisuje nemoguću fiksnu strukturu. Devet točaka i dvanaest blokova čine afinu ravninu reda tri. Stupanj svake točke u toj strukturi je četiri. Broj fiksnih blokova kroz fiksnu točku je neparan, što znači da bi svaka točka trebala biti incidentna s još barem jednim fiksnim blokom, međutim u šestom retku imamo samo tri bloka iz \mathcal{B}'_1 .

Osmi redak opisuje linearni prostor s 11 točaka i 16 blokova od kojih je jedan stupnja pet, a ostalih petnaest blokova je stupnja tri. V. Krčadinac je u svojoj disertaciji [37] utvrdio da postoji samo jedan, do na izomorfizam, takav linearni prostor koji ima šest točaka stupnja pet i pet točaka stupnja četiri. Osmi redak ne može opisivati fiksnu strukturu involutornog automorfizma 2-(45, 5, 1) dizajna, prema tvrdnji leme 4.1 i činjenici da je $b'_1 = 1$.

Deveti redak opisuje fiksnu strukturu koja odgovara linearnom prostoru (e). Jedna točka tog linearnog prostora je incidentna s tri bloka iz skupa \mathcal{B}_5 , a preostalih 12 točaka je incidentno s pet blokova od kojih je jedan iz skupa \mathcal{B}_5 , a preostala četiri bloka iz skupa \mathcal{B}_3 . Matrica incidencije tog linearnog prostora s retcima koji predstavljaju blokove je sljedeća:

$$\begin{bmatrix}
 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0
 \end{bmatrix}$$

□

Zatim promotrimo fiksnu strukturu za djelovanje grupe automorfizama reda tri na 2-(45, 5, 1) dizajn \mathcal{D} .

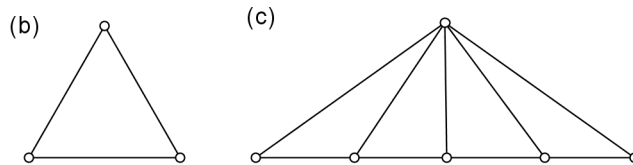
Lema 4.3. *Niti jedna nefiksna točka automorfizma reda tri dizajna \mathcal{D} s parametrima 2-(45, 5, 1) nije sadržana u svim blokovima iz neke orbite blokova duljine tri. Osim toga, niti jedan nefiksni blok ne sadrži sve točke iz neke orbite točaka duljine tri.*

Dokaz. Automorfizam reda tri dizajna \mathcal{D} ima barem tri nefiksne točke i barem tri nefiksna bloka. Ako za točku iz neke orbite točaka i duljine tri, $i \in \{1, \dots, m\}$, vrijedi da je sadržana u svim blokovima iz neke orbite blokova j duljine tri, $j \in \{1, \dots, n\}$, tada su i preostale dvije točke iz orbite i sadržane u svim blokovima iz orbite j , što znači da postoje dvije točke koje su sadržane u tri bloka, što je nemoguće jer $\lambda = 1$. Tvrdnja za blokove direktna je posljedica tvrdnje iz leme 2.1. □

Propozicija 4.2. *Automorfizam reda tri djeluje na 2-(45, 5, 1) dizajn \mathcal{D} na jedan od sljedećih načina:*

- (a) *Ne fiksira niti jednu točku i niti jedan blok.*
- (b) *Fiksira tri točke i tri bloka koji čine simetričan 2-(3, 2, 1) dizajn.*
- (c) *Fiksira šest točaka i šest blokova.*

Fiksne strukture (b) i (c) prikazane su na slici 4.2.



Slika 4.2: Fiksne strukture automorfizma reda tri koji djeluje na 2-(45, 5, 1) dizajn

Dokaz. Koristimo oznake F_3 i f_3 za broj fiksnih točaka i fiksnih blokova automorfizma reda tri koji djeluje na dizajn \mathcal{D} . Označimo sa M_3 i m_3 broj orbita točaka i orbita blokova duljine tri. Prema teoremu 2.7, za broj fiksnih točaka F_3 vrijedi nejednakost $F_3 \leq 12$. Na temelju uvedenih oznaka, možemo izraziti broj točaka, odnosno blokova dizajna \mathcal{D} :

$$45 = F_3 + 3M_3, \quad 99 = f_3 + 3m_3.$$

Neka je \mathcal{B}_i skup blokova incidentnih sa i fiksnih točaka i $b_i = |\mathcal{B}_i|$, za $i = 0, \dots, 5$. Skupovi \mathcal{B}_3 i \mathcal{B}_4 su očito prazni. Blokovi u \mathcal{B}_0 i \mathcal{B}_1 nisu fiksni, dok su blokovi u \mathcal{B}_2 i \mathcal{B}_5 fiksni prema tvrdnji leme 2.2. Blokovi u \mathcal{B}_0 i \mathcal{B}_1 ne sadrže sve točke iz neke orbite točaka duljine tri prema tvrdnji leme 4.3.

Blokovi u \mathcal{B}_0 ili sadrže dvije točke iz jedne orbite točaka duljine tri i po jednu točku iz tri orbite točaka duljine tri i te blokove označimo sa \mathcal{B}'_0 ili sadrže po jednu nefiksnu točku iz pet orbita točaka duljine tri i označimo ih sa \mathcal{B}''_0 . Označimo sa $b'_0 = |\mathcal{B}'_0|$, te sa $b''_0 = |\mathcal{B}''_0|$. Blokovi iz \mathcal{B}_1 ili sadrže dvije točke iz jedne orbite točaka duljine tri i po jednu točku iz dvije orbite točaka duljine tri i te blokove označimo sa \mathcal{B}'_1 ili sadrže po jednu točku iz četiri orbite točaka duljine tri i označimo ih sa \mathcal{B}''_1 . Ukupan broj blokova i broj fiksnih blokova možemo izraziti na sljedeći način:

$$b'_0 + b''_0 + b'_1 + b''_1 + b_2 + b_5 = 99 \quad (4.6)$$

$$b_2 + b_5 = 99 - 3m_3 \quad (4.7)$$

Svaki blok iz skupa \mathcal{B}_2 sadrži po jednu orbitu točaka duljine tri, dok blokovi iz \mathcal{B}'_0 i \mathcal{B}'_1 sadrže po dvije točke iz neke orbite točaka duljine tri, stoga vrijedi sljedeća jednakost

$$\frac{b'_0}{3} + \frac{b'_1}{3} + b_2 = M_3. \quad (4.8)$$

Sljedeće dvije jednadžbe dobivamo prebrojavanjem parova fiksnih točaka i parova nefiksnih točaka:

$$b_2 + 10b_5 = \binom{F_3}{2} = \frac{(45 - 3M_3)(44 - 3M_3)}{2}, \quad (4.9)$$

$$10b'_0 + 10b''_0 + 6b'_1 + 6b''_1 + 3b_2 = \binom{3M_3}{2} = \frac{3M_3(3M_3 - 1)}{2}. \quad (4.10)$$

Osim toga vrijedi

$$b'_0, b''_0, b'_1, b''_1 \equiv 0 \pmod{3} \quad (4.11)$$

Jednadžbe (4.7) i (4.9) imaju jedinstveno rješenje za zadane vrijednosti M_3 i m_3 i možemo ih izraziti na sljedeći način:

$$\begin{aligned} b_2 &= \frac{1}{6}(89M_3 - 3M_3^2 - 20m_3) \\ b_5 &= \frac{1}{6}(594 - 89M_3 + 3M_3^2 + 2m_3). \end{aligned} \quad (4.12)$$

Nenegativni cijeli brojevi b_2 i b_5 se dobiju za 15 parova $(M_3, m_3) \in \{11, \dots, 15\} \times \{0, \dots, 33\}$ navedenih u tablici 4.2.

Redni broj	F_3	f_3	M_3	m_3	b_2	b_5
1	0	0	15	33	0	0
2	3	3	14	32	3	0
3	6	6	13	31	5	1
4	6	15	13	28	15	0
5	9	9	12	30	6	3
6	9	18	12	27	16	2
7	9	27	12	24	26	1
8	9	36	12	21	36	0
9	12	12	11	29	6	6
10	12	21	11	26	16	5
11	12	30	11	23	26	4
12	12	39	11	20	36	3
13	12	48	11	17	46	2
14	12	57	11	14	56	1
15	12	66	11	11	66	0

Tablica 4.2: Rješenja sustava (4.12)

Iz jednadžbi (4.6), (4.8), (4.10) i (4.11) nenegativni cijeli brojevi b'_0, b''_0, b'_1, b''_1 se dobiju samo za parametre iz prva tri i iz petog retka tablice 4.2 i navodimo ih u tablici 4.3.

Peti redak u tablici 4.2, odnosno retci od 21-27 u tablici 4.3 opisuju nemoguće fiksne strukture, jer oni pretpostavljaju postojanje tri bloka iz skupa \mathcal{B}_5 , za što je potrebno barem 12 fiksnih točaka, a ima ih devet. Stoga, slijedi da prva tri retka u tablici 4.2 odgovaraju djelovanjima (a), (b) i (c) iz tvrdnje propozicije, dok preostali retci te tablice opisuju nemoguće strukture. □

Sada promotrimo na koji način automorfizam reda šest djeluje na skupu točaka i blokova 2-(45, 5, 1) dizajna \mathcal{D} . Grupa automorfizama $\langle \alpha \mid \alpha^6 = 1 \rangle$ može djelovati na skup točaka i blokova dizajna \mathcal{D} tako da formira orbite točaka, odnosno blokova duljine jedan, dva, tri ili šest, što vrijedi na temelju tvrdnje u korolaru 1.1. Na temelju toga i činjenice da je svaki blok incidentan s pet točaka slijedi tvrdnja sljedeće propozicije.

4.1 Djelovanje automorfizma reda šest na 2-(45, 5, 1) dizajn

Redni broj	F_3	f_3	M_3	m_3	b_0'	b_0''	b_1'	b_1''	b_2	b_5
1	0	0	15	33	45	54	0	0	0	0
2	3	3	14	32	33	36	0	27	3	0
3	3	3	14	32	30	39	3	24	3	0
4	3	3	14	32	27	42	6	21	3	0
5	3	3	14	32	24	45	9	18	3	0
6	3	3	14	32	21	48	12	15	3	0
7	3	3	14	32	18	51	15	12	3	0
8	3	3	14	32	15	54	18	9	3	0
9	3	3	14	32	12	57	21	6	3	0
10	3	3	14	32	9	60	24	3	3	0
11	3	3	14	32	6	63	27	0	3	0
12	6	6	13	31	24	18	0	51	5	1
13	6	6	13	31	21	21	3	48	5	1
14	6	6	13	31	18	24	6	45	5	1
15	6	6	13	31	15	27	9	42	5	1
16	6	6	13	31	12	30	12	39	5	1
17	6	6	13	31	9	33	15	36	5	1
18	6	6	13	31	6	36	18	33	5	1
19	6	6	13	31	3	39	21	30	5	1
20	6	6	13	31	0	42	24	27	5	1
21	9	9	12	30	18	0	0	72	6	3
22	9	9	12	30	15	3	3	69	6	3
23	9	9	12	30	12	6	6	66	6	3
24	9	9	12	30	9	9	9	63	6	3
25	9	9	12	30	6	12	12	60	6	3
26	9	9	12	30	3	15	15	57	6	3
27	9	9	12	30	0	18	18	54	6	3

Tablica 4.3: Rješenja sustava jednadžbi (4.6), (4.8), (4.10) i (4.11)

Propozicija 4.3. *Fiksni blok za djelovanje automorfizma reda šest na 2-(45, 5, 1) dizajn \mathcal{D} može sadržavati:*

1. *pet fiksnih točaka,*
2. *jednu fiksnu točku i sve točke iz dvije orbite točaka duljine dva,*
3. *dvije fiksne točke i sve točke iz jedne orbite točaka duljine tri,*
4. *tri fiksne točke i sve točke iz jedne orbite točaka duljine dva,*
5. *sve točke iz jedne orbite duljine dva i sve točke iz jedne orbite duljine tri.*

Napomena 4.1. Neka grupa $G = \langle \alpha \mid \alpha^6 = 1 \rangle \cong Z_6 \cong Z_3 \times Z_2$ djeluje na 2-(45, 5, 1) dizajn \mathcal{D} . Ako je $\mathcal{P}_i = G.P$ za točku P , onda je $|\mathcal{P}_i| \in \{1, 2, 3, 6\}$, za neki $i \in \{1, \dots, m\}$, $m \in \mathbb{N}$.

1. Ako je $|\mathcal{P}_i| = 1$, onda svi elementi grupe G fiksiraju točku P .

2. Ako je $|\mathcal{P}_i| = 2$, onda je $|G_P| = 3$ i možemo pretpostaviti da je $G_P = \langle \alpha^2 \rangle$. Promotrimo kako grupa G djeluje na orbiti duljine dva. Prema teoremu 1.6, dovoljno je promotriti djelovanje grupe G na desne susjedne klase podgrupe $\langle \alpha^2 \rangle$ u grupi G : $0 = \langle \alpha^2 \rangle$ i $1 = \langle \alpha^2 \rangle \alpha^3$, što znači da automorfizam α^3 na tim susjednim klasama djeluje kao ciklus $(0, 1)$, dok automorfizam α^2 djeluje na te susjedne klase tako da fiksira sve elemente:

$$0\alpha^2 = \langle \alpha^2 \rangle \alpha^2 = \langle \alpha^2 \rangle = 0, \quad 1\alpha^2 = \langle \alpha^2 \rangle \alpha^3 \alpha^2 = \langle \alpha^2 \rangle \alpha^2 \alpha^3 = 1.$$

3. Ako je $|\mathcal{P}_i| = 3$, onda je $|G_P| = 2$ i možemo pretpostaviti da je $G_P = \langle \alpha^3 \rangle$. Promotrimo kako grupa G djeluje na orbiti duljine tri. Prema teoremu 1.6, dovoljno je promotriti djelovanje grupe G na desne susjedne klase podgrupe $\langle \alpha^3 \rangle$ u grupi G : $0 = \langle \alpha^3 \rangle$, $1 = \langle \alpha^3 \rangle \alpha^2$ i $2 = \langle \alpha^3 \rangle \alpha^4$. Očigledno je da automorfizam α^2 djeluje na tim susjednim klasama kao ciklus $(0, 1, 2)$, dok automorfizam α^3 djeluje na te susjedne klase tako da fiksira sve elemente:

$$\begin{aligned} 0\alpha^3 &= \langle \alpha^3 \rangle \alpha^3 = 0, \\ 1\alpha^3 &= \langle \alpha^3 \rangle \alpha^2 \alpha^3 = \langle \alpha^3 \rangle \alpha^3 \alpha^2 = \langle \alpha^3 \rangle \alpha^2 = 1, \\ 2\alpha^3 &= \langle \alpha^3 \rangle \alpha^4 \alpha^3 = \langle \alpha^3 \rangle \alpha^4 = 2. \end{aligned}$$

4. Ako je $|\mathcal{P}_i| = 6$, onda je $|G_P| = 1$. Desne susjedne klase jedinične grupe su svi elementi grupe G : $0 = 1_G$, $1 = \alpha^2$, $2 = \alpha^4$, $3 = \alpha^3$, $4 = \alpha^5$, $5 = \alpha$. Stoga, automorfizam α^2 na G -orbiti duljine 6 djeluje kao permutacija $(0, 1, 2)(3, 4, 5)$, dok automorfizmi α^3 i α djeluju kao permutacija $(0, 3)(1, 4)(2, 5)$, odnosno kao permutacija $(0, 5, 1, 3, 2, 4)$.

S obzirom da grupa G sadrži jednu klasu konjugiranih podgrupa reda dva i jednu klasu konjugiranih podgrupa reda tri, predstavnici G -orbita točkaka iste duljine imaju konjugirane stabilizatore. Analogna tvrdnja vrijedi i za G -orbite blokova.

Broj fiksnih točkaka, odnosno fiksnih blokova za djelovanje grupe automorfizama $\langle \alpha \mid \alpha^6 = 1 \rangle$ na 2-(45, 5, 1) dizajn \mathcal{D} označimo redom sa F_6 i f_6 .

U ovom poglavlju pod oznakama D_i i d_i podrazumijevamo broj $\langle \alpha \rangle$ -orbita redom točkaka i blokova dizajna \mathcal{D} duljine i , $i \in \{1, 2, 3, 6\}$, dok za distribuciju duljina $\langle \alpha \rangle$ -orbita točkaka i duljina $\langle \alpha \rangle$ -orbita blokova uvodimo oznake redom

$$\nu = (D_1 \times 1, D_2 \times 2, D_3 \times 3, D_6 \times 6), \quad \beta = (d_1 \times 1, d_2 \times 2, d_3 \times 3, d_6 \times 6).$$

Vektor $\kappa\nu$ s informacijom o konjugiranosti stabilizatora predstavnika $\langle \alpha \rangle$ -orbita točkaka ima jednake vrijednosti za svaku $\langle \alpha \rangle$ -orbitu točkaka iste duljine, što vrijedi prema napomeni 4.1. Isto to svojstvo vrijedi i za vektor $\kappa\beta$ s informacijom o konjugiranosti stabilizatora predstavnika $\langle \alpha \rangle$ -orbita blokova. Ako vrijedi $D_i, d_i \neq 0$, $\forall i \in \{1, 2, 3, 6\}$ vektori $\kappa\nu$ i $\kappa\beta$

4.1 Djelovanje automorfizma reda šest na 2-(45, 5, 1) dizajn

imaju sljedeći zapis:

$$\kappa\nu = (D_1 \times 0, D_2 \times 1, D_3 \times 2, D_6 \times 3), \quad \kappa\beta = (d_1 \times 0, d_2 \times 1, d_3 \times 2, d_6 \times 3).$$

U sljedeće četiri leme analizirane su sve mogućnosti kako automorfizma reda šest može djelovati na skup točaka i blokova 2-(45, 5, 1) dizajna.

Lema 4.4. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn i $\alpha \in \text{Aut}(\mathcal{D})$, $\langle \alpha \rangle \cong Z_6$. Tada za broj fiksnih točaka F_2 involutornog automorfizma $\rho \in \text{Aut}(\mathcal{D})$, $\langle \rho \rangle = \langle \alpha^3 \rangle \cong Z_2$ vrijedi $F_2 \in \{5, 7, 13\}$.*

Dokaz. Prema tvrdnji propozicije 4.1 za broj fiksnih točaka involutornog automorfizma $\rho \in \text{Aut}(\mathcal{D})$ vrijedi $F_2 \in \{1, 3, 5, 7, 13\}$.

Ako je $F_2 = 1$, tada automorfizam reda tri $\phi \in \text{Aut}(\mathcal{D})$, $\langle \phi \rangle = \langle \alpha^2 \rangle$, fiksira $F_3 \equiv 1 \pmod{2}$ točaka, pa iz tvrdnje propozicije 4.2 slijedi da je $F_3 = 3$. To znači da je jedna točka dizajna \mathcal{D} zajednička fiksna točka za automorfizme ϕ i ρ . Stoga, distribucija duljina $\langle \alpha \rangle$ -orbita točaka dizajna \mathcal{D} je $\nu = (1 \times 1, 1 \times 2, 7 \times 6)$. Dalje promotrimo djelovanje grupe $\langle \alpha \rangle$ na skupu blokova dizajna \mathcal{D} . Vrijedi da α ne fiksira niti jedan blok tog dizajna, odnosno $f_6 = 0$, što slijedi iz distribucije ν i tvrdnje propozicije 4.3. Prema tvrdnji (a) propozicije 4.1 za automorfizam ρ vrijedi $f_2 = 11$, dok prema tvrdnji (b) u propoziciji 4.2 vrijedi $f_3 = 3$, odakle slijedi da automorfizmi ρ i ϕ imaju dva zajednička fiksna bloka, odnosno $f_6 = 2$ što je u kontradikciji s činjenicom da je $f_6 = 0$. Stoga, vrijedi $F_2 \neq 1$.

Ako je $F_2 = 3$, onda je $f_2 = 11$. Kako je $f_2 \equiv 2 \pmod{3}$ vrijedi da je

$$f_6 \geq 2. \tag{4.13}$$

Broj fiksnih točaka automorfizma ϕ reda tri je $F_3 \in \{0, 3, 6\}$, prema tvrdnji propozicije 4.2. Ako je $F_3 = 0$, tada grupa $\langle \alpha \rangle$ djeluje na skup točaka s distribucijom duljina orbita točaka $\nu = (1 \times 3, 7 \times 6)$. Tada prema propoziciji 4.3 grupa $\langle \alpha \rangle$ ne fiksira niti jedan blok, odnosno $f_6 = 0$, što je nemoguće zbog (4.13).

Ako je $F_3 = 3$, onda automorfizmi ϕ i ρ imaju tri zajedničke fiksne točke, odnosno distribucija duljina orbita točaka za djelovanje grupe $\langle \alpha \rangle$ je $\nu = (3 \times 1, 7 \times 6)$. Tada prema propoziciji 4.3 vrijedi $f_6 = 0$, što je nemoguće zbog (4.13).

Preostaje još slučaj kada je $F_3 = 6$. U tom slučaju automorfizmi ϕ i ρ nemaju zajedničkih fiksnih točaka, odnosno distribucija duljina orbita točaka za djelovanje grupe $\langle \alpha \rangle$ je $\nu = (3 \times 2, 1 \times 3, 6 \times 6)$. Odavde slijedi da ako α fiksira barem jedan blok, tada je on kao u petom slučaju propozicije 4.3, a takvih fiksnih blokova može biti najviše jedan (odnosno $f_6 \leq 1$) zbog tvrdnje leme 2.1, što je nemoguće zbog (4.13). Na temelju svega razmotrenog slijedi tvrdnja leme. \square

Lema 4.5. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, $\alpha \in \text{Aut}(\mathcal{D})$, $\langle \alpha \rangle \cong Z_6$ i neka involutorni automorfizam $\rho \in \text{Aut}(\mathcal{D})$, $\langle \rho \rangle = \langle \alpha^3 \rangle \cong Z_2$ fiksira pet točkaka. Tada grupa $\langle \alpha \rangle$ na dizajn \mathcal{D} može djelovati sa sljedećom distribucijom duljina orbita točkaka ν , odnosno blokova β :*

$$\begin{aligned}\nu &= (2 \times 1, 2 \times 2, 1 \times 3, 6 \times 6) \\ \beta &= (2 \times 1, 2 \times 2, 3 \times 3, 14 \times 6).\end{aligned}\tag{4.14}$$

Dokaz. Prema pretpostavci involutorni automorfizam ρ fiksira pet točkaka odnosno vrijedi $F_2 = 5$. Za broj fiksnih točkaka automorfizma ϕ reda tri dizajna \mathcal{D} vrijedi $F_3 = 2 + 2k' + 3k''$, za $k', k'' \in \mathbb{N}_0$, zbog toga što je $F_2 \equiv 2 \pmod{3}$. Stoga, iz tvrdnje propozicije 4.2 slijedi da je $F_3 = 6$. Automorfizmi ϕ i ρ imaju dvije zajedničke fiksne točke, odnosno grupa $\langle \alpha \rangle$ fiksira dvije točke ($F_6 = 2$) i na dizajn \mathcal{D} djeluje s distribucijom duljina orbita točkaka $\nu = (2 \times 1, 2 \times 2, 1 \times 3, 6 \times 6)$.

Promotrimo djelovanje grupe $\langle \alpha \rangle$ na skup blokova dizajna \mathcal{D} . Za broj fiksnih blokova grupe $\langle \alpha \rangle$ vrijedi $f_6 \equiv 2 \pmod{3}$, zbog toga što je $f_2 \equiv 2 \pmod{3}$. S druge strane, iz distribucije ν slijedi da su ti fiksni blokovi tipa kao u slučaju dva, tri ili pet iz propozicije 4.3 i pri tom vrijedi $f_6 \leq 2$, prema tvrdnji leme 2.1. Stoga, $f_6 = 2$, odnosno automorfizmi ϕ i ρ imaju dva zajednička fiksna bloka, pa grupa $\langle \alpha \rangle$ na skup blokova \mathcal{D} djeluje s distribucijom duljina orbita $\beta = (2 \times 1, 2 \times 2, 3 \times 3, 14 \times 6)$. Time je dokazana tvrdnja. \square

Lema 4.6. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, $\alpha \in \text{Aut}(\mathcal{D})$, $\langle \alpha \rangle \cong Z_6$ i neka involutorni automorfizam $\rho \in \text{Aut}(\mathcal{D})$, $\langle \rho \rangle = \langle \alpha^3 \rangle \cong Z_2$ fiksira sedam točkaka. Tada grupa $\langle \alpha \rangle$ na dizajn \mathcal{D} može djelovati sa sljedećom distribucijom duljina orbita točkaka ν , odnosno blokova β :*

$$\begin{aligned}\nu &= (1 \times 1, 1 \times 2, 2 \times 3, 6 \times 6) \\ \beta &= (1 \times 1, 1 \times 2, 4 \times 3, 14 \times 6).\end{aligned}\tag{4.15}$$

Dokaz. Budući da je prema pretpostavci leme $F_2 = 7$, onda je $f_2 = 13$. Zbog toga što je $f_2 \equiv 1 \pmod{3}$, za broj fiksnih blokova automorfizma α vrijedi

$$f_6 \equiv 1 \pmod{3}.\tag{4.16}$$

Iz (4.16) slijedi da postoji barem jedan fiksni blok dizajna \mathcal{D} za djelovanje grupe $\langle \alpha \rangle$, odnosno $f_6 \geq 1$. Za broj fiksnih točkaka automorfizma ϕ reda tri dizajna \mathcal{D} vrijedi da je $F_3 = 1 + 2k' + 3k''$, $k', k'' \in \mathbb{N}_0$, zbog toga što je $F_2 \equiv 1 \pmod{3}$. Stoga, iz tvrdnje propozicije 4.2 slijedi da je $F_3 \in \{3, 6\}$.

Ako je $F_3 = 3$, onda automorfizmi ϕ i ρ imaju jednu zajedničku fiksnu točku, odnosno grupa $\langle \alpha \rangle$ na skup točkaka dizajna \mathcal{D} djeluje s distribucijom duljina orbita $\nu = (1 \times 1, 1 \times 2, 2 \times 3, 6 \times 6)$.

Promotrimo djelovanje grupe $\langle \alpha \rangle$ na skupu blokova dizajna \mathcal{D} . Iz distribucije ν slijedi da

su fiksni blokovi tipa kao u petom slučaju propozicije 4.3 i pri tom vrijedi $f_6 \leq 1$, prema tvrdnji leme 2.1. Stoga, $f_6 = 1$, odnosno automorfizmi ϕ i ρ imaju jedan zajednički fiksni blok, pa grupa $\langle \alpha \rangle$ na skup blokova \mathcal{D} djeluje s distribucijom duljina orbita $\beta = (1 \times 1, 1 \times 2, 4 \times 3, 14 \times 6)$. Distribucije ν i β odgovaraju onima iz (4.15).

Ako pretpostavimo da je $F_3 = 6$, tada automorfizmi ϕ i ρ imaju četiri zajedničke fiksne točke, odnosno grupa $\langle \alpha \rangle$ na skup točaka dizajna \mathcal{D} djeluje s distribucijom duljina orbita $\nu = (4 \times 1, 1 \times 2, 1 \times 3, 6 \times 6)$. Iz distribucije ν slijedi da su fiksni blokovi dizajna \mathcal{D} za djelovanje grupe $\langle \alpha \rangle$ tipa kao u slučajevima tri, četiri ili pet iz propozicije 4.3 i pritom vrijedi $f_6 \leq 2$ prema tvrdnji leme 2.1. Pa iz (4.16) slijedi da je $f_6 = 1$. Međutim, $f_6 \neq 1$ jer u protivnom vrijedi $f_3 \equiv 1 \pmod{2}$, što je u kontradikciji s činjenicom da je $f_3 = 6$. Time je dokazana tvrdnja. \square

Još preostaje promotriti situaciju kada involutorni automorfizam djeluje na skup točaka dizajna \mathcal{D} tako da fiksira maksimalan broj točaka.

Lema 4.7. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, $\alpha \in \text{Aut}(\mathcal{D})$, $\langle \alpha \rangle \cong Z_6$ i neka automorfizam $\rho \in \text{Aut}(\mathcal{D})$, $\langle \rho \rangle = \langle \alpha^3 \rangle \cong Z_2$ fiksira 13 točaka. Tada grupa $\langle \alpha \rangle$ na dizajn \mathcal{D} može djelovati s jednom od sljedeće dvije distribucije duljina orbita točaka ν , odnosno blokova β :*

$$\nu = (1 \times 1, 1 \times 2, 4 \times 3, 5 \times 6), \quad \beta = (1 \times 1, 1 \times 2, 6 \times 3, 13 \times 6), \quad (4.17)$$

$$\nu = (4 \times 1, 1 \times 2, 3 \times 3, 5 \times 6), \quad \beta = (4 \times 1, 1 \times 2, 5 \times 3, 13 \times 6). \quad (4.18)$$

Dokaz. Budući da je prema pretpostavci leme $F_2 = 13$, onda je $f_2 = 19$. Zbog toga što je $f_2 \equiv 1 \pmod{3}$, za broj fiksnih blokova grupe $\langle \alpha \rangle$ vrijedi

$$f_6 \equiv 1 \pmod{3}. \quad (4.19)$$

Za broj fiksnih točaka automorfizma ϕ reda tri vrijedi $F_3 = 1 + 2k' + 3k'' \geq 1$, $k', k'' \in \mathbb{N}_0$, zbog toga što je $F_2 \equiv 1 \pmod{3}$. Stoga, iz tvrdnje propozicije 4.2 slijedi da je $F_3 \in \{3, 6\}$. Ako je $F_3 = 3$, onda automorfizmi ϕ i ρ imaju jednu zajedničku fiksnu točku, odnosno grupa $\langle \alpha \rangle$ na skup točaka dizajna \mathcal{D} djeluje s distribucijom duljina orbita $\nu = (1 \times 1, 1 \times 2, 4 \times 3, 5 \times 6)$. Iz distribucije ν slijedi da su fiksni blokovi tipa kao u petom slučaju propozicije 4.3 i pri tom vrijedi $f_6 \leq 1$, prema tvrdnji leme 2.1. Pa odavde i iz (4.19) vrijedi da je $f_6 = 1$ i grupa $\langle \alpha \rangle$ na skup blokova dizajna \mathcal{D} djeluje s distribucijom duljina orbita $\beta = (1 \times 1, 1 \times 2, 6 \times 3, 13 \times 6)$. U ovom slučaju distribucije ν i β odgovaraju onima u (4.17).

Ako je $F_3 = 6$, onda automorfizmi ϕ i ρ imaju četiri zajedničke fiksne točke, odnosno grupa $\langle \alpha \rangle$ na skup točaka dizajna \mathcal{D} djeluje s distribucijom duljina orbita $\nu = (4 \times 1, 1 \times 2, 3 \times 3, 5 \times 6)$. Iz distribucije ν slijedi da su fiksni blokovi tipa kao u trećem, četvrtom ili petom slučaju iz propozicije 4.3 i pritom vrijedi $f_6 \leq 4$, prema tvrdnji leme 2.1. Stoga,

prema (4.19) vrijedi da je $f_6 \in \{1, 4\}$. Ako je $f_6 = 1$, tada je $f_3 \equiv 1 \pmod{2}$, što je u kontradikciji s $f_3 = 6$, pa slijedi da je $f_6 = 4$, odnosno grupa $\langle \alpha \rangle$ na skup blokova dizajna \mathcal{D} djeluje s distribucijom duljina orbita $\beta = (4 \times 1, 1 \times 2, 5 \times 3, 13 \times 6)$. U ovom slučaju distribucije ν i β odgovaraju onima u (4.18). \square

4.2 Konstrukcija orbitnih matrica i njihovo profinjene

Nakon što su određene sve moguće distribucije duljina orbita točaka i blokova za djelovanje automorfizma reda šest na 2-(45, 5, 1) dizajn, pomoću algoritma za konstrukciju orbitnih matrica blokovnih dizajna, konstruirane sve (do na izomorfizam) orbitne matrice za te distribucije.

Lema 4.8. *Do na izomorfizam, postoji 4355 orbitnih matrica za djelovanje grupe automorfizama $\langle \alpha \mid \alpha^6 = 1 \rangle$ na 2-(45, 5, 1) dizajn \mathcal{D} .*

Dokaz. U prethodnom poglavlju dobivena su četiri moguća kandidata (4.14), (4.15), (4.17) i (4.18) za distribuciju ν i β pri djelovanju grupe $\langle \alpha \mid \alpha^6 = 1 \rangle$ na dizajn \mathcal{D} . Označimo te četiri distribucije brojevima 1-4. Prema napomeni 4.1, za svaku od tih distribucija, vektori s informacijom o konjugiranosti stabilizatora predstavnika orbita točaka $\kappa\nu$ (blokova $\kappa\beta$) imaju iste vrijednosti za one orbite točaka (blokova) koje su iste duljine. U algoritmu za konstrukciju orbitnih matrica blokovnih dizajna ti vektori služe za eliminaciju izomorfnih orbitnih matrica, odnosno za eliminaciju G -izomorfnih dizajna. Rezultati o broju neizomorfnih orbitnih matrica dobivenih za svaku distribuciju duljina orbita iz teorema 4.1 prikazani su u tablici 4.4, a dobiveni su primjenom programa koji je napisan na temelju spomenutog algoritma. \square

Redni broj distribucije		1	2	3	4
# orbitnih matrica		20	1066	2798	471

Tablica 4.4: Broj neizomorfnih orbitnih matrica 2-(45, 5, 1) dizajna za distribucije duljina orbita (4.14), (4.15), (4.17) i (4.18))

Iz dokaza prethodne leme vidimo da se orbitne matrice mogu konstruirati za sve distribucije (4.14), (4.15), (4.17) i (4.18), stoga slijedi tvrdnja sljedećeg teorema.

Teorem 4.1. *Grupa automorfizama $\langle \alpha \mid \alpha^6 = 1 \rangle$ na skupu točaka i blokova 2-(45, 5, 1) dizajna \mathcal{D} može djelovati s jednom od sljedeće četiri distribucije duljina orbita točaka ν , odnosno blokova β :*

1. $\nu = (4 \times 1, 1 \times 2, 3 \times 3, 5 \times 6)$
 $\beta = (4 \times 1, 1 \times 2, 5 \times 3, 13 \times 6),$

4.2 Konstrukcija orbitnih matrica i njihovo profinjenje

2. $\nu = (2 \times 1, 2 \times 2, 1 \times 3, 6 \times 6)$
 $\beta = (2 \times 1, 2 \times 2, 3 \times 3, 14 \times 6),$
3. $\nu = (1 \times 1, 1 \times 2, 2 \times 3, 6 \times 6)$
 $\beta = (1 \times 1, 1 \times 2, 4 \times 3, 14 \times 6),$
4. $\nu = (1 \times 1, 1 \times 2, 4 \times 3, 5 \times 6)$
 $\beta = (1 \times 1, 1 \times 2, 6 \times 3, 13 \times 6).$

Sljedeći korak u konstrukciji blokovnog dizajna je profinjenje konstruiranih orbitnih matrica koje se izvodi pomoću programa napisanog na temelju algoritma za profinjenje orbitnih matrica opisanog u poglavlju 3.3.1.

Napravili smo profinjenje dobivenih orbitnih matrica za djelovanje grupe automorfizama $G = \langle \alpha \mid \alpha^6 = 1 \rangle$ iz tablice 4.4 do orbitnih matrica za njenu normalnu podgrupu $\langle \alpha^3 \rangle \cong Z_2$ uz pretpostavku djelovanja kvocijentne grupe $G/Z_2 \cong \langle \alpha^2 \rangle \cong Z_3$, a rezultati dobiveni za svaku distribuciju iz teorema 4.1 su prikazani u tablici 4.5.

Redni broj distribucije (teorem 4.1)	1	2	3	4
# orbitnih matrica nakon profinjenja	0	5843	1400	92

Tablica 4.5: Broj orbitnih matrica za djelovanje normalne podgrupe $\langle \alpha^3 \rangle \triangleleft G \leq \text{Aut}(\mathcal{D})$

Dalje slijedi još jedna primjena algoritma za profinjenje dobivenih orbitnih matrica, odnosno indeksiranje. Rezultati dobiveni za svaku pojedinu distribuciju iz teorema 4.1 prikazani su u tablici 4.6. Provjera izomorfности konstruiranih dizajna je napravljena pomoću GAP paketa Design ([59]). Na kraju ovog poglavlja navedeni su predstavnici orbita blokova konstruiranih 2-(45, 5, 1) dizajna za djelovanje njegove pune grupe automorfizama. Red i struktura pune grupe automorfizama tih dizajna određeni su pomoću spomenutog paketa.

Redni broj distribucije (teorem 4.1)	1	2	3	4
# dizajna nakon indeksiranja	0	0	0	3
# neizomorfni dizajna	0	0	0	3
$ \text{Aut}(\mathcal{D}) $	0	0	0	24

Tablica 4.6: Rezultati indeksiranja i broj neizomorfnih 2-(45, 5, 1) dizajna

Kao provjeru točnosti dobivenih rezultata, radimo profinjenje orbitnih matrica iz tablice 4.4 također za djelovanje normalne podgrupe $\langle \alpha^2 \rangle \triangleleft G$, $\langle \alpha^2 \rangle \cong Z_3$ uz pretpostavku djelovanja kvocijentne grupe $G/Z_3 \cong \langle \alpha^3 \rangle \cong Z_2$, a rezultati su prikazani u tablici 4.7.

Nakon još jedne primjene algoritma za profinjenje orbitnih matrica, odnosno profinjenjem orbitnih matrica iz tablice 4.7, dobiju se isti rezultati kao u tablici 4.6.

Redni broj distribucije (teorem 4.1)	1	2	3	4
# orbitnih matrica nakon profinjenja	96	28	1262	85

Tablica 4.7: Broj orbitnih matrica za djelovanje normalne podgrupe $\langle \alpha^2 \rangle \triangleleft G \leq \text{Aut}(\mathcal{D})$

Time smo dokazali tvrdnju sljedećeg teorema.

Teorem 4.2. *Postoje tri, do na izomorfizam, 2-(45, 5, 1) dizajna na koje djeluje grupa automorfizama $\langle \alpha \mid \alpha^6 = 1 \rangle$.*

Tri konstruirana 2-(45, 5, 1) dizajna iz prethodnog teorema označimo sa $\mathcal{D}_1, \mathcal{D}_2$ i \mathcal{D}_3 . Sva tri dizajna imaju punu grupu automorfizama

$$G' \cong \langle g_1, g_2, g_3 \rangle \cong Z_2 \times A_4, \quad |G'| = 24,$$

s generatorima:

$$g_1 = (2,17)(3,20)(4,7)(6,9)(10,13)(12,15)(16,18)(19,21)(22,43)(23,29)(24,39)(25,40)(26,32)(27,36)(28,37)(30,45)(31,34)(33,42)(35,41)(38,44),$$

$$g_2 = (2,3)(16,19)(17,20)(18,21)(22,25)(23,26)(24,27)(28,31)(29,32)(30,33)(34,37)(35,38)(36,39)(40,43)(41,44)(42,45),$$

$$g_3 = (4,5,6)(7,8,9)(10,11,12)(13,14,15)(16,17,18)(19,20,21)(22,23,24)(25,26,27)(28,29,30)(31,32,33)(34,35,36)(37,38,39)(40,41,42)(43,44,45).$$

U tablici 4.8 prikazana je lista predstavnika orbita blokova za djelovanje grupe G' na dizajne $\mathcal{D}_1, \mathcal{D}_2$ i \mathcal{D}_3 .

Dizajn	Predstavnici orbita blokova
\mathcal{D}_1	[1, 2, 16, 17, 18], [1, 4, 7, 10, 13], [1, 22, 28, 34, 40] [2, 3, 4, 5, 6], [2, 7, 30, 31, 35], [2, 10, 19, 37, 40] [2, 13, 24, 26, 43], [4, 11, 12, 22, 25], [4, 23, 30, 38, 39]
\mathcal{D}_2	[1, 2, 16, 17, 18], [1, 4, 7, 10, 13], [1, 22, 28, 34, 40] [2, 3, 4, 5, 6], [2, 7, 24, 26, 28], [2, 10, 19, 37, 40] [2, 13, 33, 35, 43], [4, 11, 15, 28, 31], [4, 23, 24, 38, 45]
\mathcal{D}_3	[1, 2, 16, 17, 18], [1, 4, 7, 10, 13], [1, 22, 28, 34, 40], [2, 3, 4, 5, 6], [2, 7, 23, 27, 28], [2, 10, 19, 34, 43], [2, 13, 33, 38, 40], [4, 11, 15, 28, 31], [4, 23, 24, 38, 45]

Tablica 4.8: Predstavnici orbita blokova dizajna $\mathcal{D}_1, \mathcal{D}_2$ i \mathcal{D}_3 za djelovanje grupe G'

Poglavlje 5

Konstrukcija 2-(45, 5, 1) dizajna s grupom automorfizama $G \cong Z_3 \times Z_3$

U ovom poglavlju određena su sva moguća djelovanja grupe automorfizama $G \cong Z_3 \times Z_3$ na blokovnom dizajnu s parametrima 2-(45, 5, 1). S obzirom da u grupi G postoje četiri jednočlane klase konjugiranih podgrupa reda tri, najprije je utvrđeno predstavnici kojih orbita točaka, odnosno blokova, duljine tri imaju konjugirane stabilizatore. Zatim su za sva moguća djelovanja grupe G na 2-(45, 5, 1) dizajn konstruirane sve, do na izomorfizam, orbitne matrice uz primjenu programa za konstrukciju orbitnih matrica blokovnog dizajna. Konstruirani su svi međusobno neizomorfni 2-(45, 5, 1) dizajni uz pretpostavku djelovanja grupe $G \cong Z_3 \times Z_3$ u slučajevima kada postoje dvije podgrupe reda tri u grupi G koje djeluju na dizajn tako da nemaju zajedničkih orbita točaka i blokova duljine tri. Postoji sedam, do na izomorfizam, takvih dizajna.

5.1 Djelovanje grupe $G \cong Z_3 \times Z_3$ na 2-(45, 5, 1) dizajn

U ovom poglavlju određene su sve moguće distribucije duljina orbita točaka ν i blokova β , te pripadni vektori s informacijom o konjugiranosti stabilizatora predstavnika orbita točaka $\kappa\nu$ i orbita blokova $\kappa\beta$ pri djelovanju grupe automorfizama $G \cong Z_3 \times Z_3$ na 2-(45, 5, 1) dizajn \mathcal{D} .

Na temelju tvrdnje propozicije 4.2, grupa automorfizama reda tri na skup točaka i blokova dizajna \mathcal{D} može djelovati s jednom od sljedeće tri distribucije duljina orbita točaka ν i duljina orbita blokova β :

1. $\nu = (15 \times 3)$, $\beta = (33 \times 3)$,
2. $\nu = (3 \times 1, 14 \times 3)$, $\beta = (3 \times 1, 32 \times 3)$,
3. $\nu = (6 \times 1, 13 \times 3)$, $\beta = (6 \times 1, 31 \times 3)$.

Elementarno Abelova grupa $G = \langle \phi, \omega \mid \phi^3 = \omega^3 = 1, \phi^\omega = \phi \rangle \cong Z_3 \times Z_3$ sadrži četiri podgrupe reda tri od kojih svaka čini po jednu jednočlanu klasu konjugiranih podgrupa reda tri u G koje označimo sa

$$G_1 = \langle \phi \mid \phi^3 = 1 \rangle, G_2 = \langle \omega \mid \omega^3 = 1 \rangle, \\ G_3 = \langle \gamma \mid \gamma^3 = 1 \rangle = \langle \phi\omega \rangle, G_4 = \langle \delta \mid \delta^3 = 1 \rangle = \langle \phi^2\omega \rangle.$$

Označimo sa F_1, F_2, F_3 i F_4 broj fiksnih točaka, odnosno blokova, redom za grupe G_1, G_2, G_3 i G_4 . U ovom poglavlju za spomenute grupe reda tri i za broj njihovih fiksnih točaka (blokova) koristimo uvedene oznake.

Prema tvrdnji korolara 1.1, duljine G -orbita točaka i blokova dizajna \mathcal{D} mogu poprimiti vrijednosti iz skupa $\{1, 3, 9\}$. Kao u prethodnom poglavlju tako i ovdje koristimo oznaku za distribuciju duljina G -orbita točaka $\nu = (D_1 \times 1, D_3 \times 3, D_9 \times 9)$, gdje D_i označava broj orbita točaka duljine $i \in \{1, 3, 9\}$ i oznaku za distribuciju duljina G -orbita blokova $\beta = (d_1 \times 1, d_3 \times 3, d_9 \times 9)$, gdje d_i označava broj orbita blokova duljine $i \in \{1, 3, 9\}$. Osim toga, koristimo vektor $\kappa\nu$, odnosno vektor $\kappa\beta$, s informacijom o konjugiranosti stabilizatora predstavnika orbita točaka, odnosno predstavnika orbita blokova, koji imaju iste vrijednosti za one orbite točaka, odnosno blokova, čiji predstavnici imaju konjugirane stabilizatore. Prilikom određivanja vektora $\kappa\nu$ i $\kappa\beta$ posebnu pozornost potrebno je obratiti na činjenicu da stabilizator predstavnika neke G -orbite točaka (blokova) duljine tri može biti jedna od četiri (međusobno nekonjugirane) grupe reda tri $G_i < G$, $i = 1, \dots, 4$.

Promotrimo najprije fiksnu strukturu 2-(45, 5, 1) dizajna \mathcal{D} uz pretpostavku djelovanja grupe $G \cong Z_3 \times Z_3$.

Propozicija 5.1. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, te $G \leq \text{Aut}(\mathcal{D})$, $G \cong Z_3 \times Z_3$. Grupa G ne fiksira niti jednu točku i niti jedan blok dizajna \mathcal{D} .*

Dokaz. Za broj fiksnih točaka F i fiksnih blokova f pri djelovanju grupe G na dizajn \mathcal{D} vrijedi da je $F, f \in \{0, 3, 6\}$, što slijedi iz propozicije 4.2 i činjenice da je broj točaka $v = 45$ i blokova $b = 99$, dok duljine G -orbita točaka i blokova dizajna \mathcal{D} mogu poprimiti vrijednosti iz skupa $\{1, 3, 9\}$. Broj G -orbita točaka, odnosno blokova, duljine tri označimo redom sa M_3 i m_3 .

Ako je $F = 6$, onda vrijedi da je $M_3 \equiv 1 \pmod{3}$. U tom slučaju postoji podgrupa reda tri u grupi G koja je stabilizator svih točaka iz neke G -orbite točaka duljine tri i tada ta podgrupa fiksira više od šest točaka, što je nemoguće prema tvrdnji propozicije 4.2. Stoga, vrijedi $F \neq 6$. Na analogan način se može se pokazati da je $f \neq 6$.

Ako je $F = 3$, onda vrijedi da je $M_3 \equiv 2 \pmod{3}$. Osim toga, vrijedi da je $M_3 < 5$ jer u protivnom, prema Dirichletovom principu, postoji podgrupa reda tri u grupi G koja je

5.1 Djelovanje grupe $G \cong Z_3 \times Z_3$ na 2-(45, 5, 1) dizajn

stabilizator svih točaka iz barem dvije orbite točaka duljine tri i ujedno stabilizator triju fiksnih točaka, pa u tom slučaju ona fiksira barem devet točaka, što je nemoguće prema tvrdnji propozicije 4.2. Stoga, slijedi da je $M_3 = 2$ i $\nu = (3 \times 1, 2 \times 3, 4 \times 9)$. Prema lemi 2.2 svake dvije fiksne točke sadržane su u jedinstvenom fiksnom bloku, pa postoji barem jedan fiksni blok, točnije $f = 3$. U tom slučaju slijedi da je broj G -orbita blokova duljine tri jednak $m_3 \equiv 2 \pmod{3}$, pa iz istog razloga kao i za M_3 vrijedi da je $m_3 = 2$, odnosno $\beta = (3 \times 1, 2 \times 3, 10 \times 9)$. Međutim, ova se distribucija duljina G -orbita točaka ν i blokova β može eliminirati promatranjem fiksnih blokova. Stupanj svakog bloka je $k = 5$, pa je svaki fiksni blok incidentan sa svim točkama iz jedne orbite točaka duljine tri. U ovom slučaju postoje tri fiksna bloka i dvije orbite točaka duljine tri, stoga postoje dva fiksna bloka koji se sijeku u svim točkama neke orbite točaka duljine tri, što je nemoguće zbog svojstva iz leme 2.1. Stoga vrijedi $F \neq 3$. Iz istog razloga vrijedi $f \neq 3$. Iz svega navedenog slijedi tvrdnja. \square

Korolar 5.1. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, te $G \leq \text{Aut}(\mathcal{D})$, $G \cong Z_3 \times Z_3$. Za broj G -orbita točaka duljine tri s oznakom M_3 i broj G -orbita blokova duljine tri s oznakom m_3 vrijedi $M_3, m_3 \in \{0, 3, 6\}$.*

Dokaz. Prema tvrdnji propozicije 5.1 za broj G -orbita točaka, odnosno blokova, duljine tri vrijedi $M_3, m_3 \equiv 0 \pmod{3}$. Osim toga, vrijedi $M_3 \leq 6$, jer u protivnom ako je $M_3 > 6$ i $M_3 \equiv 0 \pmod{3}$ slijedi da je $M_3 \geq 9$, što znači da, prema Dirichletovom principu, postoji grupa reda tri $G_i < G$, $i = 1, \dots, 4$, koja fiksira više od šest točaka, što je nemoguće prema tvrdnji propozicije 4.2. Analogno se pokaže da za broj G -orbita blokova duljine tri vrijedi $m_3 \leq 6$. Stoga, vrijedi tvrdnja korolara. \square

U sljedeće tri leme analiziramo sva moguća djelovanja grupe G na dizajn \mathcal{D} .

Lema 5.1. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, te $G \leq \text{Aut}(\mathcal{D})$, $G \cong Z_3 \times Z_3$. Ako za broj G -orbita točaka duljine tri, u oznaci M_3 , vrijedi $M_3 = 0$, tada grupa G može djelovati na dizajn \mathcal{D} sa sljedećom distribucijom duljina orbita točaka ν i orbita blokova β i vektorima s informacijom o konjugiranosti stabilizatora predstavnika tih orbita $\kappa\nu$ i $\kappa\beta$:*

$$\begin{aligned} \nu &= (5 \times 9), \quad \kappa\nu = (5 \times 0), \\ \beta &= (11 \times 9), \quad \kappa\beta = (11 \times 0), \end{aligned} \tag{5.1}$$

Dokaz. Iz tvrdnje propozicije 5.1 i pretpostavke $M_3 = 0$, slijedi da je $\nu = (5 \times 9)$. Stabilizator predstavnika svih orbita iz distribucije ν je trivijalna grupa i vektor s informacijom o konjugiranosti stabilizatora predstavnika tih orbita je $\kappa\nu = (5 \times 0)$. Jasno je da tada niti jedna od grupa reda tri $G_i < G$, $i \in \{1, \dots, 4\}$ ne fiksira niti jednu točku (pa onda i niti jedan blok), odnosno vrijedi da je $F_i = 0$, za $i = 1, \dots, 4$.

Za broj G -orbita blokova duljine tri vrijedi $m_3 = 0$. Naime, ako postoji barem jedna G -orbita blokova duljine tri, tada postoji grupa reda tri G_i , za neki $i \in \{1, \dots, 4\}$ koja je stabilizator svih blokova iz neke G -orbite blokova duljine tri, što je nemoguće zbog činjenice da je $F_i = 0$, za $i = 1, \dots, 4$. Stoga, distribucija duljina G -orbita blokova je $\beta = (11 \times 9)$ i pripadni vektor s informacijom o konjugiranosti stabilizatora predstavnika tih orbita je $\kappa\beta = (11 \times 0)$. Time je dokazana tvrdnja. \square

Lema 5.2. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, te $G \leq \text{Aut}(\mathcal{D})$, $G \cong Z_3 \times Z_3$. Ako za broj G -orbita točaka duljine tri, u oznaci M_3 , vrijedi $M_3 = 3$, tada grupa G može djelovati na dizajn \mathcal{D} s jednom od sljedeće dvije distribucije duljina orbita točaka ν i orbita blokova β i vektorima s informacijom o konjugiranosti stabilizatora predstavnika tih orbita $\kappa\nu$ i $\kappa\beta$:*

$$\begin{aligned} \nu &= (3 \times 3, 4 \times 9), & \kappa\nu &= (2 \times 0, 1 \times 1, 4 \times 2) \\ \beta &= (3 \times 3, 10 \times 9), & \kappa\beta &= (2 \times 0, 1 \times 1, 10 \times 2), \end{aligned} \quad (5.2)$$

$$\begin{aligned} \nu &= (3 \times 3, 4 \times 9), & \kappa\nu &= (1 \times 0, 1 \times 1, 1 \times 2, 4 \times 3), \\ \beta &= (3 \times 3, 10 \times 9), & \kappa\beta &= (1 \times 0, 1 \times 1, 1 \times 2, 10 \times 3). \end{aligned} \quad (5.3)$$

Dokaz. Iz pretpostavke $M_3 = 3$ slijedi da je $\nu = (3 \times 3, 4 \times 9)$. Stabilizator svih točaka iz neke G -orbite točaka duljine tri je jedna od četiri međusobno nekonjugirane grupe reda tri $G_i < G$, za neki $i \in \{1, 2, 3, 4\}$. Niti jedna od tih grupa nije stabilizator predstavnika za sve tri G -orbite točaka duljine tri, što vrijedi prema tvrdnji propozicije 4.2. Stoga, vrijedi da ili stabilizator predstavnika dviju G -orbita točaka duljine tri je grupa G_i ili stabilizatori predstavnika svih triju G -orbita točaka su različite podgrupe reda tri u grupi G . Bez smanjenja općenitosti možemo pretpostaviti da je grupa $G_1 = \langle \phi \rangle$ stabilizator predstavnika dviju, dok je grupa $G_2 = \langle \omega \rangle$ stabilizator predstavnika treće orbite točaka duljine tri, što je prikazano u tablici 5.1. Isto tako u drugom slučaju možemo bez smanjenja općenitosti pretpostaviti da su stabilizatori predstavnika orbita točaka duljine tri redom grupe G_1, G_2 i $G_3 = \langle \phi\omega \rangle$, što je prikazano u tablici 5.2.

	O_1	O_2	O_3	# fiksnih točaka
ϕ	id	id	ϕ	6
ω	ω	ω	id	3
$\phi\omega$	ω	ω	ϕ	0
$\phi^2\omega$	ω	ω	ϕ^2	0

Tablica 5.1: Djelovanje grupe G na orbitama točaka duljine tri, O_1, O_2 i O_3 , u slučaju kada je grupa $\langle \phi \rangle$ stabilizator predstavnika prve dvije, a grupa $\langle \omega \rangle$ stabilizator predstavnika treće orbite točaka duljine tri

5.1 Djelovanje grupe $G \cong Z_3 \times Z_3$ na 2-(45, 5, 1) dizajn

	O_1	O_2	O_3	# fiksnih točaka
ϕ	id	ϕ	ϕ	3
ω	ω	id	ω	3
$\phi\omega$	ω	ϕ	id	3
$\phi^2\omega$	ω	ϕ^2	ϕ	0

Tablica 5.2: Djelovanje grupe G na orbitama točaka duljine tri, O_1 , O_2 i O_3 , u slučaju kada predstavnici nikoje dvije orbite duljine tri nemaju konjugirane stabilizatore

Promotrimo djelovanje grupe G na skupu blokova dizajna \mathcal{D} za oba dobivena djelovanja na skupu točaka. Pretpostavimo da grupa G djeluje na orbitama točaka duljine tri dizajna \mathcal{D} kao u tablici 5.1. Tada postoje dvije podgrupe reda tri u grupi G od kojih jedna fiksira šest, a druga tri bloka (u ovom slučaju $F_1 = 6$ i $F_2 = 3$), dok preostale dvije ne fiksiraju niti jedan blok. Podgrupe reda tri u grupi G koje fiksiraju barem jedan blok (u ovom slučaju G_1 i G_2), nemaju zajedničkih fiksnih blokova, prema tvrdnji propozicije 5.1. Slijedi da je $m_3 = 3$, odnosno da postoje dvije G -orbite blokova duljine tri za čije predstavnike vrijedi da im je stabilizator podgrupa reda tri u grupi G koja fiksira šest blokova (u ovom slučaju to je grupa G_1) i postoji jedna G -orbita blokova duljine tri čiji je stabilizator predstavnika podgrupa reda tri u grupi G koja fiksira tri bloka (u ovom slučaju to je grupa G_2). Prema tome, slijedi distribucija (5.2).

Pretpostavimo da grupa G djeluje na orbitama točaka duljine tri dizajna \mathcal{D} kao u tablici 5.2. Tada postoje tri podgrupe reda tri u grupi G koje fiksiraju po tri bloka (u ovom slučaju to su $F_1 = F_2 = F_3 = 3$), dok jedna ne fiksira niti jedan blok ($F_4 = 0$). Nikoje dvije od tri grupe koje fiksiraju barem jedan blok, nemaju zajedničkih fiksnih blokova, prema tvrdnji propozicije 5.1. Slijedi da je $m_3 = 3$, odnosno da postoje tri G -orbite blokova duljine tri čiji predstavnici nemaju konjugirane stabilizatore. Prema tome, slijedi distribucija (5.3). \square

Promotrimo posljednji slučaj djelovanja grupe G na dizajn \mathcal{D} .

Lema 5.3. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn, te $G \leq \text{Aut}(\mathcal{D})$, $G \cong Z_3 \times Z_3$. Ako za broj G -orbita točaka duljine tri, u oznaci M_3 , vrijedi $M_3 = 6$, tada grupa G može djelovati na dizajn \mathcal{D} s jednom od sljedeće dvije distribucije duljina orbita točaka ν i orbita blokova β i vektorima s informacijom o konjugiranosti stabilizatora predstavnika tih orbita $\kappa\nu$ i $\kappa\beta$:*

$$\begin{aligned} \nu &= (6 \times 3, 3 \times 9), & \kappa\nu &= (2 \times 0, 2 \times 1, 2 \times 2, 3 \times 3), \\ \beta &= (6 \times 3, 9 \times 9), & \kappa\beta &= (2 \times 0, 2 \times 1, 2 \times 2, 9 \times 3), \end{aligned} \quad (5.4)$$

$$\begin{aligned} \nu &= (6 \times 3, 3 \times 9), & \kappa\nu &= (2 \times 0, 2 \times 1, 1 \times 2, 1 \times 3, 3 \times 4), \\ \beta &= (6 \times 3, 9 \times 9), & \kappa\beta &= (2 \times 0, 2 \times 1, 1 \times 2, 1 \times 3, 9 \times 4). \end{aligned} \quad (5.5)$$

Dokaz. Iz pretpostavke $M_3 = 6$ slijedi da je $\nu = (6 \times 3, 3 \times 9)$. Za svaku G -orbitu točaka duljine tri postoji jedna od četiri podgrupe reda tri u grupi G koja je stabilizator svih točaka iz te orbite. Prema tvrdnji propozicije 4.2, svaka od te četiri podgrupe reda tri u grupi G može biti stabilizator svih točaka iz najviše dvije G -orbite točaka duljine tri. Stoga, grupa G može djelovati na skup točaka dizajna \mathcal{D} na jedan od sljedećih načina:

1. postoje tri grupe reda tri $G_i < G$, pri čemu je $i \in \{1, \dots, 4\}$, od kojih svaka fiksira različiti par G -orbite točaka duljine tri, kao što je bez smanjenja općenitosti prikazano u tablici 5.3,
2. sve četiri podgrupe reda tri u grupi G fiksiraju barem jednu G -orbitu točaka duljine tri, kao što je bez smanjenja općenitosti prikazano u tablici 5.4.

	O_1	O_2	O_3	O_4	O_5	O_6	# fiksnih točaka
ϕ	id	id	ϕ	ϕ	ϕ	ϕ	6
ω	ω	ω	id	id	ω	ω	6
$\phi\omega$	ω	ω	ϕ	ϕ	id	id	6
$\phi^2\omega$	ω	ω	ϕ^2	ϕ^2	ϕ	ϕ	0

Tablica 5.3: Djelovanje grupe G na orbitama točaka duljine tri, O_1, \dots, O_6 , uz pretpostavku da po dvije orbite duljine tri imaju konjugirane stabilizatore

	O_1	O_2	O_3	O_4	O_5	O_6	# fiksnih točaka
ϕ	id	id	ϕ	ϕ	ϕ	ϕ	6
ω	ω	ω	id	id	ω	ω	6
$\phi\omega$	ω	ω	ϕ	ϕ	id	$\phi\omega$	3
$\phi^2\omega$	ω	ω	ϕ^2	ϕ^2	ϕ	id	3

Tablica 5.4: Djelovanje grupe G na orbitama točaka duljine tri, O_1, \dots, O_6 , uz pretpostavku da sve četiri podgrupe reda tri u grupi G fiksiraju barem jednu orbitu duljine tri

Promotrimo djelovanje grupe G na skupu blokova dizajna \mathcal{D} za svako pojedino djelovanje na orbitama točaka duljine tri iz tablica 5.3 i 5.4.

Pretpostavimo da grupa G djeluje na orbitama točaka duljine tri kao u tablici 5.3. Tada postoje tri podgrupe reda tri u grupi G koje fiksiraju po šest blokova (u ovom slučaju $F_1 = F_2 = F_3 = 6$), dok preostala grupa reda tri ne fiksira niti jedan blok. Podgrupe reda tri u grupi G koje fiksiraju barem jedan blok nemaju zajedničkih fiksnih blokova, prema tvrdnji propozicije 5.1. Stoga, vrijedi da je $m_3 = 6$, odnosno za svaku podgrupu reda tri u grupi G koja fiksira po šest blokova postoje dvije G -orbite blokova duljine tri za čije predstavnike je ta grupa stabilizator. Prema tome, slijedi distribucija (5.4).

Pretpostavimo da grupa G djeluje na orbitama točaka duljine tri kao u tablici 5.4. Tada postoje dvije podgrupe reda tri u grupi G koje fiksiraju po šest blokova (u ovom

5.2 Konstrukcija orbitnih matrica i njihovo profinjenje

slučaju $F_1 = F_2 = 6$), dok preostale dvije podgrupe reda tri u G fiksiraju po tri bloka. Podgrupe reda tri u grupi G koje fiksiraju barem jedan blok, prema tvrdnji propozicije 5.1, nemaju zajedničkih fiksnih blokova. Stoga, $m_3 = 6$, odnosno za svaku podgrupu reda tri u grupi G koja fiksira po šest (po tri) bloka postoje dvije (jedna) G -orbita blokova duljine tri za čije predstavnike je stabilizator ta grupa. Prema tome, slijedi distribucija (5.5). \square

Napomena 5.1. Istaknimo da za djelovanje grupe G na dizajn \mathcal{D} s distribucijom (5.1) iz leme 5.1 i s distribucijom (5.2) iz leme 5.2 postoje dvije podgrupe reda tri u grupi G koje nemaju niti jednu zajedničku orbitu točaka, niti blokova duljine tri. Za preostala tri djelovanja grupe G na dizajn \mathcal{D} s distribucijom (5.3), (5.4) i (5.5) vrijedi da svake dvije podgrupe reda tri u grupi G imaju barem jednu zajedničku orbitu točaka i blokova duljine tri.

5.2 Konstrukcija orbitnih matrica i njihovo profinjenje

Nakon što su određene sve moguće distribucije duljina G -orbita točaka i blokova 2-(45, 5, 1) dizajna, te pripadni vektori $\kappa\nu$ i $\kappa\beta$, pomoću programa za konstrukciju orbitnih matrica blokovnih dizajna konstruirane su sve, do na izomorfizam, orbitne matrice za te distribucije.

Lema 5.4. *Do na izomorfizam, postoji 2858 orbitnih matrica za djelovanje grupe automorfizama $G \cong Z_3 \times Z_3$ na 2-(45, 5, 1) dizajn \mathcal{D} .*

Dokaz. U prethodnom poglavlju dobiveno je pet mogućih kandidata (5.1)-(5.5) za distribuciju ν i β , te za pripadne vektore $\kappa\nu$ i $\kappa\beta$, pri djelovanju grupe G na dizajn \mathcal{D} . Označimo tih pet distribucija brojevima 1-5. Primjenom programa za konstrukciju neizomorfni orbitnih matrica blokovnih dizajna uz pretpostavku djelovanja grupe G , konstruirane su orbitne matrice samo za prve tri distribucije iz prethodnog teorema, dok je prilikom konstrukcije orbitnih matrica za četvrtu i petu distribuciju dobiveno da ne postoji osmi redak tih matrica. Rezultati o broju neizomorfni orbitnih matrica za svako djelovanje grupe G na dizajn \mathcal{D} prikazani su u tablici 5.5. \square

Redni broj distribucije	1	2	3	4	5
# orbitnih matrica	51	563	2244	0	0

Tablica 5.5: Broj neizomorfni orbitnih matrica za distribucije orbita (5.1)-(5.5)

Na osnovu razmotrenog djelovanja grupe G na dizajn 2-(45, 5, 1) dizajn i dokaza prethodne leme slijedi tvrdnja sljedećeg teorema.

Teorem 5.1. *Neka je \mathcal{D} 2-(45, 5, 1) dizajn. Grupa $G \leq \text{Aut}(\mathcal{D})$, $G \cong Z_3 \times Z_3$, na skup točaka i blokova dizajna \mathcal{D} može djelovati s jednom od sljedeće tri distribucije duljina orbita točaka ν i orbita blokova β , te vektorima s informacijom o konjugiranosti stabilizatora predstavnika orbita $\kappa\nu$ i $\kappa\beta$:*

1. $\nu = (5 \times 9), \quad \kappa\nu = (5 \times 0)$
 $\beta = (11 \times 9), \quad \kappa\beta = (11 \times 0),$
2. $\nu = (3 \times 3, 4 \times 9) \quad \kappa\nu = (2 \times 0, 1 \times 1, 4 \times 2)$
 $\beta = (3 \times 3, 10 \times 9), \quad \kappa\beta = (2 \times 0, 1 \times 1, 10 \times 2),$
3. $\nu = (3 \times 3, 4 \times 9), \quad \kappa\nu = (1 \times 0, 1 \times 1, 1 \times 2, 4 \times 3),$
 $\beta = (3 \times 3, 10 \times 9), \quad \kappa\beta = (1 \times 0, 1 \times 1, 1 \times 2, 10 \times 3).$

Sljedeći korak u konstrukciji dizajna je profinjenje konstruiranih orbitnih matrica pomoću programa za profinjenje orbitnih matrica blokovnog dizajna. Pritom koristimo kompozicijski niz grupe $G \cong Z_3 \times Z_3$:

$$\{1\} \triangleleft G_i \triangleleft G \quad \text{za neki } i \in \{1, \dots, 4\}, \quad G_i \cong Z_3.$$

Profinjujemo dobivene orbitne matrice za djelovanje grupe G na dizajn \mathcal{D} do orbitnih matrica za djelovanje grupe $G_i \triangleleft G$, $G_i \cong Z_3$, uz pretpostavku djelovanja kvocijentne grupe $G/G_i \cong Z_3$.

Sada navodimo rezultate profinjenja orbitnih matrica iz tablice 5.5.

1. Ako grupa G djeluje na dizajn \mathcal{D} s prvom distribucijom iz teorema 5.1, onda postoji 51 neizomorfnih orbitnih matrica, prema rezultatu u tablici 5.5. Primjenom programa za profinjenje tih matrica do orbitnih matrica za djelovanje grupe $G_i \triangleleft G$, $G_i \cong Z_3$, za neki $i \in \{1, \dots, 4\}$, konstruirano je 5330 orbitnih matrica.
2. U slučaju djelovanja grupe G na dizajn \mathcal{D} s drugom distribucijom iz teorema 5.1, postoje 563 orbitne matrice, prema rezultatu u tablici 5.5. Za neki fiksni $i \in \{1, \dots, 4\}$, grupa $G_i \triangleleft G$, $G_i \cong Z_3$, je stabilizator predstavnika prvih dviju orbita točaka (blokova) duljine tri, dok je za neki fiksni $j \in \{1, \dots, 4\}$, $j \neq i$, grupa $G_j \triangleleft G$, $G_j \cong Z_3$ stabilizator predstavnika treće orbite točaka (blokova) duljine tri. Stoga, može se napraviti profinjenje konstruiranih 563 orbitnih matrica iz tablice 5.5 do orbitnih matrica za djelovanje grupe G_i i G_j posebno. Primjenom programa za profinjenje tih 563 orbitnih matrica do orbitnih matrica za djelovanje grupe G_i dobije se 3588 orbitnih matrica, dok se za djelovanje grupe G_j ne konstruira niti jedna orbitna

5.2 Konstrukcija orbitnih matrica i njihovo profinjenje

matrica. Iz tog razloga zaključujemo da grupa $G \cong Z_3 \times Z_3$ ne može djelovati na dizajn \mathcal{D} s drugom distribucijom iz teorema 5.1.

- U slučaju djelovanja grupe $G \cong Z_3 \times Z_3$ na dizajn \mathcal{D} s trećom distribucijom iz teorema 5.1, prema tablici 5.5 postoji 2244 orbitnih matrica. S obzirom da retke i stupce konstruiranih orbitnih matrica koji odgovaraju orbitama duljine tri nije bilo moguće permutirati, jer predstavnici tih orbita nemaju konjugirane stabilizatore, za provedbu profinjenja dobivenih 2244 orbitnih matrica do orbitnih matrica za djelovanje podgrupe $H \triangleleft G$, $H \cong Z_3$, dovoljno je, bez smanjenja općenitosti, napraviti profinjenje prve orbite točaka i prve orbite blokova duljine tri. Naime, profinjenja preostalih osam parova orbita točaka i blokova duljine tri svode se na profinjenje prve orbite točaka i blokova duljine tri. Primjenom programa za profinjenje, iz 2244 orbitnih matrica konstruirano je 14224 orbitnih matrica.

Dalje slijedi još jedna primjena programa za profinjenje dobivenih orbitnih matrica, odnosno indeksiranje. Indeksiranje smo proveli samo za orbitne matrice dobivene primjenom programa za profinjenje u slučaju kada grupa G djeluje na dizajn \mathcal{D} s prve dvije distribucije iz teorema 5.1 za koje postoje dvije podgrupe reda tri u grupi G koje nemaju niti jednu zajedničku orbitu točaka i blokova duljine tri. To činimo zbog previše procesorskog vremena potrebnog za indeksiranje orbitnih matrica u preostalom slučaju djelovanja grupe G na dizajn \mathcal{D} . Nakon indeksiranja potrebno je provjeriti izomorfnost dobivenih dizajna, što je napravljeno pomoću GAP paketa Design ([59]). Rezultati dobiveni za prvu distribuciju iz teorema 5.1 prikazani su u tablici 5.6. Popis predstavnika orbita blokova konstruiranih dizajna za djelovanje pune grupe automorfizama naveden je u nastavku.

Redni broj distribucije (teorem 5.1)	1
# dizajna nakon indeksiranja	39
# neizomorfnih dizajna	7

Tablica 5.6: Rezultat indeksiranja i broj neizomorfnih 2-(45, 5, 1) dizajna

Na temelju svega razmotrenog dokazana je tvrdnja sljedećeg teorema.

Teorem 5.2. *Postoji sedam, do na izomorfizam, 2-(45, 5, 1) dizajna s grupom automorfizama $G \cong Z_3 \times Z_3$ u slučaju kada dvije podgrupe reda tri u grupi G djeluju na dizajn tako da nemaju zajedničkih orbita točaka (blokova) duljine tri.*

Označimo sedam konstruiranih 2-(45, 5, 1) dizajna iz prethodnog teorema s oznakama $\mathcal{D}_1, \dots, \mathcal{D}_7$. Jedan od sedam konstruiranih 2-(45, 5, 1) dizajna ima punu grupu automorfizama reda 360 izomorfnu s grupom $(Z_{15} \times Z_3) : Q_8$. Taj dizajn izomorfan je s jednim od tri dizajna s tim parametrima koje je konstruirao V. Krčadinac u svojoj doktorskoj disertaciji [37], gdje je napravio klasifikaciju dizajna s tim parametrima uz pretpostavku djelovanja

automorfizma reda pet. Preostalih šest konstruiranih 2-(45, 5, 1) dizajna imaju međusobno izomorfne pune grupe automorfizama reda 72, koja je izomorfna s grupom $(Z_3 \times Z_3) : Q_8$. Koliko nam je poznato, ti dizajni nisu izomorfni s otprije poznatim dizajnima.

U nastavku navodimo generatore pune grupe automorfizama konstruiranih 2-(45, 5, 1) dizajna $\mathcal{D}_1, \dots, \mathcal{D}_7$ i i pripadne predstavnike orbita blokova za djelovanje te grupe.

Pune grupe automorfizama konstruiranih dizajna su:

$$\begin{aligned} Aut(\mathcal{D}_1) &\cong \langle g_1, g_2, g_3, g_4 \rangle, |Aut(\mathcal{D}_1)| = 72 \\ Aut(\mathcal{D}_2) &\cong \langle g_1, g_3, g_4, g_5 \rangle, |Aut(\mathcal{D}_2)| = 72 \\ Aut(\mathcal{D}_3) &\cong \langle g_1, g_3, g_6, g_7 \rangle, |Aut(\mathcal{D}_3)| = 72 \\ Aut(\mathcal{D}_4) &\cong \langle g_3, g_8, g_9, g_{10}, g_{11} \rangle, |Aut(\mathcal{D}_4)| = 360 \\ Aut(\mathcal{D}_5) &\cong \langle g_3, g_{12}, g_{13}, g_{14} \rangle, |Aut(\mathcal{D}_5)| = 72 \\ Aut(\mathcal{D}_6) &\cong \langle g_3, g_{15}, g_{16}, g_{17} \rangle, |Aut(\mathcal{D}_6)| = 72 \\ Aut(\mathcal{D}_7) &\cong \langle g_3, g_{18}, g_{19}, g_{20} \rangle, |Aut(\mathcal{D}_7)| = 72 \end{aligned}$$

pri čemu su generatori tih grupa sljedeći:

$$\begin{aligned} g_1 &= (1,2)(4,8)(5,7)(6,9)(10,18)(11,17)(12,16)(13,14)(19,21)(22,27)(23,26)(24,25)(28,31)(29,33) \\ &\quad (30,32)(34,35)(37,41)(38,40)(39,42)(43,45) \\ g_2 &= (1,11,2,17)(3,15)(4,13,8,14)(5,12,7,16)(6,18,9,10)(19,24,21,25)(22,26,27,23)(28,41,31,37) \\ &\quad (29,39,33,42)(30,45,32,43)(34,40,35,38)(36,44) \\ g_3 &= (1,3,2)(4,6,5)(7,9,8)(10,12,11)(13,15,14)(16,18,17)(19,21,20)(22,24,23)(25,27,26)(28,30,29) \\ &\quad (31,33,32)(34,36,35)(37,39,38)(40,42,41)(43,45,44) \\ g_4 &= (1,4,5,2)(3,7,6,8)(10,16,11,15)(13,17,18,14)(19,21,24,22)(20,27,23,25)(28,35,34,30) \\ &\quad (29,32,36,31)(37,40,44,42)(38,39,43,45) \\ g_5 &= (1,38,3,41)(2,43)(4,44,9,45)(5,42,8,37)(6,39,7,40)(10,11,16,18)(12,13,17,15)(19,35) \\ &\quad (20,33,21,30) (22,31,25,29)(23,28,27,32)(24,36,26,34) \\ g_6 &= (1,36,5,29)(2,31,4,32)(3,28,6,34)(7,30,8,35)(9,33)(10,24,11,19)(12,26)(13,20,18,23) \\ &\quad (14,27,17,25) (15,22,16,21)(37,45,44,39)(38,40,43,42) \\ g_7 &= (2,4,3,7)(5,6,9,8)(10,14,17,15)(11,18,16,12)(19,24,20,27)(22,23,26,25)(28,29,33,32) \\ &\quad (30,36,31,35)(37,41,40,39)(38,44,42,43) \\ g_8 &= (1,2)(4,8)(5,7)(6,9)(10,18)(11,17)(12,16)(14,15)(19,21)(22,27)(23,26)(24,25)(28,31)(29,33) \\ &\quad (30,32)(34,35)(37,41)(38,40)(39,42)(43,45) \\ g_9 &= (1,17,2,11)(3,13)(4,10,8,18)(5,15,7,14)(6,16,9,12)(19,27,21,22)(23,24,26,25)(28,43,31,45) \\ &\quad (29,38,33,40)(30,41,32,37)(34,39,35,42)(36,44) \\ g_{10} &= (2,4,3,7)(5,6,9,8)(10,12,17,18)(11,15,16,13)(19,24,20,27)(22,23,26,25)(28,29,33,32) \\ &\quad (30,36,31,35) (37,41,40,39)(38,44,42,43) \\ g_{11} &= (2,5,3,9)(4,8,7,6)(10,35,17,36)(11,29,16,32)(12,31,18,30)(13,33,15,28)(14,34)(19,39,20,41) \\ &\quad (21,45)(22,44,26,43)(23,38,25,42)(24,40,27,37) \\ g_{12} &= (1,2)(4,8)(5,7)(6,9)(10,18)(11,17)(12,16)(13,14)(19,21)(22,27)(23,26)(24,25)(28,30)(31,35) \\ &\quad (32,34)(33,36)(37,41)(38,40)(39,42)(43,45) \end{aligned}$$

5.2 Konstrukcija orbitnih matrica i njihovo profinjenje

$$g_{13} = (1,11,2,17)(3,15)(4,13,8,14)(5,12,7,16)(6,18,9,10)(19,24,21,25)(22,26,27,23)(28,38,30,40) \\ (29,44)(31,45,35,43)(32,41,34,37)(33,39,36,42)$$

$$g_{14} = (1,4,5,2)(3,7,6,8)(10,16,11,15)(13,17,18,14)(19,21,24,22)(20,27,23,25)(28,45,31,39) \\ (29,42,33,40)(30,38,32,43)(34,37,35,44)(36,41)$$

$$g_{15} = (1,2)(4,8)(5,7)(6,9)(10,18)(11,17)(12,16)(14,15)(19,21)(22,27)(23,26)(24,25)(28,30)(31,35) \\ (32,34)(33,36)(37,41)(38,40)(39,42)(43,45)$$

$$g_{16} = (1,17,2,11)(3,13)(4,10,8,18)(5,15,7,14)(6,16,9,12)(19,27,21,22)(23,24,26,25)(28,34,30,32) \\ (31,36,35,33)(37,38,41,40)(39,43,42,45)$$

$$g_{17} = (2,4,3,7)(5,6,9,8)(10,12,17,18)(11,15,16,13)(19,24,20,27)(22,23,26,25)(28,38,29,42)(30,45) \\ (31,44,34,43)(32,37,36,40)(33,41,35,39)$$

$$g_{18} = (1,2)(4,8)(5,7)(6,9)(10,18)(11,17)(12,16)(14,15)(19,21)(22,27)(23,26)(24,25)(28,32)(29,31) \\ (30,33)(34,35)(37,41)(38,40)(39,42)(43,45)$$

$$g_{19} = (1,15,6,17)(2,18,5,14)(3,11,4,10)(7,16,9,13)(8,12)(19,30,22,34)(20,31,24,33)(21,35,23,29) \\ (25,32)(26,36,27,28)(37,39,45,43)(38,41,44,42)$$

$$g_{20} = (1,25,7,20)(2,23,9,22)(3,21,8,27)(4,24)(5,19,6,26)(10,29,15,30)(11,36,14,32)(12,31,13,34) \\ (16,28)(17,35,18,33)(37,41,39,43)(40,42,44,45)$$

U tablici 5.7 dan je popis predstavnika orbita blokova dizajna $\mathcal{D}_1, \dots, \mathcal{D}_7$ za djelovanje pripadne pune grupe automorfizama.

Dizajn	$ Aut(\mathcal{D}) $	Predstavnici orbita blokova za djelovanje $Aut(\mathcal{D})$
\mathcal{D}_1	72	[1, 2, 11, 17, 20], [1, 5, 29, 36, 41], [1, 13, 21, 34, 45], [1, 22, 26, 38, 42]
\mathcal{D}_2	72	[1, 2, 11, 17, 20], [1, 5, 29, 36, 41], [1, 13, 21, 34, 45], [10, 21, 24, 29, 35],
\mathcal{D}_3	72	[1, 2, 11, 17, 20], [1, 5, 29, 36, 41], [1, 13, 21, 34, 45], [1, 22, 26, 38, 42]
\mathcal{D}_4	360	[1, 2, 11, 17, 20], [1, 14, 21, 34, 45]
\mathcal{D}_5	72	[1, 2, 11, 17, 20], [1, 5, 36, 38, 43], [1, 13, 21, 30, 45], [1, 22, 26, 33, 35]
\mathcal{D}_6	72	[1, 2, 11, 17, 20], [1, 5, 36, 38, 43], [1, 14, 21, 30, 45], [1, 22, 26, 33, 35]
\mathcal{D}_7	72	[1, 2, 11, 17, 20], [1, 5, 33, 38, 43], [1, 6, 26, 27, 40], [1, 14, 21, 34, 45]

Tablica 5.7: Predstavnici orbita blokova dizajna $\mathcal{D}_1, \dots, \mathcal{D}_7$

Poglavlje 6

Konstrukcija 2-(45, 5, 1) dizajna s grupom automorfizama S_3

Najmanja nekomutativna grupa ima šest elemenata i to je simetrična grupa S_3 , odnosno diedralna grupa D_3 . Ta grupa ima prezentaciju

$$G = \langle \rho, \phi \mid \phi^3 = 1, \rho^2 = 1, \rho\phi\rho = \phi^{-1} \rangle \cong Z_3 : Z_2. \quad (6.1)$$

U ovom poglavlju najprije promatramo djelovanje grupe automorfizama G na 2-(45, 5, 1) dizajn \mathcal{D} , a zatim primjenjujemo razvijene programe za konstrukciju i profinjenje orbitnih matrica kako bi u konačnici konstruirali dizajne. U ovom slučaju, za profinjenje orbitnih matrica koristimo kompozicijski niz

$$\{1\} \triangleleft \langle \phi \rangle \triangleleft G.$$

To je jedinstveni kompozicijski niz jer podgrupa $\langle \rho \rangle$ nije normalna u G .

Duljine orbita za djelovanje grupe G na skupu točaka i blokova dizajna \mathcal{D} mogu poprimiti vrijednosti iz skupa $\{1, 2, 3, 6\}$, prema korolaru 1.1.

Promotrimo na koji način grupa G djeluje na orbite duljine 2, 3 i 6. Za točku P dizajna \mathcal{D} označimo sa $\mathcal{P}_i = G.P$, $|\mathcal{P}_i| \in \{2, 3, 6\}$ za neki $i \in \{1, \dots, m\}$, pri čemu je $m \in \mathbb{N}$.

Ako vrijedi $|\mathcal{P}_i| = 2$, onda je $|G_P| = 3$. Budući da postoji samo jedna klasa konjugiranih podgrupa reda tri u grupi G , možemo pretpostaviti da je $G_P = \langle \phi \rangle$. Prema teoremu 1.6, dovoljno je promotriti djelovanje grupe G na desne susjedne klase podgrupe $\langle \phi \rangle$ u grupi G : $0 = \langle \phi \rangle$, i $1 = \langle \phi \rangle \rho$, stoga ρ na tim susjednim klasama djeluje kao permutacija $(0, 1)$. Automorfizam ϕ djeluje na sljedeći način: $0\phi = 0$, $1\phi = \langle \phi \rangle \rho\phi = \langle \phi \rangle \phi^{-1}\rho^{-1} = \langle \phi \rangle \rho^{-1} = \langle \phi \rangle \rho = 1$, što znači da je ϕ točkovni stabilizator $\langle \rho \rangle$ -orbite.

Ako vrijedi $|\mathcal{P}_i| = 3$, onda je $|G_P| = 2$. Budući da postoji samo jedna klasa konjugiranih podgrupa reda dva u grupi G , možemo pretpostaviti da je $G_P = \langle \rho \rangle$. Prema teoremu 1.6, dovoljno je promotriti djelovanje grupe G na desne susjedne klase podgrupe $\langle \rho \rangle$ u

grupi G : $0 = \langle \rho \rangle$, $1 = \langle \rho \rangle \phi$, $2 = \langle \rho \rangle \phi^2$.

To znači da ϕ na tim susjednim klasama djeluje kao permutacija $(0, 1, 2)$.

Automorfizam ρ djeluje na sljedeći način:

$$0\rho = \langle \rho \rangle \rho = 0,$$

$$1\rho = \langle \rho \rangle \phi\rho = \langle \rho \rangle \rho^{-1}\phi^{-1} = \langle \rho \rangle \phi^2 = 2,$$

$$2\rho = \langle \rho \rangle \phi^2\rho = \langle \rho \rangle \phi^{-1}\rho = \langle \rho \rangle \rho\phi = \langle \rho \rangle \phi = 1,$$

odnosno automorfizam ρ u G -orbiti duljine tri djeluje kao permutacija $(0)(1, 2)$.

Ako vrijedi $|\mathcal{P}_i| = |G.P| = 6$ za neki $i \in \{1, \dots, m\}$, $m \in \mathbb{N}$, onda je $|G_P| = 1$. Desne susjedne klase jedinične grupe su svi elementi grupe G :

$$0 = 1_G, 1 = \phi, 2 = \phi^2, 3 = \rho, 4 = \rho\phi, 5 = \rho\phi^2.$$

Stoga, automorfizam ϕ djeluje na G -orbiti duljine 6 kao permutacija $(0,1,2)(3,4,5)$, dok automorfizam ρ djeluje kao permutacija $(0,3)(1,5)(2,4)$.

Prije konstrukcije orbitnih matrica dizajna \mathcal{D} na koji djeluje grupa G , potrebno je odrediti sve moguće distribucije duljina G -orbita točaka i blokova. S obzirom da podgrupe $\langle \phi \rangle \leq G$ i $\langle \rho \rangle \leq G$ čine po jednu jednočlanu klasu konjugiranih podgrupa reda tri, odnosno dva, u grupi G jasno je da će G -orbite iz distribucije duljina točaka ν (blokova β) iste duljine imati konjugirane stabilizatore, pa je time određen i pripadni vektor $\kappa\nu$ ($\kappa\beta$).

Prema propoziciji 4.1 involutorni automorfizam dizajna \mathcal{D} može fiksirati jedan od sljedećih skupova točaka i blokova:

- 1) jednu točku i 11 blokova,
- 2) tri točke i 11 blokova,
- 3) pet točaka i 11 blokova,
- 4) sedam točaka i 13 blokova,
- 5) 13 točaka i 19 blokova,

Prema propozicij 4.2 automorfizam reda tri može djelovati na 2 -(45, 5, 1) dizajn na jedan od sljedeća tri načina:

- a) Ne fiksira niti jednu točku i niti jedan blok.
- b) Fiksira tri točke i tri bloka koji čine simetričan 2 -(3, 2, 1) dizajn.
- c) Fiksira šest točaka i šest blokova.

U nastavku koristimo oznake F_2 i f_2 za broj fiksnih točaka i blokova involutornog automorfizma, dok će F_3 i f_3 biti oznake za broj fiksnih točaka i blokova automorfizma reda tri.

a) Promotrimo najprije slučaj kada grupa automorfizama $\langle \phi \rangle$ reda tri djeluje na skupu točaka s distribucijom duljina orbita $\nu = (15 \times 3)$ i na skupu blokova s distribucijom duljina orbita $\beta = (33 \times 3)$. Na temelju analiziranog djelovanja automorfizma ρ u $\langle \phi \rangle$ -orbitama duljine tri dizajna \mathcal{D} moguće su sljedeće distribucije duljina G -orbita točaka i blokova.

1. Ako je $F_2 = 1$, onda vrijedi $f_2 = 11$. Stoga grupa G djeluje na dizajn \mathcal{D} s distribucijom duljina orbita

$$\nu = (1 \times 3, 7 \times 6), \quad \beta = (11 \times 3, 11 \times 6). \quad (6.2)$$

2. Ako je $F_2 = 3$, onda vrijedi $f_2 = 11$. Stoga grupa G djeluje na dizajn \mathcal{D} s distribucijom duljina orbita

$$\nu = (3 \times 3, 6 \times 6), \quad \beta = (11 \times 3, 11 \times 6). \quad (6.3)$$

3. Ako je $F_2 = 5$, onda vrijedi $f_2 = 11$. Stoga grupa G djeluje na dizajn \mathcal{D} s distribucijom duljina orbita

$$\nu = (5 \times 3, 5 \times 6), \quad \beta = (11 \times 3, 11 \times 6). \quad (6.4)$$

4. Ako je $F_2 = 7$, onda vrijedi $f_2 = 13$. Stoga grupa G djeluje na dizajn \mathcal{D} s distribucijom duljina orbita

$$\nu = (7 \times 3, 4 \times 6), \quad \beta = (13 \times 3, 10 \times 6). \quad (6.5)$$

5. Ako je $F_2 = 13$, onda vrijedi $f_2 = 19$. Stoga grupa G djeluje na dizajn \mathcal{D} s distribucijom duljina orbita

$$\nu = (13 \times 3, 1 \times 6), \quad \beta = (19 \times 3, 7 \times 6). \quad (6.6)$$

Nakon primjene razvijenih programa na svaku od distribucija (6.2)-(6.6) za sada su dobiveni parcijalni rezultati koji su dani u tablici 6.1. Rezultati su nepotpuni zbog memorijskog ograničenja programa GAP, (6.6).

Iz rezultata prikazanih u tablici 6.1 slijedi tvrdnja sljedeće leme.

Lema 6.1. *Neka grupa S_3 djeluje kao grupa automorfizama na 2-(45, 5, 1) dizajn tako da njezina podgrupa reda tri ne fiksira niti jednu točku. Tada S_3 može djelovati s jednom od sljedeće dvije distribucije duljina orbita:*

1. $\nu = (5 \times 3, 5 \times 6), \quad \beta = (11 \times 3, 11 \times 6),$
2. $\nu = (13 \times 3, 1 \times 6), \quad \beta = (19 \times 3, 7 \times 6).$

Distribucija duljina G -orbita	(6.2)	(6.3)	(6.4)	(6.5)	(6.6)
# orbitnih matrica za G	0	6456	13214	1620	
# orbitnih matrica nakon profinjenja	0	461	32861	55224	
# dizajna nakon indeksiranja	0	0	21	0	
# neizomorfnih dizajna	0	0	9	0	

Tablica 6.1: Djelovanje grupe G na 2-(45, 5, 1) dizajn uz pretpostavku $F_3 = 0$

b) Promotrimo slučaj kada grupa automorfizama $\langle \phi \rangle$ djeluje na dizajn \mathcal{D} s distribucijom duljina orbita $\nu = (3 \times 1, 14 \times 3)$ i $\beta = (3 \times 1, 32 \times 3)$.

Ovdje razlikujemo sljedeće slučajeve.

1. Ako je $F_2 = 1$, onda vrijedi $f_2 = 11$. Automorfizmi ρ i ϕ imaju jednu zajedničku fiksnu točku i fiksni blok. Vrijedi da je $\nu = (1 \times 1, 1 \times 2, 7 \times 6)$. Međutim, fiksni blok nije moguće konstruirati s obzirom na distribuciju ν , pa ovakvo djelovanje nije moguće.
2. Ako je $F_2 = 3$, onda vrijedi $f_2 = 11$. Automorfizmi ρ i ϕ mogu imati jednu ili tri zajedničke fiksne točke (bloka). Ako imaju tri zajedničke fiksne točke, onda je $\nu = (3 \times 1, 7 \times 6)$. U tom slučaju nije moguće konstruirati fiksni blok. Stoga, ti automorfizmi mogu imati samo jednu zajedničku fiksnu točku, pa slijedi da je $\nu = (1 \times 1, 1 \times 2, 2 \times 3, 6 \times 6)$. Iz te distribucije je jasno da automorfizmi ρ i ϕ mogu imati samo jedan zajednički fiksni blok, stoga vrijedi

$$\nu = (1 \times 1, 1 \times 2, 2 \times 3, 6 \times 6), \quad \beta = (1 \times 1, 1 \times 2, 10 \times 3, 11 \times 6). \quad (6.7)$$

3. Ako je $F_2 = 5$, onda vrijedi $f_2 = 11$. Automorfizmi ρ i ϕ mogu imati jednu ili tri zajedničke fiksne točke (bloka). Ako imaju tri zajedničke fiksne točke, onda je $\nu = (3 \times 1, 2 \times 3, 6 \times 6)$. Budući da ne postoji G -orbita duljine 2, prema lemi 2.2 grupa G mora imati barem tri fiksna bloka. To nije moguće jer postoje samo dvije G -orbite duljine 3. Stoga ti automorfizmi mogu imati samo jednu zajedničku fiksnu točku, pa slijedi da je $\nu = (1 \times 1, 1 \times 2, 4 \times 3, 5 \times 6)$. Iz te distribucije je jasno da automorfizmi ρ i ϕ mogu imati samo jedan zajednički fiksni blok, stoga vrijedi

$$\nu = (1 \times 1, 1 \times 2, 4 \times 3, 5 \times 6), \quad \beta = (1 \times 1, 1 \times 2, 10 \times 3, 11 \times 6). \quad (6.8)$$

4. Ako je $F_2 = 7$, onda vrijedi $f_2 = 13$. Automorfizmi ρ i ϕ mogu imati jednu ili tri zajedničke fiksne točke (bloka). Ako oni imaju tri zajedničke fiksne točke, onda je $\nu = (3 \times 1, 4 \times 3, 5 \times 6)$. U tom slučaju ρ i ϕ imaju tri zajednička fiksna

bloka i vrijedi

$$\nu = (3 \times 1, 4 \times 3, 5 \times 6), \quad \beta = (3 \times 1, 10 \times 3, 11 \times 6). \quad (6.9)$$

Ako ρ i ϕ imaju jednu zajedničku fiksnu točku, onda je $\nu = (1 \times 1, 1 \times 2, 6 \times 3, 4 \times 6)$. Iz te distribucije je jasno da automorfizmi ρ i ϕ mogu imati samo jedan zajednički fiksni blok, stoga vrijedi

$$\nu = (1 \times 1, 1 \times 2, 6 \times 3, 4 \times 6), \quad \beta = (1 \times 1, 1 \times 2, 12 \times 3, 10 \times 6). \quad (6.10)$$

5. Ako je $F_2 = 13$, onda vrijedi $f_2 = 19$. Automorfizmi ρ i ϕ mogu imati jednu ili tri zajedničke fiksne točke (bloka). Ako imaju tri zajedničke fiksne točke, onda je $\nu = (3 \times 1, 10 \times 3, 2 \times 6)$. U tom slučaju ρ i ϕ imaju tri zajednička fiksna bloka i vrijedi

$$\nu = (3 \times 1, 10 \times 3, 2 \times 6), \quad \beta = (3 \times 1, 16 \times 3, 8 \times 6). \quad (6.11)$$

Ako ρ i ϕ imaju jednu zajedničku fiksnu točku, onda je $\nu = (1 \times 1, 1 \times 2, 12 \times 3, 1 \times 6)$. Iz te distribucije je jasno da automorfizmi ρ i ϕ mogu imati samo jedan zajednički fiksni blok, stoga vrijedi

$$\nu = (1 \times 1, 1 \times 2, 12 \times 3, 1 \times 6), \quad \beta = (1 \times 1, 1 \times 2, 18 \times 3, 7 \times 6). \quad (6.12)$$

Nakon primjene razvijenih programa na svaku od distribucija (6.7)-(6.12) za sada su dobiveni parcijalni rezultati koji su dani u tablici 6.2. Rezultati su nepotpuni zbog memorijskog ograničenja programa GAP, (6.12).

Distribucija duljina G -orbita	(6.7)	(6.8)	(6.9)	(6.10)	(6.11)	(6.12)
# orbitnih matrica za G	5411	4889	85	258	0	
# orbitnih matrica nakon profinjenja	4	617	99	1105	0	
# dizajna nakon indeksiranja	0	0	0	0	0	

Tablica 6.2: Djelovanje grupe G na 2-(45, 5, 1) dizajn uz pretpostavku $F_3 = 3$

Iz rezultata prikazanih u tablici 6.2 slijedi tvrdnja sljedeće leme.

Lema 6.2. *Neka S_3 djeluje kao grupa automorfizama na 2-(45, 5, 1) dizajn tako da njezina podgrupa reda tri fiksira tri točke. Tada S_3 može djelovati sa sljedećom distribucijom duljina orbita:*

$$\nu = (1 \times 1, 1 \times 2, 12 \times 3, 1 \times 6), \quad \beta = (1 \times 1, 1 \times 2, 18 \times 3, 7 \times 6).$$

c) Na kraju promotrimo slučaj kada grupa automorfizama $\langle \phi \rangle$ djeluje na dizajn \mathcal{D} s distribucijom duljina orbita $\nu = (6 \times 1, 13 \times 3)$ i $\beta = (6 \times 1, 31 \times 3)$.

Ovdje razlikujemo sljedeće slučajeve.

1. Ako je $F_2 = 1$, onda vrijedi $f_2 = 11$. Automorfizmi ρ i ϕ tada nemaju zajedničkih fiksnih točaka, odnosno vrijedi da je $\nu = (3 \times 2, 1 \times 3, 6 \times 6)$. Iz te distribucije je jasno da ρ i ϕ mogu imati najviše jedan zajednički fiksni blok. Stoga, s obzirom da je $f_3 = 6$, slijedi

$$\nu = (3 \times 2, 1 \times 3, 6 \times 6), \quad \beta = (3 \times 2, 11 \times 3, 10 \times 6). \quad (6.13)$$

2. Ako je $F_2 = 3$, onda vrijedi $f_2 = 11$. Automorfizmi ρ i ϕ mogu imati nula ili dvije zajedničke fiksne točke. Ako pretpostavimo da imaju dvije zajedničke fiksne točke, onda je $\nu = (2 \times 1, 2 \times 2, 1 \times 3, 6 \times 6)$. U tom slučaju ρ i ϕ moraju imati barem jedan zajednički fiksni blok, prema lemi 2.2. Stoga iz $f_3 = 6$ i ν slijedi da ti automorfizmi imaju dva zajednička fiksna bloka, pa vrijedi

$$\nu = (2 \times 1, 2 \times 2, 1 \times 3, 6 \times 6), \quad \beta = (2 \times 1, 2 \times 2, 9 \times 3, 11 \times 6). \quad (6.14)$$

Ako pretpostavimo da ρ i ϕ nemaju zajedničkih fiksnih točaka, onda je $\nu = (3 \times 2, 3 \times 3, 5 \times 6)$. Stoga ti automorfizmi mogu imati najviše tri zajednička fiksna bloka, pa iz $f_3 = 6$ slijedi da ρ i ϕ mogu imati nula ili dva zajednička fiksna bloka. Ako pretpostavimo da oni imaju dva zajednička fiksna bloka, tada vrijedi

$$\nu = (3 \times 2, 3 \times 3, 5 \times 6), \quad \beta = (2 \times 1, 2 \times 2, 9 \times 3, 11 \times 6). \quad (6.15)$$

Ako pretpostavimo da automorfizmi ρ i ϕ nemaju zajedničkih fiksnih blokova, tada vrijedi

$$\nu = (3 \times 2, 3 \times 3, 5 \times 6), \quad \beta = (3 \times 2, 11 \times 3, 10 \times 6). \quad (6.16)$$

3. Ako je $F_2 = 5$, onda vrijedi $f_2 = 11$. Automorfizmi ρ i ϕ mogu imati nula, dvije ili četiri zajedničke fiksne točke. Ako pretpostavimo da nemaju zajedničkih fiksnih točaka, onda je $\nu = (3 \times 2, 5 \times 3, 4 \times 6)$. Iz te distribucije je jasno da ρ i ϕ mogu imati najviše tri zajednička fiksna bloka, pa grupa G može djelovati na dizajn sa jednom od sljedeće dvije distribucije duljina orbita:

$$\nu = (3 \times 2, 5 \times 3, 4 \times 6), \quad \beta = (2 \times 1, 2 \times 2, 9 \times 3, 11 \times 6), \quad (6.17)$$

$$\nu = (3 \times 2, 5 \times 3, 4 \times 6), \quad \beta = (3 \times 2, 11 \times 3, 10 \times 6). \quad (6.18)$$

Ako pretpostavimo da ρ i ϕ imaju dvije zajedničke fiksne točke, onda je $\nu = (2 \times 1, 2 \times 2, 3 \times 3, 5 \times 6)$. Iz distribucije ν , leme 2.2 i $f_3 = 6$ slijedi da ρ i ϕ imaju dva zajednička fiksna bloka, pa vrijedi

$$\nu = (2 \times 1, 2 \times 2, 3 \times 3, 5 \times 6), \quad \beta = (2 \times 1, 2 \times 2, 9 \times 3, 11 \times 6). \quad (6.19)$$

Ako pretpostavimo da ρ i ϕ imaju četiri zajedničke fiksne točke, onda je $\nu = (4 \times 1, 1 \times 2, 1 \times 3, 6 \times 6)$. Iz ν i leme 2.2 slijedi da takvo djelovanje nije moguće realizirati.

4. Ako je $F_2 = 7$, onda vrijedi $f_2 = 13$. Automorfizmi ρ i ϕ mogu imati nula, dvije, četiri ili šest zajedničkih fiksnih točaka. Ako pretpostavimo da ρ i ϕ nemaju zajedničkih fiksnih točaka, onda je $\nu = (3 \times 2, 7 \times 3, 3 \times 6)$. Iz ν i $f_3 = 6$ slijedi da ρ i ϕ mogu imati nula ili dva zajednička fiksna bloka, odnosno grupa G može djelovati na dizajn s jednom od sljedeće dvije distribucije duljina orbita:

$$\nu = (3 \times 2, 7 \times 3, 3 \times 6), \quad \beta = (3 \times 2, 13 \times 3, 9 \times 6), \quad (6.20)$$

$$\nu = (3 \times 2, 7 \times 3, 3 \times 6), \quad \beta = (2 \times 1, 2 \times 2, 11 \times 3, 10 \times 6). \quad (6.21)$$

Ako pretpostavimo da ρ i ϕ imaju dvije zajedničke fiksne točke, onda je $\nu = (2 \times 1, 2 \times 2, 5 \times 3, 4 \times 6)$. Iz ν , leme 2.2 i $f_3 = 6$ slijedi da ρ i ϕ imaju dva zajednička fiksna bloka, odnosno vrijedi

$$\nu = (2 \times 1, 2 \times 2, 5 \times 3, 4 \times 6), \quad \beta = (2 \times 1, 2 \times 2, 11 \times 3, 10 \times 6). \quad (6.22)$$

Ako ρ i ϕ imaju četiri zajedničke fiksne točke, onda je $\nu = (4 \times 1, 1 \times 2, 3 \times 3, 5 \times 6)$. Iz ν , leme 2.2 slijedi da ρ i ϕ imaju četiri zajednička fiksna bloka, odnosno vrijedi

$$\nu = (4 \times 1, 1 \times 2, 3 \times 3, 5 \times 6), \quad \beta = (4 \times 1, 1 \times 2, 9 \times 3, 11 \times 6). \quad (6.23)$$

Ako ρ i ϕ imaju šest zajedničkih fiksnih točaka, onda je $\nu = (6 \times 1, 1 \times 3, 6 \times 6)$. Iz ν slijedi da ρ i ϕ mogu imati najviše dva zajednička fiksna bloka, što nije dovoljno za formiranje fiksne strukture, prema lemi 2.2.

5. Ako je $F_2 = 13$, onda vrijedi $f_2 = 19$. Automorfizmi ρ i ϕ mogu imati nula, dvije, četiri ili šest zajedničkih fiksnih točaka. Ako pretpostavimo da ρ i ϕ nemaju zajedničkih fiksnih točaka, onda je $\nu = (3 \times 2, 13 \times 3)$. Iz ν i $f_3 = 6$ slijedi da ρ i ϕ mogu imati nula ili dva zajednička fiksna bloka, odnosno da grupa G može djelovati na dizajn s jednom od sljedeće dvije distribucije duljina orbita:

$$\nu = (3 \times 2, 13 \times 3), \quad \beta = (3 \times 2, 19 \times 3, 6 \times 6), \quad (6.24)$$

$$\nu = (3 \times 2, 13 \times 3), \quad \beta = (2 \times 1, 2 \times 2, 17 \times 3, 7 \times 6). \quad (6.25)$$

Ako pretpostavimo da ρ i ϕ imaju dvije zajedničke fiksne točke, onda je $\nu = (2 \times 1, 2 \times 2, 11 \times 3, 1 \times 6)$. Iz ν , leme 2.2 i $f_3 = 6$ slijedi da ρ i ϕ imaju dva zajednička fiksna bloka, odnosno vrijedi

$$\nu = (2 \times 1, 2 \times 2, 11 \times 3, 1 \times 6), \quad \beta = (2 \times 1, 2 \times 2, 17 \times 3, 7 \times 6). \quad (6.26)$$

Ako ρ i ϕ imaju četiri zajedničke fiksne točke, onda je $\nu = (4 \times 1, 1 \times 2, 9 \times 3, 2 \times 6)$. Tada ρ i ϕ imaju četiri ili šest zajedničkih fiksnih blokova, odnosno vrijedi

$$\nu = (4 \times 1, 1 \times 2, 9 \times 3, 2 \times 6), \quad \beta = (4 \times 1, 1 \times 2, 15 \times 3, 8 \times 6), \quad (6.27)$$

$$\nu = (4 \times 1, 1 \times 2, 9 \times 3, 2 \times 6), \quad \beta = (6 \times 1, 13 \times 3, 9 \times 6), \quad (6.28)$$

Ako ρ i ϕ imaju šest zajedničkih fiksnih točaka, onda je $\nu = (6 \times 1, 7 \times 3, 3 \times 6)$. Fiksna struktura u tom slučaju ima šest točaka i isto toliko blokova, pa vrijedi

$$\nu = (6 \times 1, 7 \times 3, 3 \times 6), \quad \beta = (6 \times 1, 13 \times 3, 9 \times 6). \quad (6.29)$$

Nakon primjene razvijenih programa na svaku od distribucija (6.13)-(6.29) dobiveni su rezultati koji su dani u tablici 6.3.

Distribucija	# orbitnih matrica	# orbitnih matrica nakon profinjenja	# dizajna
6.13	0	0	0
6.14	104	1	0
6.15	0	0	0
6.16	0	0	0
6.17	0	0	0
6.18	0	0	0
6.19	43	0	0
6.20	0	0	0
6.21	0	0	0
6.22	0	0	0
6.23	72	4	0
6.24	0	0	0
6.25	0	0	0
6.26	0	0	0
6.27	0	0	0
6.28	0	0	0
6.29	0	0	0

Tablica 6.3: Djelovanje grupe G na 2-(45, 5, 1) dizajn uz pretpostavku $F_3 = 6$

Iz leme 6.1, leme 6.2 i rezultata prikazanih u tablici 6.3 slijedi tvrdnja sljedećeg teorema.

Teorem 6.1. *Grupa S_3 može djelovati kao grupa automorfizama na 2-(45, 5, 1) dizajn s jednom od sljedeće tri distribucije duljina orbita:*

1. $\nu = (5 \times 3, 5 \times 6), \quad \beta = (11 \times 3, 11 \times 6),$
2. $\nu = (13 \times 3, 1 \times 6), \quad \beta = (19 \times 3, 7 \times 6),$
3. $\nu = (1 \times 1, 1 \times 2, 12 \times 3, 1 \times 6), \quad \beta = (1 \times 1, 1 \times 2, 18 \times 3, 7 \times 6).$

Također, iz dosadašnjih razmatranja (tablica 6.1) slijedi tvrdnja sljedećeg teorema.

Teorem 6.2. *Postoji barem devet, do na izomorfizam, 2-(45, 5, 1) dizajna na koje djeluje grupa automorfizama S_3 .*

Napomena 6.1. Sedam dizajna iz prethodnog teorema izomorfni su s dizajnama konstruiranim u poglavlju 5.2. Za preostala dva konstruirana dizajna, koje označimo sa \mathcal{D}_1 i \mathcal{D}_2 , vrijedi $Aut(\mathcal{D}_1) \cong Aut(\mathcal{D}_2) \cong S_3$. Pretpostavljamo da ti dizajni nisu poznati od ranije.

U tablici 6.4 navodimo predstavnike orbita blokova dizajna \mathcal{D}_1 i \mathcal{D}_2 za djelovanje njihove pune grupe automorfizama.

$$Aut(\mathcal{D}_1) \cong Aut(\mathcal{D}_2) \cong \langle g_1, g_2 \rangle,$$

pri čemu su g_1 i g_2 jednaki:

$$g_1 = (1,2)(4,6)(7,8)(10,11)(13,14)(16,21)(17,20)(18,19)(22,26)(23,25)(24,27)(28,32)(29,31)(30,33)(34,37)(35,39)(36,38)(40,45)(41,44)(42,43),$$

$$g_2 = (2,3)(4,5)(8,9)(11,12)(14,15)(16,20)(17,19)(18,21)(22,25)(23,27)(24,26)(28,31)(29,33)(30,32)(34,39)(35,38)(36,37)(40,44)(41,43)(42,45)$$

Dizajn	$Aut(\mathcal{D})$	Predstavnicu orbita blokova za djelovanje $Aut(\mathcal{D})$
\mathcal{D}_1	S_3	[1, 2, 5, 17, 20], [1, 6, 7, 10, 13], [1, 8, 9, 22, 25], [1, 11, 12, 28, 31], [1, 14, 26, 37, 45], [1, 18, 29, 30, 35], [1, 23, 34, 43, 44], [4, 5, 7, 35, 38], [4, 10, 18, 23, 42], [4, 13, 21, 30, 41], [4, 22, 24, 32, 39], [4, 28, 33, 40, 43], [7, 11, 22, 29, 42], [7, 14, 17, 32, 40], [7, 16, 20, 41, 43], [7, 18, 31, 34, 36], [10, 14, 15, 34, 39], [10, 16, 17, 25, 38], [10, 36, 37, 40, 44], [13, 17, 19, 23, 27], [13, 24, 26, 29, 33], [16, 23, 29, 39, 45]
\mathcal{D}_2	S_3	[1, 2, 5, 17, 20], [1, 6, 7, 10, 13], [1, 8, 9, 22, 25], [1, 11, 12, 28, 31], [1, 14, 23, 34, 41], [1, 18, 29, 30, 35], [1, 24, 36, 44, 45], [4, 5, 7, 35, 38], [4, 10, 18, 23, 42], [4, 13, 21, 30, 41], [4, 22, 24, 32, 39], [4, 28, 33, 40, 43], [7, 11, 22, 29, 42], [7, 14, 17, 32, 40], [7, 16, 20, 41, 43], [7, 18, 31, 34, 36], [10, 14, 15, 36, 37], [10, 16, 17, 25, 38], [10, 34, 39, 40, 44], [13, 17, 19, 23, 27], [13, 24, 26, 29, 33], [16, 23, 29, 39, 45]

Tablica 6.4: Predstavnicu orbita blokova dizajna \mathcal{D}_1 i \mathcal{D}_2

Poglavlje 7

Klasifikacija 2-(78, 22, 6) dizajna s grupom automorfizama $Frob_{39} \times Z_2$

Do sada su, do na izomorfizam, poznata samo tri simetrična 2-(78, 22, 6) dizajna. Prvi simetričan dizajn s parametrima 2-(78, 22, 6) konstruirali su Z. Janko i T. van Trung metodom taktičke dekompozicije ([34]). Oni su promatrali poseban slučaj kada na dizajn s tim parametrima djeluje nekomutativna grupa automorfizama reda 39, $Frob_{39} \cong Z_{13} : Z_3$, uz pretpostavku da automorfizam reda 13 ne fiksira niti jednu točku i automorfizam reda tri (skupovno) fiksira sve orbite za djelovanje automorfizma reda 13. Isto tako pokazali su da je puna grupa automorfizama konstruiranog dizajna izomorfna s grupom $Frob_{39} \times Z_2$. Nakon toga je V. D. Tonchev konstruirao dva međusobno dualna 2-(78, 22, 6) dizajna koji imaju punu grupu automorfizama izomorfnu s $E_8 : Frob_{21}$ ([62]). S. Pfaff u svojoj doktorskoj disertaciji [51] dokazuje da su, do na izomorfizam, to jedini dizajni s takvom grupom automorfizama.

U ovom poglavlju primjenjujemo računalne programe koji se temelje na razvijenom algoritmu za konstrukciju i algoritmu za profinjenje orbitnih matrica blokovnih dizajna, kako bi napravili klasifikaciju 2-(78, 22, 6) dizajna uz djelovanje grupe $Frob_{39} \times Z_2$. U ovom je slučaju algoritam za profinjenje orbitnih matrica prilagođen konkretnoj grupi automorfizama koja djeluje na dizajn sa zadanim parametrima. Pokazali smo da je dizajn koji su konstruirali Z. Janko i T. van Trung, jedini, do na izomorfizam, 2-(78, 22, 6) dizajn na koji djeluje grupa automorfizama $Frob_{39} \times Z_2$.

Osim toga, važan rezultat ovog poglavlja je i dokaz tvrdnje da ne postoji (78, 22, 6) diferencijski skup u grupi $Frob_{39} \times Z_2$, što, prema nama dostupnim podacima, nije bilo poznato od ranije.

7.1 Djelovanje grupe $Frob_{39} \times Z_2$ na 2-(78, 22, 6) dizajn

Prvi korak u konstrukciji blokovnog dizajna je analiza djelovanja odgovarajuće grupe automorfizama na taj dizajn. U ovom poglavlju promatramo na koji način grupa $Frob_{39} \times Z_2$ može djelovati na simetričan 2-(78, 22, 6) dizajn \mathcal{D} .

Kako bi analizirali djelovanje te grupe, najprije ćemo pogledati kako nekomutativna grupa automorfizama reda 39 djeluje na dizajn \mathcal{D} .

Postoji točno jedna, do na izomorfizam, nekomutativna grupa reda 39 koju označimo sa

$$G = \langle \rho, \sigma \mid \rho^{13} = \sigma^3 = 1, \rho^\sigma = \rho^3 \rangle \cong Z_{13} : Z_3 \cong Frob_{39}.$$

Promotrimo najprije djelovanje automorfizma reda 13 na dizajn \mathcal{D} .

Lema 7.1. *Neka je \mathcal{D} dizajn s parametrima 2-(78, 22, 6) i neka je ρ automorfizam dizajna \mathcal{D} reda 13. Tada ρ ne fiksira niti jednu točku i niti jedan blok dizajna \mathcal{D} .*

Dokaz. Grupa $\langle \rho \rangle$ djeluje standardno na dizajn \mathcal{D} . Broj fiksnih točaka (blokova) za djelovanje automorfizma ρ na \mathcal{D} označimo sa F . Vrijedi da je $F \equiv 0 \pmod{13}$, pa prema propoziciji 2.7 slijedi da je $F \in \{0, 13\}$. Ako je $F = 13$, onda postoji pet $\langle \rho \rangle$ -orbita točaka duljine 13. Svaki fiksni blok je incidentan s devet fiksnih točaka i sa svim točkama iz jedne $\langle \rho \rangle$ -orbite točaka duljine 13. U ovom slučaju postoje barem dva fiksna bloka koji sadrže sve točke iz iste orbite točaka duljine 13, što je nemoguće jer je $\lambda = 6$. Dakle, vrijedi da je $F = 0$. \square

Iz prethodne leme je jasno da djelovanje automorfizma ρ reda 13 na skupu točaka (blokova) dizajna \mathcal{D} možemo, bez smanjenja općenitosti, prikazati na sljedeći način

$$\rho = (I_0, I_1, \dots, I_{12}), \quad I = 1, 2, \dots, 6, \tag{7.1}$$

gdje je $\{I_j \mid I = 1, \dots, 6, j = 0, 1, \dots, 12\}$ skup od 78 točaka (blokova) dizajna \mathcal{D} .

Korolar 7.1. *Neka je \mathcal{D} 2-(78, 22, 6) dizajn. Grupa $G \leq Aut(\mathcal{D})$, $G \cong Frob_{39}$ može djelovati na skup točaka i blokova dizajna \mathcal{D} u orbitama duljine 13 ili 39.*

Dokaz. Duljine orbita na skupu točaka i blokova za djelovanje grupe $Frob_{39}$ na dizajn \mathcal{D} mogu poprimiti vrijednosti iz skupa $\{1, 3, 13, 39\}$, prema tvrdnji korolara 1.1. Ako postoji orbita točaka (blokova) duljine 1 ili 3 za djelovanje grupe $Frob_{39}$ na dizajn \mathcal{D} , to znači da automorfizam reda 13 fiksira barem jednu točku (blok), što je u kontradikciji s tvrdnjom leme 7.1. Stoga, vrijedi tvrdnja korolara. \square

U nastavku koristimo oznaku G za grupu $G \leq Aut(\mathcal{D})$, $G \cong Frob_{39}$.

Grupa G djeluje polustandardno na dizajn \mathcal{D} . Naime, prema tvrdnji korolara 7.1 i činjenici da σ preslikava $\langle \rho \rangle$ -orbite na $\langle \rho \rangle$ -orbite, postoje sljedeće tri mogućnosti za distribuciju duljina G -orbita na skupu točaka i blokova dizajna \mathcal{D}

$$\nu^1 = (13, 13, 13, 13, 13, 13), \quad \nu^2 = (13, 13, 13, 39), \quad \nu^3 = (39, 39). \quad (7.2)$$

Razmotrimo kako grupa G djeluje na orbitama $\mathcal{P}_i = G.P$, $|\mathcal{P}_i| \in \{13, 39\}$, gdje je P točka dizajna \mathcal{D} i $i \in \{1, \dots, m\}$, $m \in \mathbb{N}$.

1. Neka je $|\mathcal{P}_i| = 13$, tada je $|G_P| = 3$. Budući da postoji samo jedna klasa konjugiranih podgrupa reda tri u grupi G , možemo pretpostaviti da je $G_P = \langle \sigma \rangle$. Prema teoremu 1.6, dovoljno je promotriti djelovanje grupe G na desne susjedne klase podgrupe $\langle \sigma \rangle$ u grupi G :

$$0 = \langle \sigma \rangle, \quad 1 = \langle \sigma \rangle \rho, \quad 2 = \langle \sigma \rangle \rho^2, \quad 3 = \langle \sigma \rangle \rho^3, \quad 4 = \langle \sigma \rangle \rho^4, \quad 5 = \langle \sigma \rangle \rho^5, \quad 6 = \langle \sigma \rangle \rho^6, \\ 7 = \langle \sigma \rangle \rho^7, \quad 8 = \langle \sigma \rangle \rho^8, \quad 9 = \langle \sigma \rangle \rho^9, \quad 10 = \langle \sigma \rangle \rho^{10}, \quad 11 = \langle \sigma \rangle \rho^{11}, \quad 12 = \langle \sigma \rangle \rho^{12}.$$

To znači da ρ na tim susjednim klasama djeluje kao permutacija $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$.

Automorfizam σ djeluje na sljedeći način:

$$0\sigma = \langle \sigma \rangle \sigma = \langle \sigma \rangle = 0, \\ 1\sigma = \langle \sigma \rangle \rho \sigma = \langle \sigma \rangle \sigma \rho^3 = \langle \sigma \rangle \rho^3 = 3, \\ 2\sigma = \langle \sigma \rangle \rho^2 \sigma = \langle \sigma \rangle \rho \sigma \rho^3 = \langle \sigma \rangle \sigma \rho^6 = 6, \\ 3\sigma = \langle \sigma \rangle \rho^3 \sigma = \langle \sigma \rangle \rho^2 \sigma \rho^3 = \langle \sigma \rangle \rho \sigma \rho^6 = \langle \sigma \rangle \sigma \rho^9 = \langle \sigma \rangle \rho^9 = 9, \\ 4\sigma = \langle \sigma \rangle \rho^4 \sigma = \dots = 12, \\ 5\sigma = \langle \sigma \rangle \rho^5 \sigma = \dots = 2, \\ 6\sigma = \langle \sigma \rangle \rho^6 \sigma = \dots = 5, \\ 7\sigma = \langle \sigma \rangle \rho^7 \sigma = \dots = 8, \\ 8\sigma = \langle \sigma \rangle \rho^8 \sigma = \dots = 11, \\ 9\sigma = \langle \sigma \rangle \rho^9 \sigma = \dots = 1, \\ 10\sigma = \langle \sigma \rangle \rho^{10} \sigma = \dots = 4, \\ 11\sigma = \langle \sigma \rangle \rho^{11} \sigma = \dots = 7, \\ 12\sigma = \langle \sigma \rangle \rho^{12} \sigma = \dots = 10,$$

odnosno automorfizam σ na G -orbiti duljine 13 djeluje kao permutacija

$$(0)(1, 3, 9)(2, 6, 5)(4, 12, 10)(7, 8, 11). \quad (7.3)$$

2. Neka je $|\mathcal{P}_i| = 39$, tada je $|G_P| = 1$. Desne susjedne klase trivijalne grupe u grupi G su svi elementi grupe G :

$$0 = 1, \quad 1 = \rho, \quad 2 = \rho^2, \quad 3 = \rho^3, \quad 4 = \rho^4, \quad 5 = \rho^5, \quad 6 = \rho^6, \\ 7 = \rho^7, \quad 8 = \rho^8, \quad 9 = \rho^9, \quad 10 = \rho^{10}, \quad 11 = \rho^{11}, \quad 12 = \rho^{12}, \\ 13 = \sigma, \quad 14 = \sigma \rho, \quad 15 = \sigma \rho^2, \quad 16 = \sigma \rho^3, \quad 17 = \sigma \rho^4, \quad 18 = \sigma \rho^5,$$

7.1 Djelovanje grupe $Frob_{39} \times Z_2$ na 2-(78, 22, 6) dizajn

$$19 = \sigma\rho^6, 20 = \sigma\rho^7, 21 = \sigma\rho^8, 22 = \sigma\rho^9, 23 = \sigma\rho^{10}, 24 = \sigma\rho^{11}, 25 = \sigma\rho^{12}, \\ 26 = \sigma^2, 27 = \sigma^2\rho, 28 = \sigma^2\rho^2, 29 = \sigma^2\rho^3, 30 = \sigma^2\rho^4, 31 = \sigma^2\rho^5, 32 = \sigma^2\rho^6, \\ 33 = \sigma^2\rho^7, 34 = \sigma^2\rho^8, 35 = \sigma^2\rho^9, 36 = \sigma^2\rho^{10}, 37 = \sigma^2\rho^{11}, 38 = \sigma^2\rho^{12}.$$

To znači da ρ na tim susjednim klasama djeluje kao permutacija
 $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)(13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25)$
 $(26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38)$.

Automorfizam σ djeluje na sljedeći način:

$$0\sigma = \sigma = 13, \\ 1\sigma = \rho\sigma = \sigma\rho^3 = 16, \\ 2\sigma = \rho^2\sigma = \rho\sigma\rho^3 = \sigma\rho^6 = 19, \\ 3\sigma = 22, 4\sigma = 25, 5\sigma = 15, 6\sigma = 18, 7\sigma = 21, 8\sigma = 24, 9\sigma = 14, 10\sigma = 17, \\ 11\sigma = 20, 12\sigma = 23, 13\sigma = 26, 14\sigma = 29, 15\sigma = 32, 16\sigma = 35, 17\sigma = 38, \\ 18\sigma = 28, 19\sigma = 31, 20\sigma = 34, 21\sigma = 37, 22\sigma = 27, 23\sigma = 30, 24\sigma = 33, \\ 25\sigma = 36, 26\sigma = 0, 27\sigma = 3, 28\sigma = 6, 29\sigma = 9, 30\sigma = 12, 31\sigma = 2, \\ 32\sigma = 5, 33\sigma = 8, 34\sigma = 11, 35\sigma = 1, 36\sigma = 4, 37\sigma = 7, 38\sigma = 10, \\ \text{odnosno automorfizam } \sigma \text{ na } G\text{-orbiti duljine 39 djeluje kao permutacija} \\ (0, 13, 26)(1, 16, 35)(2, 19, 31)(3, 22, 27)(4, 25, 36)(5, 15, 32)(6, 18, 28) \\ (7, 21, 37)(8, 24, 33)(9, 14, 29)(10, 17, 38)(11, 20, 34)(12, 23, 30).$$

Svako djelovanje grupe G na orbitama točaka duljine 13 i 39 permutacijski je izomorfno upravo navedenim djelovanjima. Analogno bi se moglo pokazati da tvrdnja vrijedi i za G -orbite blokova duljine 13 i 39.

Ako grupa G djeluje na dizajn \mathcal{D} s distribucijom $\nu^1 = (13, 13, 13, 13, 13, 13)$ iz (7.2), tada automorfizam σ reda tri fiksira šest točaka (blokova) i skupovno fiksira svaku orbitu duljine 13, prema (7.3). U tom slučaju djelovanje automorfizma σ u svakoj $\langle\rho\rangle$ -orbiti duljine 13 možemo, bez smanjenja općenitosti, zapisati na sljedeći način (u skladu s oznakom djelovanja automorfizma ρ (7.1)):

$$\sigma = (I_0)(I_1, I_3, I_9)(I_2, I_6, I_5)(I_4, I_{12}, I_{10})(I_7, I_8, I_{11}), \quad I = 1, 2, \dots, 6, \quad (7.4)$$

gdje je $\{I_j \mid I = 1, \dots, 6, j = 0, 1, \dots, 12\}$ skup od 78 točaka (blokova) dizajna \mathcal{D} , a za indekse vrijedi $j \rightarrow 3j \pmod{13}$.

Ako grupa G djeluje na dizajn \mathcal{D} s distribucijom duljina orbita $\nu^2 = (13, 13, 13, 39)$ iz (7.2), tada automorfizam σ reda tri fiksira tri točke (bloka) i skupovno fiksira svaku orbitu duljine 13, dok za djelovanje grupe G s distribucijom $\nu^3 = (39, 39)$ iz (7.2) automorfizam σ ne fiksira niti jednu točku (blok), što je vidljivo iz ranije analiziranog djelovanja grupe G na orbitama duljine 13 i 39.

Promotrimo djelovanje grupe

$$H = \langle \rho, \sigma, \mu \mid \rho^{13} = \sigma^3 = \mu^2 = 1, \rho^\sigma = \rho^3, \rho^\mu = \rho, \sigma^\mu = \sigma \rangle \cong Frob_{39} \times Z_2$$

na simetričan 2-(78, 22, 6) dizajn \mathcal{D} , $H \leq Aut(\mathcal{D})$.

Grupa H djeluje polustandardno na dizajn \mathcal{D} . Duljine orbita na skupu točaka i skupu blokova dobivenih djelovanjem grupe H na dizajn \mathcal{D} mogu poprimiti vrijednosti iz skupa $\{13, 26, 39, 78\}$, prema tvrdnji korolara 1.1 i korolara 7.1. Involutori automorfizam μ komutira s automorfizmima ρ i σ , stoga slijedi da automorfizam μ može djelovati u H -orbiti točaka duljine 39 samo tako da fiksira sve točke, što je nemoguće zbog propozicije 2.7. Stoga, duljine H -orbita točaka i blokova dizajna \mathcal{D} mogu poprimiti vrijednosti iz skupa $\{13, 26, 78\}$.

Prema tvrdnji leme 7.1, automorfizam ρ ne fiksira niti jednu točku i niti jedan blok dizajna \mathcal{D} . Stoga, djelovanje automorfizma ρ na skupu točaka (blokova) dizajna \mathcal{D} možemo definirati kao u (7.1).

Ako pretpostavimo da postoji H -orbita točaka (blokova) duljine 13, tada broj takvih orbita može biti 2, 4 ili 6. Involutori automorfizam μ fiksira najviše 26 točaka (blokova), prema propoziciji 2.7. Automorfizmi μ i ρ komutiraju, odakle slijedi da μ djeluje na svaku $\langle \rho \rangle$ -orbitu tako da fiksira sve elemente te orbite. Stoga, broj H -orbita duljine 13 ne može biti veći od dva, pa je u ovom slučaju distribucija duljina H -orbita točaka (blokova) upravo sljedeća

$$\nu = (13, 13, 26, 26). \tag{7.5}$$

Naime, involutori automorfizam μ u ovom slučaju fiksira 26 točaka (blokova), odnosno fiksira sve točke (blokove) iz dvije H -orbite točaka (blokova) duljine 13.

Prema ranije analiziranom djelovanju automorfizma σ reda tri na $\langle \rho \rangle$ -orbiti duljine 13, automorfizam σ u svakoj takvoj orbiti fiksira po jednu točku (blok). Stoga, djelovanje od σ na H -orbitama duljine 13 možemo, bez smanjenja općenitosti, zapisati u obliku (u skladu s djelovanjem ρ iz (7.1)):

$$\sigma = (I_0)(I_1, I_3, I_9)(I_2, I_6, I_5)(I_4, I_{12}, I_{10})(I_7, I_8, I_{11}), \quad I = 1, 2.$$

Promotrimo na koji način grupa H djeluje u orbiti duljine 26.

Neka je P točka dizajna \mathcal{D} i $\mathcal{P}_i = H.P$, $|\mathcal{P}_i| = 26$, za neki $i \in \{1, \dots, m\}$, $m \in \mathbb{N}$. Vrijedi da je $|H_P| = 3$. Budući da postoji samo jedna klasa konjugiranih podgrupa reda tri u grupi H , možemo pretpostaviti da je $H_P = \langle \sigma \rangle$. Prema teoremu 1.6, dovoljno je promotriti djelovanje grupe H na desne susjedne klase podgrupe $\langle \sigma \rangle$ u grupi H :

$$\begin{aligned} 0 &= \langle \sigma \rangle, & 1 &= \langle \sigma \rangle \rho, & 2 &= \langle \sigma \rangle \rho^2, & 3 &= \langle \sigma \rangle \rho^3, & 4 &= \langle \sigma \rangle \rho^4, & 5 &= \langle \sigma \rangle \rho^5, & 6 &= \langle \sigma \rangle \rho^6, \\ 7 &= \langle \sigma \rangle \rho^7, & 8 &= \langle \sigma \rangle \rho^8, & 9 &= \langle \sigma \rangle \rho^9, & 10 &= \langle \sigma \rangle \rho^{10}, & 11 &= \langle \sigma \rangle \rho^{11}, & 12 &= \langle \sigma \rangle \rho^{12}, \end{aligned}$$

7.1 Djelovanje grupe $Frob_{39} \times Z_2$ na 2-(78, 22, 6) dizajn

$13 = \langle \sigma \rangle \mu$, $14 = \langle \sigma \rangle \mu\rho$, $15 = \langle \sigma \rangle \mu\rho^2$, $16 = \langle \sigma \rangle \mu\rho^3$, $17 = \langle \sigma \rangle \mu\rho^4$, $18 = \langle \sigma \rangle \mu\rho^5$,
 $19 = \langle \sigma \rangle \mu\rho^6$, $20 = \langle \sigma \rangle \mu\rho^7$, $21 = \langle \sigma \rangle \mu\rho^8$, $22 = \langle \sigma \rangle \mu\rho^9$, $23 = \langle \sigma \rangle \mu\rho^{10}$, $24 = \langle \sigma \rangle \mu\rho^{11}$,
 $25 = \langle \sigma \rangle \mu\rho^{12}$.

To znači da ρ na tim susjednim klasama djeluje kao permutacija
 $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)(13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25)$.

Automorfizam σ djeluje na sljedeći način:

$0\sigma = \langle \sigma \rangle \sigma = \langle \sigma \rangle = 0$,
 $1\sigma = \langle \sigma \rangle \rho\sigma = \langle \sigma \rangle \sigma\rho^3 = 3$,
 $2\sigma = \langle \sigma \rangle \rho^2\sigma = \langle \sigma \rangle \rho\sigma\rho^3 = \langle \sigma \rangle \sigma\rho^6 = 6$,
 $3\sigma = 9$, $4\sigma = 12$, $5\sigma = 2$, $6\sigma = 5$, $7\sigma = 8$, $8\sigma = 11$, $9\sigma = 1$, $10\sigma = 4$,
 $11\sigma = 7$, $12\sigma = 10$, $13\sigma = 13$, $14\sigma = 16$, $15\sigma = 19$, $16\sigma = 22$, $17\sigma = 25$,
 $18\sigma = 15$, $19\sigma = 18$, $20\sigma = 21$, $21\sigma = 24$, $22\sigma = 14$, $23\sigma = 17$, $24\sigma = 20$,
 $25\sigma = 23$,

odnosno automorfizam σ na H -orbiti duljine 26 djeluje kao permutacija
 $(0)(13)(1, 3, 9)(2, 6, 5)(4, 12, 10)(7, 8, 11)(14, 16, 22)(15, 19, 18)(17, 25, 23)(20, 21, 24)$.

Involutorni automorfizam μ djeluje na sljedeći način:

$0\mu = \langle \sigma \rangle \mu = 13$,
 $1\mu = \langle \sigma \rangle \rho\mu = \langle \sigma \rangle \mu\rho = 14$,
 \vdots
 $25\mu = \langle \sigma \rangle \mu\rho^{12}\mu = \langle \sigma \rangle \rho^{12} = 12$,

odakle slijedi da djelovanje involutornog automorfizma na orbiti duljine 26 možemo pisati kao niz transpozicija $(i, i + 13)$, $i = 0, \dots, 12$.

Svako djelovanje grupe H na orbitama točaka duljine 26 permutacijski je izomorfno upravo navedenim djelovanjima. Analogno bi se moglo pokazati da tvrdnja vrijedi i za H -orbite blokova duljine 26.

Na temelju razmotrenog djelovanja grupe H na dizajn \mathcal{D} s distribucijom duljina orbita točaka (blokova) $\nu = (13, 13, 26, 26)$, djelovanje automorfizma ρ na skupu točaka (blokova) dizajna \mathcal{D} možemo zapisati kao u (7.1). U skladu s distribucijom ν i djelovanjem automorfizma ρ , možemo djelovanje od σ i μ na skupu točaka (blokova) dizajna \mathcal{D} prikazati na sljedeći način

$$\sigma = (I_0)(I_1, I_3, I_9)(I_2, I_6, I_5)(I_4, I_{12}, I_{10})(I_7, I_8, I_{11}), \quad I = 1, \dots, 6, \quad (7.6)$$

$$\mu = (1_j)(2_j)(3_j, 4_j)(5_j, 6_j), \quad j = 0, 1, \dots, 12. \quad (7.7)$$

Ako pak pretpostavimo da grupa H ne djeluje na skupu točaka i blokova dizajna \mathcal{D} u orbitama duljine 13, to znači da involutorni automorfizam μ ne fiksira niti jednu

točku (blok). Stoga, djelovanje od μ na skupu točaka (blokova) dizajna \mathcal{D} možemo, bez smanjenja općenitosti, definirati ovako:

$$\mu = (1_j, 2_j)(3_j, 4_j)(5_j, 6_j), \quad j = 0, 1, \dots, 12. \quad (7.8)$$

Ovdje razlikujemo sljedeća dva načina djelovanja automorfizma σ na skupu točaka (blokova) dizajna \mathcal{D} .

1. Automorfizam σ fiksira šest točaka (blokova), odnosno po jednu točku (blok) u svakoj $\langle \rho \rangle$ -orbiti i skupovno fiksira svaku $\langle \rho \rangle$ -orbitu točaka. U tom slučaju možemo, bez smanjenja općenitosti, pretpostaviti da je djelovanje od σ na skupu točaka (blokova) dizajna \mathcal{D} dano kao u (7.6). Stoga, grupa H djeluje na dizajn \mathcal{D} sa sljedećom distribucijom duljina orbita točaka (blokova)

$$\nu = (26, 26, 26). \quad (7.9)$$

2. Ako automorfizam σ ne fiksira niti jednu točku (blok) dizajna \mathcal{D} , tada grupa H djeluje regularno na skupu točaka i blokova dizajna \mathcal{D} . Za takvo djelovanje je jasno da grupa H djeluje na skupu točaka i blokova dizajna \mathcal{D} u jednoj orbiti duljine 78, odnosno

$$\nu = (78). \quad (7.10)$$

Razmotrimo kako grupa H djeluje u orbiti duljine 78.

Neka je P proizvoljna točka dizajna \mathcal{D} . Tada je $\mathcal{P} = H.P$ i $|H_P| = 1$.

Desne susjedne klase trivijalne grupe u grupi H su svi elementi grupe H koje možemo označiti na sljedeći način:

$$\begin{aligned} 0 &= 1, \quad 1 = \rho, \quad 2 = \rho^2, \quad 3 = \rho^3, \quad 4 = \rho^4, \quad 5 = \rho^5, \quad 6 = \rho^6, \\ 7 &= \rho^7, \quad 8 = \rho^8, \quad 9 = \rho^9, \quad 10 = \rho^{10}, \quad 11 = \rho^{11}, \quad 12 = \rho^{12}, \\ 13 &= \sigma, \quad 14 = \sigma\rho, \quad 15 = \sigma\rho^2, \quad 16 = \sigma\rho^3, \quad 17 = \sigma\rho^4, \quad 18 = \sigma\rho^5, \quad 19 = \sigma\rho^6, \\ 20 &= \sigma\rho^7, \quad 21 = \sigma\rho^8, \quad 22 = \sigma\rho^9, \quad 23 = \sigma\rho^{10}, \quad 24 = \sigma\rho^{11}, \quad 25 = \sigma\rho^{12}, \quad 26 = \sigma^2, \\ 27 &= \sigma^2\rho, \quad 28 = \sigma^2\rho^2, \quad 29 = \sigma^2\rho^3, \quad 30 = \sigma^2\rho^4, \quad 31 = \sigma^2\rho^5, \quad 32 = \sigma^2\rho^6, \\ 33 &= \sigma^2\rho^7, \quad 34 = \sigma^2\rho^8, \quad 35 = \sigma^2\rho^9, \quad 36 = \sigma^2\rho^{10}, \quad 37 = \sigma^2\rho^{11}, \quad 38 = \sigma^2\rho^{12}, \\ 39 &= \mu, \quad 40 = \mu\rho, \quad 41 = \mu\rho^2, \quad 42 = \mu\rho^3, \quad 43 = \mu\rho^4, \quad 44 = \mu\rho^5, \quad 45 = \mu\rho^6, \\ 46 &= \mu\rho^7, \quad 47 = \mu\rho^8, \quad 48 = \mu\rho^9, \quad 49 = \mu\rho^{10}, \quad 50 = \mu\rho^{11}, \quad 51 = \mu\rho^{12}, \\ 52 &= \mu\sigma, \quad 53 = \mu\sigma\rho, \quad 54 = \mu\sigma\rho^2, \quad 55 = \mu\sigma\rho^3, \quad 56 = \mu\sigma\rho^4, \quad 57 = \mu\sigma\rho^5, \quad 58 = \mu\sigma\rho^6, \\ 59 &= \mu\sigma\rho^7, \quad 60 = \mu\sigma\rho^8, \quad 61 = \mu\sigma\rho^9, \quad 62 = \mu\sigma\rho^{10}, \quad 63 = \mu\sigma\rho^{11}, \quad 64 = \mu\sigma\rho^{12}, \\ 65 &= \mu\sigma^2, \quad 66 = \mu\sigma^2\rho, \quad 67 = \mu\sigma^2\rho^2, \quad 68 = \mu\sigma^2\rho^3, \quad 69 = \mu\sigma^2\rho^4, \quad 70 = \mu\sigma^2\rho^5, \\ 71 &= \mu\sigma^2\rho^6, \quad 72 = \mu\sigma^2\rho^7, \quad 73 = \mu\sigma^2\rho^8, \quad 74 = \mu\sigma^2\rho^9, \quad 75 = \mu\sigma^2\rho^{10}, \quad 76 = \mu\sigma^2\rho^{11}, \\ 77 &= \mu\sigma^2\rho^{12}. \end{aligned}$$

To znači da ρ na tim susjednim klasama djeluje kao permutacija

(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)(13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25)
 (26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38)
 (39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51)
 (52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64)
 (65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77).

Stoga, bez smanjenja općenitost možemo pretpostaviti da je djelovanje automorfizma ρ na skupu točaka dizajna \mathcal{D} određeno kao u (7.1).

Automorfizam σ djeluje na sljedeći način:

$$\begin{aligned} 0\sigma &= 1\sigma = 13, \\ 1\sigma &= \rho\sigma = \sigma\rho^3 = 16, \\ 2\sigma &= \rho^2\sigma = \rho\sigma\rho^3 = \sigma\rho^6 = 19, \\ 3\sigma &= \rho^3\sigma = \rho\sigma\rho^6 = \sigma\rho^9 = 22, \\ 4\sigma &= 25, \quad 5\sigma = 15, \quad 6\sigma = 18, \text{ itd.} \end{aligned}$$

odnosno automorfizam σ na H -orbiti duljine 78 djeluje kao permutacija
 (0, 13, 26)(1, 16, 35)(2, 19, 31)(3, 22, 27)(4, 25, 36)(5, 15, 32)(6, 18, 28)(7, 21, 37)
 (8, 24, 33)(9, 14, 29)(10, 17, 38)(11, 20, 34)(12, 23, 30)(39, 52, 65)(40, 55, 74)
 (41, 58, 70)(42, 61, 66)(43, 64, 75)(44, 54, 71)(45, 57, 67)(46, 60, 76)(47, 63, 72)
 (48, 53, 68)(49, 56, 77)(50, 59, 73)(51, 62, 69).

Involutorni automorfizam μ djeluje na sljedeći način:

$$\begin{aligned} 0\mu &= 1\mu = \mu = 39, \\ 1\mu &= \rho\mu = \mu\rho = 40, \\ &\vdots \\ 77\mu &= \mu\sigma^2\rho^{12}\mu = \sigma^2\rho^{12} = 38, \end{aligned}$$

odnosno djelovanje involutornog automorfizma na orbiti duljine 78 možemo pisati kao niz transpozicija $(i, i + 39)$, $i = 0, \dots, 38$.

U ovom je slučaju svako djelovanje grupe H na skupu točaka dizajna \mathcal{D} permutacijski izomorfno navedenim djelovanjima.

Analogno bi se moglo pokazati da tvrdnja vrijedi i za djelovanje grupe H na skupu blokova tog dizajna.

U skladu s djelovanjem automorfizma ρ (7.1), možemo, bez smanjenja općenitosti, definirati djelovanje automorfizama σ i μ na skupu točaka (blokova) dizajna \mathcal{D} na sljedeći način

$$\sigma = (1_i, 2_{3i}, 3_{9i})(4_i, 5_{3i}, 6_{9i}), \quad i = 0, \dots, 12 \quad (7.11)$$

$$\mu = (1_i, 4_i)(2_i, 5_i)(3_i, 6_i), \quad i = 0, \dots, 12. \quad (7.12)$$

Napomena 7.1. Na temelju provedene analize zaključujemo da grupa H na 2-(78, 22, 6) dizajn \mathcal{D} , $H \leq Aut(\mathcal{D})$, može djelovati s jednom od sljedeće tri distribucije duljina orbita točaka i blokova:

1. $\nu = (13, 13, 26, 26)$, gdje automorfizmi σ i μ fiksiraju šest točaka (blokova), odnosno 26 točaka (blokova),
2. $\nu = (26, 26, 26)$, gdje automorfizmi σ i μ fiksiraju šest točaka (blokova), odnosno niti jednu točku (blok),
3. $\nu = (78)$, gdje grupa H djeluje regularno na dizajn \mathcal{D} , pri čemu automorfizmi σ i μ ne fiksiraju niti jednu točku (blok) tog dizajna.

7.2 Konstrukcija orbitnih matrica i njihovo profinjenje

U napomeni 7.1 istaknuto je da grupa $H \cong Frob_{39} \times Z_2$ može djelovati na 2-(78, 22, 6) dizajn s tri moguće distribucije. Sljedeći korak u konstrukciji dizajna je konstrukcija orbitnih matrica za odgovarajuće distribucije orbita.

Algoritam za profinjenje orbitnih matrica blokovnih dizajna, opisan u poglavlju 3.3.1, ovdje je prilagođen za dizajn \mathcal{D} i grupu $G \leq Aut(\mathcal{D})$,

$$G = \langle \rho, \sigma, \mu \mid \rho^p = \sigma^q = \mu^t = 1, \rho^\sigma = \rho^k, \rho^\mu = \rho, \sigma^\mu = \sigma \rangle \cong Frob_{p \cdot q} \times Z_t,$$

za p, q i t proste brojeve, $t \neq p, t \neq q$, te $(p, q(k-1)) = 1$, $0 \leq k < p$ i $k^q \equiv 1 \pmod{p}$.

Taj modificirani algoritam temelji se na primjeni glavnog niza grupe G :

$$\{1\} \triangleleft \langle \mu \rangle \triangleleft \langle \rho, \mu \rangle \triangleleft G, \text{ odnosno } \{1\} \triangleleft Z_t \triangleleft Z_{p \cdot t} \triangleleft Frob_{p \cdot q} \times Z_t,$$

pri čemu se u svakom koraku vodi računa o djelovanju cijele grupe G na dizajn.

Za profinjenje orbitnih matrica dobivenih djelovanjem grupe G na dizajn \mathcal{D} , iz algoritma Z. Janka ([33]) preuzet je način korištenja stabilizatora predstavnika orbita točaka, kao što to koristi D. Crnković u [13], što znatno smanjuje broj mogućnosti prilikom određivanja tih predstavnika i time skraćuje vrijeme potrebno za konstrukciju dizajna. Naime, prilikom izgradnje i -tog retka točkovne orbitne matrice, za neki $i \in \{1, \dots, m\}$, nećemo dodavati sve mogućnosti za taj redak koje zadovoljavaju uvjete iz definicije točkovne orbitne matrice. Naime, ukoliko je duljina orbite točaka \mathcal{P}_i jednaka p ili $p \cdot t$, tada određivanjem podgrupe grupe G koja je stabilizator predstavnika te orbite smanjujemo

broj mogućnosti za odgovarajuće elemente u profinjenoj matrici. U G -orbitama točaka duljine p , stabilizator svake točke konjugiran je s grupom $\langle \sigma, \mu \rangle \cong Z_{q \cdot t}$, dok je u G -orbitama duljine $p \cdot t$ stabilizator svake točke konjugiran s grupom $\langle \sigma \rangle \cong Z_q$, gdje djelovanje od σ i μ na orbitama duljine p i $p \cdot t$ određujemo slično kao što je prikazano u poglavlju 7.1 za djelovanje grupe $Frob_{39} \times Z_2$ na orbitama duljine 13 i 26. Iz tog se razloga u svakoj G -orbiti točaka duljine p , odnosno $p \cdot t$, nalazi točka za koju vrijedi da je stabilizator upravo grupa $\langle \sigma, \mu \rangle$, odnosno $\langle \sigma \rangle$ i tu točku uzimamo za predstavnika pripadne orbite.

Neka je $\nu_i = p$ iz distribucije duljina G -orbita točaka ν , za neki $i \in \{1, \dots, m\}$, te neka je $\beta_j \in \{p, p \cdot t\}$ iz distribucije duljina G -orbita blokova β , za neki $j \in \{1, \dots, n\}$.

Ako je $\beta_j = p$, tada automorfizam μ fiksira sve elemente j -te G -orbite blokova, zbog toga što ρ i μ komutiraju. Stoga, grupa $\langle \sigma \rangle$ djeluje na skupu od p blokova iz j -te orbite u jednoj orbiti duljine jedan i $\frac{p-1}{q}$ orbita duljine q , pa za element točkovne orbitne matrice $a_{i,j}$ pri djelovanju grupe G , vrijedi

$$a_{i,j} \equiv 0, 1 \pmod{q}. \quad (7.13)$$

Ako je $\beta_j = p \cdot t$, tada vrijedi

$$a_{i,j} \equiv 0, t \pmod{q} \quad \text{i} \quad a_{i,j} \equiv 0 \pmod{t}. \quad (7.14)$$

Uvjet (7.13) vrijedi i za one elemente $a_{i,j}$ za koje je $\nu_i = p \cdot t$ i $\beta_j = p$.

U nastavku ovog poglavlja oznaka H predstavlja grupu

$$H = \langle \rho, \sigma, \mu \mid \rho^{13} = \sigma^3 = \mu^2 = 1, \rho^\sigma = \rho^3, \rho^\mu = \rho, \sigma^\mu = \sigma \rangle \cong Frob_{39} \times Z_2,$$

dok je \mathcal{D} oznaka za simetrični 2-(78, 22, 6) dizajn.

Najprije pretpostavimo da grupa H djeluje kao grupa automorfizama na skupu točaka i blokova dizajna \mathcal{D} s prvom distribucijom iz napomene 7.1,

$$\nu = (13, 13, 26, 26).$$

Za takvo djelovanje postoji jedan, do na izomorfizam, 2-(78, 22, 6) dizajn kojeg su konstruirali Z. Janko i T. van Trung u [34]. Oni su takav dizajn konstruirali na način da su pretpostavili djelovanje nekomutativne grupe reda 39 s distribucijom duljina orbita (13,13,13,13,13,13) na skupu točaka i blokova dizajna i zatim su pokazali da je puna grupa automorfizama konstruiranog dizajna izomorfna s grupom $Frob_{39} \times Z_2$.

Pokažimo u nastavku kako dolazimo do istog rezultata primjenom, u sklopu ovog rada, razvijenih programa.

Bez smanjenja općenitosti, automorfizme ρ, σ i μ možemo definirati redom kao u

(7.1), (7.6) i (7.7). Primjenom programa za konstrukciju orbitnih matrica blokovnih dizajna, dobili smo četiri tipa za retke točkovne orbitne matrice dizajna \mathcal{D} na koji djeluje grupa H . Dobiveni predstavnici dani su u tablici 7.1. Uzimamo da je predstavnik orbite

Redni broj	Duljina orbite	Predstavnik tipa
1	13	7 3 6 6
2	13	5 1 10 6
3	26	5 5 6 6
4	26	3 3 10 6

Tablica 7.1: Predstavnici tipova orbita točkova za djelovanje grupe H na 2-(78, 22, 6) dizajn s distribucijom duljina orbita (13,13,26,26)

točkova duljine 13 ona točka čiji je stabilizator grupa $\langle \sigma, \mu \rangle$, dok za predstavnika orbite točkova duljine 26 uzimamo onu točku čiji je stabilizator grupa $\langle \sigma \rangle$. Samo tipovi 1 i 4 iz tablice 7.1 zadovoljavaju svojstva (7.13) i (7.14). Predstavnici H -orbita jednakih duljina iz distribucije ν imaju konjugirane stabilizatore, pa možemo uzeti da je $\kappa\nu = \kappa\beta = (0, 0, 1, 1)$. Primjenom programa za konstrukciju orbitnih matrica utvrđeno je da postoji jedna, do na izomorfizam, orbitna matrica 2-(78, 22, 6) dizajna za djelovanje grupe H s distribucijom duljina orbita (13,13,26,26), s oznakom OM:

OM	13	13	26	26
13	7	3	6	6
13	3	7	6	6
26	3	3	10	6
26	3	3	6	10

Profinjenje dobivene orbitne matrice OM provodimo primjenom glavnog niza grupe H , $1 \triangleleft \langle \mu \rangle \triangleleft \langle \rho, \mu \rangle \triangleleft H \cong Frob_{39} \times Z_2$. Budući da je distribucija duljina orbita za djelovanje grupe $\langle \rho, \mu \rangle$ na dizajn \mathcal{D} jednaka distribuciji duljina H -orbita, orbitna matrica OM ujedno je i orbitna matrica za djelovanje grupe $\langle \rho, \mu \rangle$.

Vodeći računa o djelovanju cijele grupe H profinjujemo matricu OM kako bismo dobili orbitne matrice za djelovanje grupe $\langle \mu \rangle$ na dizajn. Pritom se svaka orbita duljine 13, odnosno duljine 26, profinjuje na 13 orbita duljine 1, odnosno duljine 2, prema teoremu 1.8. Za redukciju broja izomorfnih orbitnih matrica prilikom profinjenja orbitne matrice OM koristimo automorfizme te orbitne matrice i sljedeće tri permutacije α_l , $l = 2, 4, 7$,

$$\alpha_l(I_i) = I_j, \quad \text{gdje je } j \equiv (l \cdot i) \pmod{13}, \quad i = 0, \dots, 12, \quad I = 1, \dots, 6 \quad (7.15)$$

koje su sadržane u normalizatoru grupe H u $S = S(\mathcal{P}) \times S(\mathcal{B})$ i posebno u centralizatoru grupe $\langle \sigma \rangle$ u S , jer vrijedi $\rho^{\alpha_l} = \rho^l$, $\sigma^{\alpha_l} = \sigma$ i $\mu^{\alpha_l} = \mu$ za $l = 2, 4, 7$. Time se tijekom konstrukcije eliminiraju orbitne matrice koje se djelovanjem tih permutacija mogu prevesti

	OM ₁	OM ₂	OM ₃	OM ₄
# dizajna	0	0	1	1

Tablica 7.3: Broj konstruiranih 2-(78, 22, 6) dizajna

Na temelju svega navedenog, slijedi tvrdnja sljedeće leme.

Lema 7.2. *Postoji jedan, do na izomorfizam, 2-(78, 22, 6) dizajn \mathcal{D} na koji polustandardno djeluje grupa automorfizama $H \cong Frob_{39} \times Z_2$ s distribucijom duljina orbita točaka i blokova (13, 13, 26, 26). Puna grupa automorfizama $Aut(\mathcal{D})$ izomorfna je s grupom $Frob_{39} \times Z_2$.*

Napomena 7.2. Dizajn \mathcal{D} iz prethodne leme izomorfan je s dizajnom konstruiranim u [34].

$Aut(\mathcal{D}) \cong \langle h_1, h_2, h_3 \rangle$, pri čemu su generatori:

$$\begin{aligned}
 h_1 = & (1,2,3,4,5,6,7,8,9,10,11,12,13) (14,15,16,17,18,19,20,21,22,23,24,25,26) \\
 & (27,29,31,33,35,37,39,41,43,45,47,49,51) (28, 30, 32, 34,36,38,40,42,44,46,48,50,52) \\
 & (53,55,57,59,61,63,65,67,69,71,73,75,77) (54,56,58,60,62,64,66,68,70,72,74,76,78), \\
 h_2 = & (2,4,10) (3,7,6) (5,13,11) (8,9,12) (15,17,23) (16,20,19)(18,26,24) (21,22,25) \\
 & (29,33,45) (30,34,46) (31,39,37) (32,40,38) (35,51,47) (36,52,48) (41,43,49) (42,44,50) \\
 & (55,59,71) (56,60,72) (57,65,63) (58,66,64) (61,77,73) (62,78,74) (67,69,75) (68,70,76), \\
 h_3 = & (27,28) (29,30) (31,32) (33,34) (35,36) (37,38) (39,40) (41,42) (43,44) (45,46) \\
 & (47,48) (49,50) (51,52) (53,54) (55,56) (57,58) (59,60) (61,62) (63,64) (65,66) (67,68) \\
 & (69,70) (71,72) (73,74) (75,76) (77,78)
 \end{aligned}$$

U tablici 7.4 navodimo predstavnike orbita blokova za djelovanje pune grupe automorfizama na dizajn \mathcal{D} .

Dizajn	Predstavnici orbita blokova
\mathcal{D}	$[1, 2, 3, 5, 6, 11, 12, 16, 18, 24, 33, 34, 39, 40, 41, 42, 57, 58, 61, 62, 73, 74],$ $[1, 2, 5, 16, 21, 23, 27, 29, 35, 44, 50, 52, 53, 55, 60, 61, 64, 65, 69, 74, 75, 77]$ $[1, 3, 8, 14, 16, 17, 18, 20, 21, 26, 27, 28, 31, 32, 41, 42, 63, 64, 69, 70, 71, 72],$ $[1, 3, 8, 15, 24, 25, 29, 33, 36, 37, 40, 43, 45, 47, 49, 52, 55, 64, 70, 72, 73, 75]$

Tablica 7.4: Predstavnici orbita blokova dizajna \mathcal{D} za djelovanje $Aut(\mathcal{D})$

Sada pretpostavimo da grupa $H = \langle \rho, \sigma, \mu \mid \rho^{13} = \sigma^3 = \mu^2 = 1, \rho^\sigma = \rho^3 \rangle \cong Frob_{39} \times Z_2$ djeluje kao grupa automorfizama na dizajn \mathcal{D} s drugom distribucijom iz napomene 7.1, odnosno da je

$$\nu = (26, 26, 26).$$

Bez smanjenja općenitosti, automorfizme ρ, σ i μ možemo definirati redom kao u (7.1), (7.6) i (7.12). Za predstavnika H -orbite točaka uzimamo onu točku čiji je stabilizator

U ovom slučaju, bez smanjenja općenitosti, djelovanje automorfizma ρ na skupu točaka i blokova dizajna \mathcal{D} možemo definirati kao u (7.1), a djelovanje automorfizama σ i μ na dizajn \mathcal{D} možemo definirati redom kao u (7.11) i (7.12).

Najprije profinjenje provodimo za djelovanje grupe $\langle \rho, \mu \rangle$ uzimajući u obzir djelovanje kvocijentne grupe $H / \langle \rho, \mu \rangle \cong \langle \sigma \rangle$. Pritom se H -orbita duljine 78 profinjuje na tri orbite duljine 26. Primjenom programa za profinjenje, iz polazne matrice OM' konstruirana je jedna, do na izomorfizam, orbitna matrica za djelovanje grupe $\langle \rho, \mu \rangle$ na dizajn, koja odgovara matrici OS.

Sljedeći korak je profinjenje orbitne matrice OS do orbitnih matrica za djelovanje grupe $\langle \mu \rangle$ vodeći računa o djelovanju grupe $\langle \rho, \sigma \rangle$. Ovdje je djelovanje grupe $\langle \rho, \sigma \rangle$ drugačije nego u prethodnim slučajevima, pa profinjenje orbitne matrice OS provodimo na drugačiji način. Zbog tranzitivnog djelovanja grupe H na 2-(78, 22, 6) dizajn, dovoljno je odrediti sve moguće kandidate samo za prvi redak orbitne matrice dobivene profinjenjem matrice OS, odnosno za prvu $\langle \mu \rangle$ -orbitu točaka duljine 2 dobivenu profinjenjem prve H -orbite točaka iz distribucije ν . Preostalih 38 redaka orbitne matrice dobivene profinjenjem jednoznačno je određeno djelovanjem grupe $\langle \rho, \sigma \rangle$ na dizajn \mathcal{D} .

Za redukciju broja izomorfnih orbitnih matrica prilikom profinjenja matrice OS, koristimo automorfizme te matrice koji ne narušavaju djelovanje grupe $\langle \rho, \sigma \rangle$ na $\langle \mu \rangle$ -orbitama. Osim toga, za redukciju koristimo i permutacije α_l , $l = 2, \dots, 12$:

$$\alpha_l(I_i) = I_j, \quad \text{gdje je } j \equiv (l \cdot i) \pmod{13}, \quad i = 0, \dots, 12, \quad I = 1, \dots, 6,$$

za koje vrijedi $\rho^{\alpha_l} = \rho^l$, $\sigma^{\alpha_l} = \sigma$, $\mu^{\alpha_l} = \mu$, odnosno koje su elementi normalizatora grupe H u S .

Profinjenjem matrice OS nije dobivena niti jedna orbitna matrica za djelovanje grupe $\langle \mu \rangle$.

Iz leme 7.2 i svega navedenog slijedi tvrdnja sljedećeg teorema.

Teorem 7.1. *Postoji jedan, do na izomorfizam, 2-(78, 22, 6) dizajn \mathcal{D} uz pretpostavku djelovanja grupe $H \cong Frob_{39} \times Z_2$ na dizajn \mathcal{D} kao grupe automorfizama. Grupa H djeluje polustandardno na dizajn \mathcal{D} s distribucijom duljina orbita (13, 13, 26, 26) i vrijedi $H \cong Aut(\mathcal{D})$.*

U ovom poglavlju utvrdili smo da ne postoji 2-(78, 22, 6) dizajn na koji grupa $Frob_{39} \times Z_2$ djeluje regularno kao grupa automorfizama. Stoga, prema teoremu 2.8, vrijedi tvrdnja sljedećeg teorema.

Teorem 7.2. *Ne postoji (78, 22, 6) diferencijski skup u grupi $Frob_{39} \times Z_2$.*

Poglavlje 8

Nepotpuna potraga za dizajnama primjenom genetskog algoritma

Heurističke metode (tabu search, hill-climbing, simulated annealing, genetski algoritam) su prikladne za rješavanje niza kombinatoričkih optimizacijskih problema. Primjena heurističkih metoda je prikladnija za veće probleme, kada metode direktne i iscrpne pretrage ne daju rezultate ili ne daju dovoljno rezultata u razumnom vremenu. Nema garancije da će heuristički algoritmi pronaći optimalno rješenje, međutim odlika dobrih heurističkih algoritama je da često puta pronalaze optimalna ili dovoljno dobre aproksimacije optimalnih rješenja. Neki od primjera primjene heurističkih metoda prilikom konstrukcije dizajna su opisani u [9],[37],[43],[44] i [48].

Genetski algoritam se pokazao kao korisna metoda za rješavanje raznih optimizacijskih NP-teških problema. To je heuristička metoda za optimizaciju i pretraživanje, koja za razliku od ostalih heurističkih metoda, koristi populaciju i utemeljena je na evolucijskom procesu. U svakom se koraku genetskog algoritma nastoji optimizirati populacija koja se sastoji od jedinki (kromosoma) koje predstavljaju moguće optimalno rješenje. U svakoj iteraciji odabire se odgovarajući broj najbolje rangiranih jedinki (roditelji) na temelju vrijednosti funkcije cilja i tako odabrani roditelji sudjeluju u križanju. Križanjem njihovih gena proizvode se nove jedinke (djeca) koje zamjenjuju lošije rangirane jedinke u populaciji i time osiguravaju konvergenciju k lokalnom optimumu. Na jedinke (djecu) dobivene križanjem djeluje mutacija koja ima funkciju "izlaska" iz lokalnog optimuma. U svakoj iteraciji dobiva se nova generacija, odnosno populacija jedinki i proces se ponavlja sve dok ne nastupi odgovarajući uvjet za prekid.

U ovom poglavlju opisat ćemo modificirane genetske algoritme za traženje unitala i drugih poddizajna, pretraživanjem matrica incidencije (simetričnih) blokovnih dizajna. Prvi dio ovog poglavlja odnosi se na rezultate dobivene u članku [16], dok se drugi dio odnosi na ispitivanje postoje li još neki, osim poznatih, 2 -(11, 5, 2) poddizajni u simetričnim 2 -(66, 26, 10) dizajnama konstruiranim u [19]. Primjena modificiranog genetskog algoritma u potrazi za odgovarajućim poddizajnama u blokovnom dizajnu s proizvoljnim

parametrima omogućuje brži dolazak do odgovora na pitanje o egzistenciji tih struktura za razliku od metode iscrpne potrage, u slučajevima kada ona ima veliku vremensku složenost.

8.1 Modificirani genetski algoritam (MGU) za traženje unitala u simetričnim dizajnama

U ovom poglavlju opisujemo razvijeni modificirani genetski algoritam (MGU) za traženje unitala u simetričnim dizajnama. Razvili smo modificirani genetski algoritam koji parcijalno mijenja populaciju, što je varijacija genetskog algoritma danog u [65]. Radi se o genetskom algoritmu sa 4-turnirskom selekcijom i križanjem s dvije točke. U svakoj turnirskoj selekciji od po četiri jedinke generiraju se dvije nove jedinke (djeca) koje zamjenjuju dvije najlošije rangirane jedinke tog turnira. Algoritam ima kao ulazne parametre matricu incidencije simetričnog dizajna, veličinu populacije i veličinu turnira, s tim da veličina populacija mora biti djeljiva s veličinom turnira.

Neka je \mathcal{D} simetričan $2-(v, k, \lambda)$ dizajn i M njegova $b \times v$ matrica incidencije. Broj točaka unitala \mathcal{U} u dizajnu \mathcal{D} označimo sa u . Svaku jedinku u populaciji prezentiramo kao $b \times u$ matricu koja je dobivena odabirom odgovarajućih u stupaca iz matrice M , koje nazivamo genima. Broj jedinki u populaciji označimo sa POP. Početna populacija je generirana proizvoljnim odabirom, odnosno jedinke su formirane proizvoljnim odabirom u stupaca matrice M . Na temelju definicije 2.27, jedinka je unital ako je svaka njegova točka incidentna sa $k - 1$ sekanti i jednom tangentom.

Funkcija cilja (fitnes funkcija) mjeri odstupanje jedinke od svojstva iz definicije 2.27. Označimo broj tangenti i sekanti kroz točku $p_i \in \mathcal{U}$ redom sa t_i i s_i , za $1 \leq i \leq u$. Vrijednost funkcije cilja neke jedinke definiramo kao sumu prosječne vrijednosti odstupanja od odgovarajućeg broja sekanti i tangenti u svakoj točki (genu) jedinke. Označimo skup svih jedinki u populaciji sa X i definiramo funkciju cilja $c : X \rightarrow \mathbb{R}_0^+$,

$$c(x) = \frac{\sum_{i=1}^u |t_i - 1|}{u} + \frac{\sum_{i=1}^u |s_i - (k - 1)|}{u}, \quad \forall x \in X. \quad (8.1)$$

Minimalna (optimalna) vrijednost funkcije cilja c je nula i ako je ona dosegnuta, pronađen je unital.

4-turnirska selekcija jedinki realizirana je odabirom četiri susjedne jedinke. Prije tog odabira, poredak jedinki se mijenja primjenom proizvoljne permutacije s ciljem da susjedne jedinke iz prethodne iteracije ne ostaju i dalje susjedne, što daje bolje rezultate nakon križanja gena. Zatim se odabiru dvije najbolje rangirane jedinke (roditelji), od njih četiri u turniru, čiji se geni križaju pomoću dvije točke. Točnije, proizvoljno se odabiru dva

8.1 Modificirani genetski algoritam (MGU) za traženje unitala u simetričnim dizajnama

stupca (gena) x i y , $1 \leq x \leq y \leq u$, u nizu gena roditelja kao točke križanja. Geni koje nasljeđuju nove jedinke (djeca) su kopije roditeljskih gena na odgovarajućim pozicijama, kao što je prikazano u sljedećem primjeru za unital u simetričnom 2-(66, 26, 10) dizajnu, pri čemu je svaka jedinka prezentirana nizom točaka, odnosno nizom indeksa stupaca matrice incidencije tog dizajna.

$$\left[\begin{array}{cccc|cccc} 1 & 2 & 3 & 5 & 10 & 18 & 29 & 31 & 42 & 53 & 66 \end{array} \right] \textit{ roditelj 1}$$

$$\left[\begin{array}{cccc|cccc} 2 & 4 & 6 & 10 & 16 & 25 & 31 & 38 & 51 & 61 & 65 \end{array} \right] \textit{ roditelj 2}$$

$$\left[\begin{array}{cccc|cccc} 1 & 2 & 3 & 5 & 16 & 25 & 31 & 38 & 42 & 53 & 66 \end{array} \right] \textit{ dijete 1}$$

$$\left[\begin{array}{cccc|cccc} 2 & 4 & 6 & 10 & 10 & 18 & 29 & 31 & 51 & 61 & 65 \end{array} \right] \textit{ dijete 2}$$

Na dvije nove jedinke dobivene križanjem djeluje operator provjere koji provjerava ima li ponovljenih gena u jedinki i u tom slučaju ponovljeni gen se zamjenjuje novim, proizvoljno odabranim, genom koji nije prisutan u nizu gena te jedinke.

Kako bi se osigurala raznovrsnost jedinki u populaciji, odnosno što manji broj ponavljanja najbolje rangiranih jedinki, za odabrane roditelje u turniru provjerava se jesu li jednaki i u tom se slučaju, jedan se roditelj zamjenjuje proizvoljno odabranom jedinkom. Operatori mutacije djeluju na oba djeteta s jednakom vjerojatnosti p_m , što je utvrđeno na temelju nekoliko eksperimentalnih postupaka. Jednom djetetu mutira se jedan gen, a drugom dva gena, proizvoljnim odabirom. Mutirana djeca zamjenjuju dvije najlošije rangirane jedinke u turniru. U cilju bolje efikasnosti algoritma, napravili smo i mutaciju na roditeljima tako da se proizvoljno odabere jedan gen i zamijeni novim. Novi gen je proizvoljno odabrani stupac matrice incidencije M koji već nije sadržan u nizu gena tog roditelja. Taj postupak se ponavlja 5 puta na prvom i 4 puta na drugom roditelju, što je utvrđeno kao optimalan broj na temelju nekoliko eksperimenata. Nedovoljan broj mutiranih gena povećava vjerojatnost da će algoritam "zaglaviti" na skoro optimalnom rješenju (lokalni minimum koji nije globalni). Stoga, takvo rješenje (jedinka) treba niz promjena u svojim genima. Mutirani roditelj zamjenjuje prethodnog ako ima vrijednost funkcije cilja manju od prethodnog (očuvanje elitizma). Na kraju se svakoj jedinki u novoj generaciji određuje vrijednost funkcije cilja i algoritam se ponovno pokreće na toj generaciji ukoliko unital nije pronađen ili ako nije pokrenut mehanizam za resetiranje. Mehanizam za resetiranje se pokreće kada je prisutna stagnacija u poboljšanju najbolje vrijednosti funkcije cilja nakon formiranja nekoliko novih generacija. Naime, postoje dva mehanizma za resetiranje. Jedan mehanizam resetiranja realizira se tako da se očuva određeni postotak ($f\%$) najbolje rangiranih jedinki u trenutnoj populaciji, dok su ostale

jedinke zamijenjene na proizvoljan način. Drugi mehanizam resetiranja u potpunosti resetira populaciju i nastupa ako se nakon prvog mehanizma za resetiranje i dalje nastavlja stagnacija najbolje vrijednosti funkcije cilja.

Slijedi pseudokod razvijenog algoritma.

Modificirani genetski algoritam za traženje unitala u simetričnom dizajnu

```
1:  $POP \leftarrow$  veličina populacije
2: for  $POP$  #generiranje početne populacije
3:  $P \leftarrow P \cup \{\text{nova proizvoljna jedinka}\}$ 
4: end
5:  $c \leftarrow 0$  # broj iteracija
6: for svaku jedinku  $P_i \in P$ 
7:  $f_i \leftarrow$  Funkcija cilja( $P_i$ )
8: end
9:  $Best \leftarrow \min(f_i)$ 
10: while  $Best > 0$ 
11:  $P \leftarrow$  promjena pozicija jedinki u trenutnoj populaciji
12:  $i \leftarrow 1$ 
13: while  $i < POP$ 
14:  $P_a, P_b \leftarrow$  odabir dviju naboljih jedinki u razmaku od  $i$ -te i  $(i + 3)$ -te jedinke
15: if  $P_a == P_b$ 
16:  $P_b \leftarrow$  nova proizvoljna jedinka
17: Djeca  $C_a, C_b \leftarrow$  Križanje2Točke(Kopija( $P_a$ ), Kopija( $P_b$ ))
18:  $C_a, C_b \leftarrow$  ProvjeraPonavljanja( $C_a, C_b$ ) #zamjena ponovljenih stupaca
19:  $C_a \leftarrow$  Mutacija( $C_a$ ),  $C_b \leftarrow$  Mutacija( $C_b$ )
20:  $P_c, P_d \leftarrow C_a, C_b$  # zamjena dvije preostale jedinke u turniru
21:  $MP_a \leftarrow$  Mutacija( $P_a$ ),  $MP_b \leftarrow$  Mutacija( $P_b$ )
22: if Funkcija cilja( $MP_a$ ) < Funkcija cilja( $P_a$ )
23:  $P_a \leftarrow MP_a$ 
24: end
25: if Funkcija cilja( $MP_b$ ) < Funkcija cilja( $P_b$ )
26:  $P_b \leftarrow MP_b$ 
27: end
28:  $i \leftarrow i + 4$ 
29: end
30: for za svaku jedinku  $P_i \in P$ 
31:  $f_i \leftarrow$  Funkcija cilja( $P_i$ )
32: end
33:  $c \leftarrow c + 1$ 
```

8.1 Modificirani genetski algoritam (MGU) za traženje unitala u simetričnim dizajnim

```

34: Best ← min( $f_i$ )
35: if postoji stagnacija u najboljoj vrijednosti funkcije cilja
36:  $P$  ← Resetiranje( $P$ )
37: end
38: end

```

Koristimo modificirani genetski algoritam jer za razliku od klasičnog genetskog algoritma, radimo samo na jednoj populaciji i tako koristimo dvostruko manje memorije. Osim toga, primjena definiranih mutacija i operatora provjere ponavljanja istih jedinki omogućuje izbjegavanje višestrukog ponavljanja najbolje rangiranih jedinki koje zbog elitizma ostaju očuvane kroz generacije i time algoritam ulazi u rizik zastoja u lokalnom minimumu koji nije globalni.

Poznato je barem 590 međusobno neizomorfnih simetričnih 2-(66,26,10) dizajna ([19], [47], [50], [64]). D. Crnković i S. Rukavina dokazali su u članku [19] da postoje tri, do na izomorfizam, simetrična 2-(66, 26, 10) dizajna na koje djeluje grupa $G \cong FroB_{55}$ i to s distribucijom duljina orbita točaka i blokova (11, 55). Označimo te dizajne sa \mathcal{D}_1 , \mathcal{D}_2 i \mathcal{D}_3 . Za jedan od njih, recimo dizajn \mathcal{D}_3 , isti su autori dokazali da je to jedini, do na izomorfizam, simetričan 2-(66, 26, 10) dizajn na koji djeluje grupa G s distribucijom duljina orbita točaka i blokova (11, 11, 11, 11, 11, 11). Njegova orbitna matrica za takvo djelovanje grupe automorfizama je (detalji su u [19]):

OM	11	11	11	11	11	11
11	1	5	5	5	5	5
11	5	5	5	5	5	1
11	5	5	5	5	1	5
11	5	5	5	1	5	5
11	5	5	1	5	5	5
11	5	1	5	5	5	5

Dizajn \mathcal{D}_3 izomorfan je s prvim dizajnom koji je konstruiran s tim parametrima uopće, a konstruirao ga je T. van Trung ([64]). Unital u simetričnom 2-(66, 26, 10) dizajnu je blokovni dizajn s parametrima 2-(11, 5, 10). Broj neizomorfnih 2-(11, 5, 10) dizajna je barem 10^4 , što je ustanovio V. Krčadinac u [37] primjenom algoritma lokalne potrage za blokovnim dizajnim (*tabu search*). Na temelju načina konstrukcije dizajna \mathcal{D}_1 , \mathcal{D}_2 i \mathcal{D}_3 jasno je da svaki od njih sadrži barem šest unitala koji sadrže sve točke iz orbite točaka duljine 11. U primjeru 2.4 pokazano je da u 2-(66, 26, 10) dizajnu \mathcal{D}_3 postoji barem šest unitala. Nove unitale u tim simetričnim dizajnim vrlo je teško pronaći direktnim pretraživanjem zbog prevelikog broja mogućnosti koje treba obraditi, a u ovom slučaju on iznosi $\binom{66}{11}$. Pomoću opisanog genetskog algoritma pronašli smo 11 novih unitala u dizajnu \mathcal{D}_3 i dani su rezultati u tablici 8.1.

Unital	Indeksi stupaca matrice incidencije dizajna \mathcal{D}_3										
U_1	1	2	3	4	5	6	7	8	9	10	11
U_2	12	13	14	15	16	17	18	19	20	21	22
U_3	23	24	25	26	27	28	29	30	31	32	33
U_4	34	35	36	37	38	39	40	41	42	43	44
U_5	45	46	47	48	49	50	51	52	53	54	55
U_6	56	57	58	59	60	61	62	63	64	65	66
U_7	1	2	3	7	9	10	20	31	42	53	64
U_8	1	2	4	5	6	10	12	23	34	45	56
U_9	1	2	6	8	9	11	19	30	41	52	63
U_{10}	1	3	4	5	9	11	22	33	44	55	66
U_{11}	1	3	4	6	7	8	14	25	36	47	58
U_{12}	1	5	7	8	10	11	18	29	40	51	62
U_{13}	2	3	4	8	10	11	21	32	43	54	65
U_{14}	2	3	5	6	7	11	13	24	35	46	57
U_{15}	2	4	5	7	8	9	15	26	37	48	59
U_{16}	3	5	6	8	9	10	16	27	38	49	60
U_{17}	4	6	7	9	10	11	17	28	39	50	61

Tablica 8.1: Unitali u 2-(66,26,10) dizajnu \mathcal{D}_3 dobiveni primjenom MGU

Podaci o međusobnoj izomorfности unitala iz tablice 8.1 i redovima njihovih punih grupa automorfizama dobiveni su pomocu paketa Design ([59]). Podaci su prikazani u tablici 8.2.

Izomorfni unitali u \mathcal{D}_3	$ Aut(\mathcal{D}) $	$Aut(\mathcal{D})$
U_1	660	$PSL(2,11)$
$U_2 \cong U_3 \cong \dots \cong U_6$	55	$Z_{11} : Z_5$
$U_7 \cong U_8 \cong \dots \cong U_{17}$	100	$D_{10} \times D_{10}$

Tablica 8.2: Izomorfnost i red pune grupe automorfizama pronađenih unitala u dizajnu \mathcal{D}_3

Utvrđili smo da postoje barem tri, do na izomorfizam, unitala u simetričnom 2-(66, 26, 10) dizajnu \mathcal{D}_3 . Zbog stohastičke prirode genetskih algoritama, primjenom MGU ne možemo odrediti koliko je točno unitala sadržano u simetričnim dizajnama s odgovarajućim parametrima, već primjenom tog algoritma možemo razmatrati pitanje egzistencije takvih podstruktura.

Optimalne parametre genetskog algoritma određujemo eksperimentiranjem. Za traženje unitala u dizajnu \mathcal{D}_3 koristili smo veličinu populacije $POP \in \{40, 60, 100\}$, vjerojatnost mutacije $p_m \in \{0.9, 0.99, 1\}$, te mehanizam resetiranja sa $f\% = 10\%$ koji su se pokazali kao optimalni.

Vrijeme izvođenja genetskog algoritma očituje se u broju iteracija (generacija). Vremenska složenost algoritma ovisi o nizu faktora: genetskim operatorima, načinu njihove implementacije, prezentaciji jedinki, veličini populacije, definiranju funkcije cilja, me-

8.1 Modificirani genetski algoritam (MGU) za traženje unitala u simetričnim dizajnama

hanizmima resetiranja i ostalim parametrima dizajna. Ne postoje univerzalno najbolji parametri za genetski algoritam koji će pronaći rješenje svih problema. Zbog svoje stohastičke prirode ([2]), vremensku složenost genetskog algoritma je teško odrediti. Analiza vremenske složenosti ne daje preciznu informaciju o vremenu potrebnom za pronalazak rješenja ([49]). Na temelju nekoliko eksperimenata, primijetili smo da algoritam vrlo brzo pronalazi rješenje čija je vrijednost funkcije cilja dosta blizu one optimalne, ali nakon toga potrebno je dosta iteracija koje donose mala poboljšanja najboljih rješenja. Ta je karakteristika genetskog algoritma primijećena i pri rješavanju drugih kombinatoričkih problema [26].

Modificirani genetski algoritam (MGU) za traženje unitala u 2-(66, 26, 10) dizajnu izvodi 4.2 iteracije u sekundi na četverojezgrenom procesoru (3,2 GHz) sa sljedećim parametrima:

- veličinom populacije $POP = 100$,
- 4-turnirskom selekcijom,
- križanjem s 2 točke,
- vjerojatnosti mutacije $p_m = 0.99$,
- mehanizmom za resetiranje populacije sa $f\% = 10\%$ najbolje rangiranih jedinki koji se pokreće nakon 90 minuta stagnacije,
- mehanizmom za potpuno resetiranje populacije nakon ukupno 180 minuta stagnacije.

Za takav procesor i parametre trebalo je u prosjeku 72 minute za pronalazak unitala, dok je najkraće vrijeme za pronalaženje unitala bilo 23 minute, što je prikazano u tablici 8.3. Broj pronađenih unitala označen je sa $nsol$, broj neizomorfni unitala označen je sa $niso$, minimalan i prosječan broj iteracija algoritma izvedenih prije dolaska do rješenja označeni su sa $nmin$ i $navi$, te standardna devijacija sa σ . Na opisanom procesoru potrebno je 2.3 godine za izvođenje pretrage za svim unitalima u 2-(66, 26, 10) dizajnama ukoliko pretražujemo po svim 11-teročlanim podskupovima skupa od 66 točaka. Međutim, ta bi se pretraga svakako mogla skratiti primjenom odgovarajućeg egzaktnog algoritma, budući da u slučaju da neki blok siječe neki podskup skupa točaka S u više od α točaka, sve 11-teročlane nadskupove tog skupa S ne moramo provjeravati, odnosno ti nadskupovi ne mogu biti skupovi točaka unitala.

Dizajn	$nsol$	$niso$	$nmin$	$navi$	σ
\mathcal{D}_3	17	3	5774	18088,27	21728,99

Tablica 8.3: Rezultati i iteracije MGU primijenjenog na dizajnu \mathcal{D}_3

U preostala dva 2-(66, 26, 10) dizajna \mathcal{D}_1 i \mathcal{D}_2 primjenom MGU nisu pronađeni novi unitali.

U simetričnom 2-(36, 15, 6) dizajnu \mathcal{D}' konstruiranom u [14] s punom grupom automorfizama reda 42 izomorfnom s grupom $Frob_{21} \times Z_2$, pronašli smo 66 unitala pomoću MGU. U primjeru 2.3 prikazana su tri unitala u takvom dizajnu. Rezultati o broju unitala i izvedenim iteracijama algoritma prikazani su u tablici 8.4, pri čemu smo koristili sljedeće parametre $POP = 100$, $p_m = 0.99$ i $f\% = 10\%$.

<i>Dizajn</i>	<i>nsol</i>	<i>niso</i>	<i>nmin</i>	<i>navi</i>	σ
\mathcal{D}'	66	6	4	1660,83	1958,15

Tablica 8.4: Rezultati i iteracije MGU primijenjenog na dizajnu \mathcal{D}'

Unital u simetričnom 2-(36, 15, 6) dizajnu je blokovni dizajn s parametrima 2-(8, 4, 6). Postoji točno 2310 dizajna s parametrima 2-(8, 4, 6) ([12]). Označimo 66 pronađenih unitala u dizajnu sa U'_1, \dots, U'_{66} . U tablici 8.5 ti unitali prikazani su u obliku niza indeksa stupaca matrice incidencije dizajna \mathcal{D}' . Pomoću programa GAP ([25]), provjereno je da do na izomorfizam postoji točno šest unitala u dizajnu \mathcal{D}' , što je prikazano u tablici 8.6.

Direktnom pretragom je provjereno da postoji točno 66 unitala u dizajnu \mathcal{D}' i svi su dobiveni pomoću MGU. U ovom slučaju, direktna pretraga je brzo izvedena zbog relativno malog broja svih mogućih kombinacija za provjeru, a ima ih $\binom{36}{8} = 30260340$.

8.2 Modificirani genetski algoritam (MGPD) za traženje poddizajna u simetričnim dizajnim

Matricu incidencije nekog blokovnog dizajna možemo pretraživati s ciljem pronalaska (ispitivanja egzistencije) poddizajna s proizvoljnim parametrima. U tu svrhu razvili smo modificirani genetski algoritam (MGPD) koji je sličan MGU algoritmu, a glavna je razlika u definiciji funkcije cilja i načinu odabira početne populacije. MGPD ima smisla primijeniti u slučaju kada direktno traženje poddizajna traje predugo.

MGPD je modificiran genetski algoritam sa 4-turnirskom selekcijom i križanjem s dvije točke koje se realizira se na sličan način kao i kod MGU algoritma. Razlike između tih algoritama opisujemo u nastavku.

Neka je \mathcal{D} 2 -(v, k, λ) dizajn u kojem tražimo poddizajn \mathcal{D}' s parametrima 2 -(v', k', λ'). Neka je M $b \times v$ matrica incidencije dizajna \mathcal{D} . Jasno je da će traženi poddizajn biti pronađen ako je odabrano onih b' redaka i v' stupaca matrice M koji odgovaraju blokovima i točkama poddizajna \mathcal{D}' .

Prva razlika između spomenutih algoritama je u načinu odabira početne populacije. U MGPD algoritmu najprije se na proizvoljan način odabire v' stupaca matrice M i skup točaka dizajna \mathcal{D} koje odgovaraju odabranim stupcima označimo sa T . Zatim se iz skupa redaka matrice M odabiru oni retci koji odgovaraju blokovima koji sadrže k' točaka iz skupa T . Označimo sa S tako odabrane blokove.

Za potpunu potragu za poddizajnim \mathcal{D}' , kojima je T skup točaka, potrebno je za svaki b' -člani podskup u skupu S , kojeg označimo sa S' , ispitati jesu li svake dvije točke iz skupa T sadržane u λ' blokova iz skupa S' . Broj mogućnosti koje pritom treba obraditi je $\binom{|S|}{b'}$, što može trajati predugo. Stoga, u takvim situacijama ima smisla primijeniti MGPD algoritam i u njegovoj programskoj realizaciji uzimaju se samo oni skupovi točaka T za koje je $\binom{|S|}{b'}$ reda veličine barem 10^7 .

Svaka jedinka u populaciji prezentirana je kao $b' \times v'$ podmatrica matrice M , pri čemu retci odgovaraju blokovima iz skupa S i stupci odgovaraju točkama iz skupa T . Odabir b' blokova iz skupa S koji čine niz gena neke jedinice za odabrani skup točaka T izvodi se na proizvoljan način.

Druga razlika između spomenutih algoritama je u funkciji cilja. U nekoj jedinki označimo broj blokova koji sadrže i -ti par točaka sa λ'_i , za $1 \leq i \leq \binom{v'}{2}$. Funkcija cilja MGPD algoritma mjeri odstupanje jedinice od svojstva da je ona matrica incidencije 2 -(v', k', λ') dizajna. Stoga, vrijednost funkcije cilja neke jedinice definiramo kao prosječnu vrijednost odstupanja "presjeka" svih parova točaka od tražene vrijednosti parametra λ' . Označimo

skup svih jedinki u populaciji sa X , te sa $p = \binom{v'}{2}$ i definiramo funkciju cilja $c : X \rightarrow \mathbb{R}_0^+$:

$$c(x) = \frac{\sum_{i=1}^p |\lambda'_i - \lambda'|}{p}, \quad \forall x \in X. \quad (8.2)$$

Minimalna (optimalna) vrijednost funkcije cilja c je nula i ako je ona dosegnuta, pronađen je 2- (v', k', λ') poddizajn u dizajnu \mathcal{D} . Preostali operatori u MGPD algoritmu (križanje, mutacija djece i roditelja, zamjena redosljeda jedinki) realizirani su kao u MGU algoritmu. Mehanizam resetiranja je samo jedan (potpuno resetiranje cijele populacije) i pokreće se nakon određenog vremena stagnacije najbolje vrijednosti funkcije cilja.

Na temelju MGPD algoritma napisan je računalni program koji kao ulazne parametre ima matricu M , veličinu populacije POP , veličinu turnira, te parametre k' i λ' .

Razvijeni program primijenili smo za traženje 2- $(11, 5, 2)$ poddizajna u simetričnim 2- $(66, 26, 10)$ dizajnama \mathcal{D}_1 , \mathcal{D}_2 i \mathcal{D}_3 ([19]) i rezultate navodimo u nastavku. S obzirom da se radi o simetričnim dizajnama, umjesto promatranja parova točaka u definiciji funkcije cilja, možemo promatrati parove blokova, prema tvrdnji teorema 2.6.

Na temelju nekoliko eksperimentalnih ispitivanja, odredili smo da ćemo raditi s $POP = 100$, 4-turnirskom selekcijom, s vjerojatnošću mutacije djece $p_m = 0,99$ i s potpunim resetiranjem populacije, odnosno novim izborom elemenata skupa T koji se sastoji od 11 točaka, nakon 1500 sekundi stagnacije. Program s takvim parametrima i postavkama primijenili smo na matricama incidencije dizajna \mathcal{D}_1 , \mathcal{D}_2 i \mathcal{D}_3 i nakon 24 sata rada dobili smo sljedeće rezultate. U dizajnama \mathcal{D}_1 i \mathcal{D}_2 nije pronađen niti jedan (uz resetiranje redom 46 i 42 puta), dok su u dizajnu \mathcal{D}_3 pronađena četiri 2- $(11, 5, 2)$ poddizajna (uz 44 resetiranja). Ti su poddizajni prikazani u tablici 8.7 pomoću indeksa redaka i stupaca matrice incidencije dizajna \mathcal{D}_3 , s tim da su retci (stupci) te matrice numerirani 1-66 i retci predstavljaju blokove tog dizajna.

2- $(66, 26, 10)$ dizajn \mathcal{D}_3 dobiven je indeksiranjem orbitne matrice OM, dane u poglavlju 8.1, za djelovanje grupe $Frob_{55} \cong Z_{11} : Z_5$ s distribucijom duljina orbita točaka (blokova) $(11, 11, 11, 11, 11, 11)$. Na analogan način kao što se u poglavlju 7.1 pokazalo djelovanje grupe Z_3 u $Frob_{39}$ -orbitama duljine 13, tako se i za grupu $Frob_{55}$ može pokazati da podgrupa Z_5 u orbitama duljine 11 djeluje kao permutacija: $(0)(1, 3, 9, 5, 4)(2, 6, 7, 10, 8)$.

Uzmemo li da je stabilizator predstavnika svih orbita grupa izomorfna sa Z_5 , to znači da postoje samo dvije mogućnosti za indeksne skupove elemenata orbitne matrice OM koji su jednaki 5, a to su skupovi $\{1, 3, 4, 5, 9\}$ ili $\{2, 6, 7, 8, 10\}$. Vidimo da su vrijednosti skupa $\{1, 3, 4, 5, 9\}$ nenul kvadratni ostaci u $GF(11)$. Stoga, ako se indeksiranjem elementa čija je vrijednost 5 u orbitnoj matrici OM dobije upravo ovaj skup indeksa, tada će podmatrica N reda 11 u matrici incidencije dizajna \mathcal{D}_3 , koja je nastala indeksiranjem tog elementa, biti matrica incidencije Paleyjeve dvoravnine, prema Paleyjevoj

8.2 Modificirani genetski algoritam (MGPD) za traženje poddizajna u simetričnim dizajnama

konstrukciji za $q \equiv 3 \pmod{4}$, gdje je q potencija neparnog prostog broja ([41]). Komplement simetričnog dizajna s parametrima $2-(11, 5, 2)$ također je simetričan dizajn ali s parametrima $2-(11, 6, 3)$. Njegovu matricu incidencije označimo sa N' . Budući da je N kososimetrična matrica, vrijedi $N' - I = N^T$. To znači da će podmatrica reda 11 u matrici incidencije dizajna \mathcal{D}_3 , koja je nastala indeksiranjem elementa jednakog 5 u matrici OM, biti kososimetrična matrica N ili N^T . Matrice N i N^T su matrice incidencije Payleyjeve dvoravnine, odnosno njezinog duala. Na temelju svega razmotrenog, jasno je da će u dizajnu \mathcal{D}_3 postojati poddizajni s parametrima $2-(11, 5, 2)$ i to za svaku od šest orbita točaka duljine 11 po pet takvih poddizajna. Oni nisu među rezultatima danim u tablici 8.7, stoga smo ponovno pokrenuli MGPD algoritam, ali ovaj put s unaprijed određenim stupcima matrice incidencije dizajna \mathcal{D}_3 .

Nakon 90 minuta rada na nizu točaka iz svake orbite duljine 11 posebno (uz resetiranje populacije nakon 1500 sekundi stagnacije), dobiveni su rezultati o broju pronađenih $2-(11, 5, 2)$ poddizajna u dizajnu \mathcal{D}_3 , koji su prikazani u tablici 8.8. $nmin$ ($nmax$) je oznaka za minimalan (maksimalan) broj iteracija algoritma izvedenih prije dolaska do novog rješenja.

U tablici 8.9 su dani rezultati dobiveni primjenom MGPD programa na dizajne \mathcal{D}_1 i \mathcal{D}_2 , na isti način kao što su dobiveni rezultati u tablici 8.8 za dizajn \mathcal{D}_3 . S obzirom da je za dizajne \mathcal{D}_1 i \mathcal{D}_2 dobiveno puno manje $2-(11, 5, 2)$ poddizajna, u tablici 8.9 navodimo indekse redaka (blokovi) i stupaca (točke) matrica incidencije dizajna \mathcal{D}_1 i \mathcal{D}_2 koje formiraju takve poddizajne.

Unitali	Indeksi stupaca matrice incidencije dizajna \mathcal{D}'							
U'_1	1	16	17	18	19	20	21	22
U'_2	1	16	17	21	23	24	28	32
U'_3	1	16	18	19	23	25	26	34
U'_4	1	16	20	22	23	27	29	31
U'_5	1	17	18	22	24	25	29	33
U'_6	1	17	19	20	24	26	27	35
U'_7	1	18	20	21	25	27	28	36
U'_8	1	19	21	22	26	28	29	30
U'_9	1	23	24	25	26	27	28	29
U'_{10}	1	30	31	32	33	34	35	36
U'_{11}	2	3	4	6	16	33	35	36
U'_{12}	2	3	4	7	19	20	22	25
U'_{13}	2	3	5	8	22	32	34	35
U'_{14}	2	3	6	8	18	19	21	24
U'_{15}	2	3	7	11	16	17	21	32
U'_{16}	2	3	7	11	25	26	27	29
U'_{17}	2	4	5	6	17	21	22	27
U'_{18}	2	4	5	13	16	18	19	34
U'_{19}	2	4	5	13	24	27	28	29
U'_{20}	2	4	7	8	21	31	33	34
U'_{21}	2	5	6	7	19	31	32	36
U'_{22}	2	5	7	8	17	18	20	23
U'_{23}	2	6	8	10	16	20	22	31
U'_{24}	2	6	8	10	24	25	26	28
U'_{25}	2	12	14	15	16	17	18	20
U'_{26}	2	12	14	15	26	28	29	30
U'_{27}	3	4	5	7	17	30	34	36
U'_{28}	3	4	5	8	16	20	21	26
U'_{29}	3	4	8	12	17	18	22	33
U'_{30}	3	4	8	12	23	26	27	28
U'_{31}	3	5	6	7	16	18	22	28
U'_{32}	3	5	6	14	17	19	20	35
U'_{33}	3	5	6	14	23	25	28	29
U'_{34}	3	6	7	8	20	30	32	33
U'_{35}	3	9	13	15	17	18	19	21
U'_{36}	3	9	13	15	23	27	29	31
U'_{37}	4	5	6	8	18	30	31	35
U'_{38}	4	6	7	8	16	17	19	29
U'_{39}	4	6	7	15	18	20	21	36
U'_{40}	4	6	7	15	23	24	26	29
U'_{41}	4	9	10	14	18	19	20	22
U'_{42}	4	9	10	14	23	24	28	32
U'_{43}	5	7	8	9	19	21	22	30
U'_{44}	5	7	8	9	23	24	25	27
U'_{45}	5	10	11	15	16	19	20	21
U'_{46}	5	10	11	15	24	25	29	33
U'_{47}	6	9	11	12	17	20	21	22
U'_{48}	6	9	11	12	23	25	26	34
U'_{49}	7	10	12	13	16	18	21	22
U'_{50}	7	10	12	13	24	26	27	35
U'_{51}	8	11	13	14	16	17	19	22
U'_{52}	8	11	13	14	25	27	28	36
U'_{53}	9	10	11	13	23	33	35	36
U'_{54}	9	10	11	14	18	26	27	29
U'_{55}	9	10	12	15	29	32	34	35
U'_{56}	9	10	13	15	17	25	26	28
U'_{57}	9	11	12	13	20	24	28	29
U'_{58}	9	11	14	15	28	31	33	34
U'_{59}	9	12	13	14	26	31	32	36
U'_{60}	9	12	14	15	16	24	25	27
U'_{61}	10	11	12	14	24	30	34	36
U'_{62}	10	11	12	15	19	23	27	28
U'_{63}	10	12	13	14	21	23	25	29
U'_{64}	10	13	14	15	27	30	32	33
U'_{65}	11	12	13	15	25	30	31	35
U'_{66}	11	13	14	15	22	23	24	26

Tablica 8.5: Unitali u 2-(36,15,6) dizajnu \mathcal{D}' dobiveni primjenom MGU

Izomorfni unitali u \mathcal{D}'	$ Aut(\mathcal{D}) $	$Aut(\mathcal{D})$
U'_{10}	21	$Z_7 : Z_3$
$U'_1 \cong U'_9$	336	$PSL(3,2):Z_2$
$U'_2 \cong U'_3 \cong \dots \cong U'_8$	6	Z_6
$U'_{11} \cong U'_{13} \cong U'_{20} \cong U'_{21} \cong U'_{27} \cong U'_{34} \cong U'_{37} \cong U'_{53} \cong U'_{55} \cong U'_{58} \cong U'_{59} \cong U'_{61} \cong U'_{64} \cong U'_{65}$	6	S_3
$U'_{12} \cong U'_{14} \cong U'_{17} \cong U'_{22} \cong U'_{28} \cong U'_{31} \cong U'_{38} \cong U'_{54} \cong U'_{56} \cong U'_{57} \cong U'_{60} \cong U'_{62} \cong U'_{63} \cong U'_{66}$	3	Z_3
$U'_{15} \cong U'_{16} \cong U'_{18} \cong U'_{19} \cong U'_{23} \cong U'_{24} \cong U'_{25} \cong U'_{26} \cong U'_{29} \cong U'_{30} \cong U'_{32} \cong U'_{33} \cong U'_{35} \cong U'_{36} \cong U'_{39} \cong \dots \cong U'_{52}$	6	Z_6

Tablica 8.6: Izomornost i red pune grupe automorfizama svih unitala u dizajnu \mathcal{D}'

8.2 Modificirani genetski algoritam (MGPD) za traženje poddizajna u simetričnim dizajnim

Točke	Blokovi
15 21 23 24 28 29 30 38 42 44 47	1 2 3 4 5 6 7 8 9 10 11
12 16 32 41 57 58 59 61 62 64 66	1 2 3 4 5 6 7 8 9 10 11
38 41 42 44 51 54 56 57 58 59 61	1 2 3 4 5 6 7 8 10 11 39
12 13 17 26 32 36 40 49 53 63 66	1 2 3 5 6 7 8 9 10 11 47

Tablica 8.7: 2-(11, 5, 2) poddizajni u \mathcal{D}_3 prikazani indeksima redaka (blokovi) i stupaca (točke) matrice incidencije od \mathcal{D}_3 , primjena MGPD

Točke u \mathcal{D}_3	# 2-(11, 5, 2) poddizajna	$nmin$	$nmax$
1-11	1675	1	50
12-22	184	14	320
23-33	212	8	276
34-44	188	8	228
45-55	141	7	260
56-66	120	5	255

Tablica 8.8: 2-(11, 5, 2) poddizajni u \mathcal{D}_3 dobiveni nakon 90 minuta primjene MGPD

Dizajn \mathcal{D}	Točke	Blokovi	$nmin$	$nmax$
\mathcal{D}_1	1-11	0		
	12-22	45-55	973	9377
	23-33	34-44	2209	3667
	34-44	23-33	291	3823
		8,16,17,26,27,28,31,32,33,48,50	291	3823
	45-55	12-22	510	4842
56-66	56-66	1836	7969	
\mathcal{D}_2	1-11	0		
	12-22	45-55	6008	6008
	23-33	34-44	2251	8426
	34-44	23-33	350	10751
	45-55	12-22	336	7563
	56-66	56-66	1360	7223

Tablica 8.9: 2-(11, 5, 2) poddizajni u \mathcal{D}_1 i \mathcal{D}_2 dobiveni nakon 90 minuta primjene MGPD

Bibliografija

- [1] M. Aschbacher, On Colineation Groups of Symmetric Block Designs, *Journal of Combinatorial Theory* 11, 1971., 272–281.
- [2] T. Bäck, D. B. Fogel, Z. Michalewics, *Handbook of Evolutionary Computation*, IOP Publishing Ltd, Bristol, UK (1997)
- [3] S. Bagchi, B. Bagchi, Designs from pairs of finite fields I. A cyclic unital $U(6)$ and other regular Steiner 2-designs, *Journal of Combinatorial Theory A* 52 (1989), 51–61
- [4] S. Barwick, G. Ebert, *Unitals in Projective Planes*, Springer, 2008.
- [5] L. M. Batten, A. Beutelspacher, *The theory of finite linear spaces*, Cambridge University Press, 1993.
- [6] B. Baumslag, B. Chandler, *Theory and Problems of Group Theory*, Schaum's Series, McGraw - Hill, New York, 1968.
- [7] H. Beker, C. Mitchell, F. Piper, Tactical decompositions of designs, *Aequationes mathematicae*, vol. 25, pp 123–152, 1982.
- [8] R. E. Block, On the orbits of collineation groups, *Math. Z.* 96 (1967), 33–49.
- [9] P. Bofill, R. Guimera, C. Torras, Comparison of simulated annealing and mean field annealing as applied to the generation of block designs, *Neural Networks* 16 (2003), 1421–1428.
- [10] A. E. Brouwer, Some unitals on 28 points and their embeddings in projective planes of order 9, in M. Aigner and D. Jungnickel (eds.), *Geometries and Groups*, Lecture Notes in Mathematics, Springer, Berlin, 893, 1981., 183–188.
- [11] C. J. Colbourn, A Steiner 2-Design with an Automorphism Fixing Exactly $r + 2$ Points, *J. Combinatorial Designs* 7 (1999), 375–380.
- [12] C. J. Colbourn, J.H. Dinitz (Eds.), *CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton (1996.)

- [13] D. Crnković, Konstrukcije nekih novih simetričnih nacrtava kvadratnog reda, doktorska disertacija, Sveučilište u Zagrebu, 1998.
- [14] D. Crnković, Symmetric $(36,15,6)$ design having $U(3,3)$ as an automorphism group, Glas. Mat., III.Ser. Vol. 34(54), No. 1 (1999), 1–3.
- [15] D. Crnković, Symmetric $(70,24,8)$ designs having $Frob_{21} \times Z_2$ as an automorphism group, Glas. Mat. Ser. III 34 (54), No. 2 (1999), 109–121.
- [16] D. Crnković, D. Dumičić Danilović, Finding unitals in symmetric designs using a modified genetic algorithm, Math. Pannon. 24 (2014), 183–196.
- [17] D. Crnković, M. O. Pavčević, Some new symmetric designs with parameters $(64,28,12)$, Discrete Math. 237, No. 1–3 (2001), 109–118.
- [18] D. Crnković, S. Rukavina, Construction of block designs admitting an Abelian automorphism group, Metrika, 02/2005; 62(2), 175–183
- [19] D. Crnković, S. Rukavina, Symmetric $(66,26,10)$ designs having $Frob_{55}$ as an automorphism group, Glasnik Matematički 35(55)(2000), 271–281.
- [20] D. Crnković, B. G. Rodrigues, S. Rukavina, L. Simčić, Ternary codes from the strongly regular $(45,12,3,3)$ graphs and orbit matrices of 2- $(45,12,3)$ designs, Discrete Math. 312 (2012), 3000–3010.
- [21] V. Čepulić, On Symmetric Block Designs $(40,13,4)$ with Automorphisms of Order 5, Discrete Math. 128(1-3), 45–60 (1994)
- [22] P. Dembowski, Finite Geometries, Springer, Berlin-Heidelberg-New York, 1968.
- [23] P. Dembowski, Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen, Math. Z. 69, 1958.
- [24] J. D. Dixon, B. Mortimer, Permutation groups, Springer, New York, 1996.
- [25] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.7.2; 2013. (<http://www.gap-system.org>)
- [26] M. Golub, I. Martinjak, Comparison of Heuristic Algorithms for the N-Queen Problem, ITI, Cavtat/Dubrovnik, 2007.
- [27] H. Hanani, Balanced incomplete block designs and related designs, Discrete Mathematics 11, (1975), 255–369
- [28] D. Held, M. O. Pavčević, Symmetric $(79,27,9)$ designs admitting a faithful action of a Frobenius group of order 39, European J. Combin. 18 (1997), 409–416.

-
- [29] D. R. Hughes, F.C. Piper, Projective Planes, Springer, New York, 1973.
- [30] T. W. Hungerford, Algebra, Springer, 1974.
- [31] N. Jacobson, Basic Algebra 1, W.H.Freeman and Company, New York, 1985.
- [32] Z. Janko, Coset enumeration in groups and constructions of symmetric designs, Combinatorics '90 (Gaeta, 1990), Ann. Discrete Math. 52 (1992), 275–277.
- [33] Z. Janko, The existence of symmetric designs with parameters $(105,40,15)$, J. Combin. Des. 7 (1999), 17–19.
- [34] Z. Janko, T. van Trung, Construction of a new symmetric block design for $(78,22,6)$ with the help of tactical decompositions, J. Combin. Theory A 40, (1985) 451–455.
- [35] D. Jungnickel, "Difference sets," in J.H. Dinitz and D.R. Stinson, editors, Contemporary Design Theory: a collection of surveys, Wiley, New York, 1992, pp. 241–324.
- [36] E. S. Kramer, D. M. Mesner, t -designs on hypergraphs, Discrete Math. 15 (1976), 263–296.
- [37] V. Krčadinac, Construction and classification of finite structures by computer, PhD thesis, University of Zagreb, 2004.
- [38] V. Krčadinac, Steiner 2-designs $S(2,4,28)$ with nontrivial automorphisms, Glas. Mat. Ser. III 37 (2002), no. 57, 259–268.
- [39] V. Krčadinac, Unitali, skripta, PMF-Matematički odsjek, 2010.
- [40] 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.
- [41] E. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press, Cambridge, 1983.
- [42] V. Mandekić-Botteri, On symmetric block designs $(45, 12, 3)$ with involutory automorphism fixing 15 points, Glas. Mat., Vol.36, No.2, 01/2001.
- [43] I. Martinjak, M. O. Pavčević, Modified genetic algorithm for BIBD construction, ITI 2009, 647–652.
- [44] R. Mathon, Computational methods in design theory, in Computational and Constructive Design Theory, Kluwer Academic Publishers, Dordrecht, 1996, pp. 29–48.
- [45] R. Mathon, Constructions for cyclic Steiner 2-designs, Ann.Discrete Math., Vol.34, 1987. 353–362.

- [46] R. Mathon, T. van Trung, Unitals and Unitary Polarities in Symmetric Designs, Designs, Codes and Cryptography 10, 1997., 237–250.
- [47] I. Matulić-Bedenić, K. Horvatić-Baldasar, E. Kramer, Construction of new symmetric designs with parameters $(66,26,10)$, Journal of Combinatorial Designs 3 (1995), 405–410.
- [48] L. B. Morales, Constructing 1-rotational NRDFs through an optimization approach: New $(46,9,8)$, $(51,10,9)$ and $(55,9,8)$ -NRBDs, Journal of Statistical Planning and Inference Volume 139, Issue 1, (2009), 62–68.
- [49] P. S. Oliveto, J. He, X. Yao, Time Complexity of Evolutionary Algorithms for Combinatorial Optimization: A Decade of Results, International Journal of Automation and Computing 04(3) (2007), 281–293.
- [50] M. O. Pavčević, E. Spence, Some new symmetric designs with $\lambda = 10$ having an automorphism of order 5, Discrete Mathematics 196 (1999), 257–266.
- [51] S. Pfaff, Ispitivanje egzistencije dizajna $(121,16,2)$ i $(78,22,6)$, Doktorska disertacija, Sveučilište u Zagrebu, 1992.
- [52] M. J. de Resmini, On sets of type (m,n) in BIBD's with $\lambda \geq 2$, Ann.Discr.Math., Vol.14, 1982., 183–206.
- [53] D. Robinson, A Course in the Theory of groups, Springer-Verlag, Berlin Heidelberg, New York, 1998.
- [54] H. E. Rose, A course on Finite Groups, Springer UTM, 2009.
- [55] S. Rukavina, Enumeration of symmetric $(69,17,4)$ designs admitting Z_6 as an automorphism group, Glasnik Matematički, Vol. 34(54)(1999),129 – 145.
- [56] S. Rukavina, Simetrični blokovni nacrti s automorfizmima reda šest, Doktorska disertacija, Sveučilište u Zagrebu, 1999.
- [57] S. Rukavina, Some new triplanes of order twelve, Glasnik Matematički, Vol. 36(56)(2001), 105–125.
- [58] H. J. Ryser, A note on a combinatorial problem, Proc. Amer. Math. Soc., 1 (1950), 422–424.
- [59] L.H. Soicher, DESIGN - a GAP package, Version 1.6, 23/11/2011. (<http://www.gap-system.org/Packages/design.html>)
- [60] D. R. Stinson, Combinatorial Designs: Constructions and Analysis, Springer, New York, 2004.

- [61] S. D. Stoichev, V.D. Tonchev, Unital designs in planes of order 16, *Discrete Appl. Math.* 102 (2000), 151–158.
- [62] V. D. Tonchev, Embedding of Witt-Mathieu system $S(3, 6, 22)$ in a symmetric 2- $(78, 22, 6)$ design, *Geometriae Dedicata*, 22, (1987), 49–75.
- [63] V. D. Tonchev, *Combinatorial Configurations Designs, Codes, Graphs*, Wiley, New York, 1988.
- [64] T. van Trung, The existence of symmetric block designs with parameters $(41, 16, 6)$ i $(66, 26, 10)$, *J. Comb. Theory A* Vol. 33 (1982), 201–204.
- [65] W. D. Wallis, *Computational and Constructive Design Theory*, Kluwer Academic Publishers, Dordrecht, Boston, 1996.

Prilog

Ovdje navodimo točkovne orbitne matrice OM_1 , OM_2 , OM_3 i OM_4 dobivene primjenom programa za profinjenje orbitne matrice OM iz poglavlja 7.2. Osim toga, navodimo točkovne orbitne matrice OS_1 , OS_2 , OS_3 i OS_4 dobivene primjenom programa za profinjenje orbitne matrice OS iz poglavlja 7.2.

121201100200001110110010000101100001101
 012120110020000111011001001010110000110
 001212011002000011101100100101011000011
 000121201100200001110110011010101100001
 200012120110010000111011001101010110000
 020001212011001000011101100110101011000
 002000121201100100001110110011010101100
 100200012120110010000111010001101010110
 110020001212011001000011100000110101011
 011002000121201100100001111000011010101
 201100200012110110010000111100001101010
 120110020001211011001000010110000110101
 212011002000111101100100001011000011010
 010100011101010201220001010010011110010
 001010001110111020122000100001001111001
 100101000111001102012200011000100111100
 010010100011110110201220000100010011110
 101001010001101011020122000010001001111
 110100101000100101102012201001000100111
 111010010100000010110201221100100010011
 011101001010020001011020121110010001001
 001110100101022000101102011111001000100
 000111010010112200010110200111100100010
 100011101001001220001011020011110010001
 010001110100120122000101101001111001000
 101000111010002012200010110100111100100
 000010011011100101110001011202100002101
 100001001101110010111000101120210000210
 110000100110101001011100010112021000021
 111000010011010100101110001011202100002
 011100001001101010010111002101120210000
 101110000100100101001011100210112021000
 110111000010000010100101110021011202100
 011011100001010001010010110002101120210
 001101110000111000101001010000210112021
 100110111000011100010100101000021011202
 010011011100001110001010012100002101120
 001001101110010111000101000210000210112
 000100110111001011100010102021000021011

Tablica 8.14: OS_1

1212011002000011101100100001010000111010
 012120110020000111011001000010100011101
 001212011002000011101100101001010001110
 000121201100200001110110010100101000111
 200012120110010000111011001010010100011
 020001212011001000011101101101001010001
 002000121201100100001110111110100101000
 100200012120110010000111010111010010100
 110020001212011001000011100011101001010
 011002000121201100100001110001110100101
 201100200012110110010000111000111010010
 120110020001211011001000010100011101001
 212011002000111101100100001010001110100
 010110000110110100112200200010011110010
 101011000011001010011220020001001111001
 010101100001120101001122001000100111100
 101010110000102010100112200100010011110
 110101011000000201010011220010001001111
 011010101100020020101001121001000100111
 001101010110022002010100111100100010011
 000110101011012200201010011110010001001
 000011010101111220020101001111001000100
 100001101010101122002010100111100100010
 110000110101000112200201010011110010001
 011000011010110011220020101001111001000
 101100001101001001122002010100111100100
 000010011011100101110001011101000221020
 100001001101110010111000100110100022102
 110000100110101001011100012011010002210
 111000010011010100101110000201101000221
 011100001001101010010111001020110100022
 101110000100100101001011102102011010002
 110111000010000010100101112210201101000
 011011100001010001010010110221020110100
 001101110000111000101001010022102011010
 100110111000011100010100100002210201101
 010011011100001110001010011000221020110
 001001101110010111000101000100022102011
 000100110111001011100010101010002210201

Tablica 8.15: OS_2

121201100200001011000011010000100110111
 012120110020010101100001101000010011011
 001212011002001010110000111100001001101
 000121201100210101011000011110000100110
 200012120110011010101100000111000010011
 020001212011001101010110001011100001001
 002000121201100110101011001101110000100
 100200012120100011010101100110111000010
 110020001212000001101010110011011100001
 011002000121210000110101011001101110000
 201100200012111000011010100100110111000
 120110020001201100001101010010011011100
 212011002000110110000110100001001101110
 011101100100010100112200200010111000101
 001110110010001010011220021001011100010
 000111011001020101001122000100101110001
 000011101100102010100112201010010111000
 100001110110000201010011220101001011100
 010000111011020020101001120010100101110
 001000011101122002010100110001010010111
 100100001110112200201010011000101001011
 110010000111011220020101001100010100101
 011001000011101122002010101110001010010
 101100100001100112200201010111000101001
 110110010000110011220020101011100010100
 111011001000001001122002010101110001010
 010100011101000100111100101101000221020
 001010001110100010011110010110100022102
 100101000111010001001111002011010002210
 010010100011101000100111100201101000221
 101001010001100100010011111020110100022
 110100101000110010001001112102011010002
 111010010100011001000100112210201101000
 011101001010011100100010010221020110100
 001110100101011110010001000022102011010
 000111010010101111001000100002210201101
 100011101001000111100100011000221020110
 010001110100110011110010000100022102011
 101000111010001001111001001010002210201

Tablica 8.16: OS_3

121201100200001010001110100000100110111
 012120110020000101000111011000010011011
 001212011002010010100011101100001001101
 000121201100201001010001111110000100110
 200012120110010100101000110111000010011
 020001212011011010010100011011100001001
 002000121201111101001010001101110000100
 100200012120101110100101000110111000010
 110020001212000111010010100011011100001
 011002000121200011101001011001101110000
 201100200012110001110100100100110111000
 120110020001201000111010010010011011100
 212011002000110100011101000001001101110
 011101100100010201220001010010111000101
 001110110010011020122000101001011100010
 000111011001001102012200010100101110001
 000011101100110110201220001010010111000
 100001110110001011020122000101001011100
 010000111011000101102012200010100101110
 001000011101100010110201220001010010111
 100100001110120001011020121000101001011
 110010000111022000101102011100010100101
 011001000011112200010110201110001010010
 101100100001101220001011020111000101001
 110110010000120122000101101011100010100
 111011001000002012200010110101110001010
 010110000110100100111100101202100002101
 101011000011000010011110011120210000210
 010101100001110001001111000112021000021
 101010110000101000100111101011202100002
 110101011000000100010011112101120210000
 011010101100010010001001110210112021000
 001101010110011001000100110021011202100
 000110101011011100100010010002101120210
 000011010101111110010001000000210112021
 100001101010101111001000101000021011202
 110000110101000111100100012100002101120
 011000011010110011110010000210000210112
 101100001101001001111001002021000021011

Tablica 8.17: OS_4

Sažetak

U ovoj disertaciji opisani su algoritmi za konstrukciju blokovnih dizajna pomoću orbitnih matrica, uz pretpostavku djelovanja određene grupe na dizajn. Radi se o algoritmu za konstrukciju neizomorfnih točkovnih orbitnih matrica blokovnih dizajna s proizvoljnim dopustivim parametrima na koje djeluje proizvoljna grupa. Taj je algoritam generalizacija algoritma za konstrukciju neizomorfnih blokovnih orbitnih matrica simetričnih dizajna, opisanog u članku [21]. U sklopu ove disertacije, razvili smo i algoritam za profinjenje (dekompoziciju) orbitnih matrica koji se temelji na primjeni kompozicijskog niza rješive grupe automorfizama blokovnih dizajna. Opisani algoritmi implementirani su u programsku podršku napisanu u programu GAP ([25]).

Pomoću razvijenih programa napravljena je klasifikacija 2-(45, 5, 1) dizajna na koje djeluje automorfizam reda šest, te klasifikacija 2-(45, 12, 3) dizajna na koje djeluje involutorni automorfizam. Isto tako, konstruirani su svi, do na izomorfizam, 2-(45, 5, 1) dizajni na koje djeluje grupa $G \cong Z_3 \times Z_3$ u slučajevima kada postoje dvije podgrupe reda tri u grupi G koje djeluju na dizajn tako da nemaju zajedničkih orbita točaka i blokova duljine tri. Konstruirani su također i 2-(45, 5, 1) dizajni na koje djeluje grupa S_3 .

Osim toga, napravljena je klasifikacija 2-(78, 22, 6) dizajna na koje djeluje grupa $Frob_{39} \times Z_2$, pri čemu se u ovom slučaju algoritam za profinjenje orbitnih matrica temelji na primjeni glavnog niza konkretne grupe koja djeluje na taj dizajn.

Jedan od bitnih rezultata ove disertacije je dokaz da ne postoji (78, 22, 6) diferencijski skup u grupi $Frob_{39} \times Z_2$, a dobiven je primjenom spomenutih programa.

U sklopu ovog rada razvili smo modificirane genetske algoritme za traženje unitala i drugih poddizajna, pretraživanjem matrica incidencije (simetričnih) blokovnih dizajna. Ti su algoritmi implementirani u programsku podršku napisanu u Matlab-u. Pronađeni su unitali u simetričnim 2-(66, 26, 10) i 2-(36, 15, 6) dizajnama i 2-(11, 5, 2) poddizajni u simetričnim 2-(66, 26, 10) dizajnama.

Summary

In this thesis we describe the algorithms for construction of block designs admitting an action of an automorphism group using orbit matrices. We develop and describe a program which constructs mutually nonisomorphic orbit matrices for arbitrary block design and automorphism group, which is a generalisation of the program for obtaining orbit matrices for some symmetric design and automorphism group described in the paper [21].

The second step in the construction is often called an indexing of orbit matrices, respectively construction of block designs from orbit matrices. Indexing often lasts too long, therefore we develop an algorithm for the refinement of orbit matrices, based on the application of the composition series of the solvable automorphism group which acts on design. Mentioned algorithms are used as a base for computer programs written in program GAP. Classification of all $2-(45, 5, 1)$ designs admitting an action of an automorphism of order 6 and classification of all $2-(45, 12, 3)$ designs admitting an action of an involution is presented. Moreover, we have constructed all, up to isomorphism, $2-(45, 5, 1)$ designs admitting an action of group $Z_3 \times Z_3$ in the cases when there exist two subgroups of order 3 in the group $Z_3 \times Z_3$ that act on the design having no common point and block orbits of length 3. Besides this, we have constructed $2-(45, 5, 1)$ designs admitting an action of group S_3 . The classification of all $2-(78, 22, 6)$ admitting an action of group $G \cong Frob_{39} \times Z_2$ is presented. In this case, the algorithm for the refinement of orbit matrices is based on the application of the principal series of the group G . An important result of the thesis is the proof that there does not exist $(78, 22, 6)$ difference set in the group G .

Besides that, the subject of the thesis is to examine the existence of certain subdesigns in a block designs using an incomplete search with a modified genetic algorithm, in case when complete methods (exhaustive search) do not give enough or any results in a reasonable period of time. Therefore modified genetic algorithms for finding subdesigns probing incidence matrices for some block designs we develop and describe. Modified genetic algorithm for finding unitals in symmetric designs is applied on search for unitals in symmetric designs with parameters $2-(66, 26, 10)$ and $2-(36, 15, 6)$. Moreover, modified genetic algorithm for finding subdesigns with given parameters in arbitrary block design is applied on search for $2-(11, 5, 2)$ subdesigns in $2-(66, 26, 10)$ designs.

Životopis

Doris Dumičić Danilović je rođena 02. kolovoza 1983. u Rijeci, gdje je završila osnovnu školu te "Prvu riječku hrvatsku gimnaziju". Godine 2007. je diplomirala na Sveučilišnom studiju matematike i informatike na Filozofskom fakultetu Sveučilišta u Rijeci, obranom diplomskog rada "Moduli", pod mentorstvom prof. dr. sc. Deana Crnkovića. Iste te godine dobila je Rektorovu nagradu za najboljeg studenta na Filozofskom fakultetu Sveučilišta u Rijeci.

Od travnja 2008. godine zaposlena je kao asistent na Odjelu za matematiku Sveučilišta u Rijeci. Akademske godine 2008./2009. upisala je poslijediplomski doktorski studij matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.

Članica je Seminara za konačnu matematiku u Rijeci, u sklopu kojeg je održala niz seminara. Članica je Društva matematičara i fizičara u Rijeci, te Alumni kluba Odjela za matematiku Sveučilišta u Rijeci.

Znanstveni radovi:

- D. Crnković, D. Dumičić Danilović, Finding unitals in symmetric designs using a modified genetic algorithm, *Math. Pannon.* 24 (2014), 183–196.