Samodualni kodovi i PD-skupovi konstruirani iz kombinatoričkih dizajna

Mostarac, Nina

Doctoral thesis / Disertacija

2017

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://urn.nsk.hr/urn:nbn:hr:217:010482

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-12**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

Sveučilište u Zagrebu

PRIRODOSLOVNO-MATEMATIČKI FAKULTET

Nina Mostarac

SAMODUALNI KODOVI I PD-SKUPOVI KONSTRUIRANI IZ KOMBINATORIČKIH DIZAJNA

DOKTORSKI RAD

Zagreb, 2017.

University of Zagreb

FACULTY OF SCIENCE

Nina Mostarac

SELF-DUAL CODES AND PD-SETS CONSTRUCTED FROM COMBINATORIAL DESIGNS

DOCTORAL THESIS

Zagreb, 2017

Sveučilište u Zagrebu

PRIRODOSLOVNO-MATEMATIČKI FAKULTET

Nina Mostarac

SAMODUALNI KODOVI I PD-SKUPOVI KONSTRUIRANI IZ KOMBINATORIČKIH DIZAJNA

DOKTORSKI RAD

Mentor:

Prof. dr. sc. Dean Crnković

Zagreb, 2017.

University of Zagreb

FACULTY OF SCIENCE

Nina Mostarac

SELF-DUAL CODES AND PD-SETS CONSTRUCTED FROM COMBINATORIAL DESIGNS

DOCTORAL THESIS

Supervisor:

Professor Dean Crnković, PhD

Zagreb, 2017

Ova disertacija je predana na ocjenu Prirodoslovno-matematičkom fakultetu, Matematičkom odsjeku, Sveučilišta u Zagrebu, u svrhu stjecanja znanstvenog stupnja doktora znanosti iz područja prirodnih znanosti, znanstvenog polja matematika.

Izjava o izvornosti rada

Ja, Nina Mostarac, studentica Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu, s prebivalištem na adresi [redacted], ovim putem izjavljujem pod materijalnom i kaznenom odgovornošću da je moj doktorski rad pod naslovom: Samodualni kodovi i PD-skupovi konstruirani iz kombinatoričkih dizajna, isključivo moje autorsko djelo, koje je u potpunosti samostalno napisano uz naznaku izvora drugih autora i dokumenata korištenih u radu.

U Zagrebu, listopad 2017.

Nina Mostarac

Zahvale

Iskreno se zahvaljujem svom mentoru prof. dr. sc. Deanu Crnkoviću na vođenju, pomoći, sugestijama, te upućivanju u zanimljiva područja istraživanja tijekom izrade ove disertacije, te tijekom mog doktorskog studija.

Hvala i prof. dr. sc. Sanji Rukavini na korisnim prijedlozima i savjetima tijekom mog znanstvenog istraživanja. Također se zahvaljujem i svim članovima Seminara za konačnu matematiku u Rijeci na strpljenju i sugestijama tijekom mojih izlaganja koja su vodila ka pisanju ove disertacije. Upućujem i zahvalu članovima povjerenstva na vremenu i trudu uloženom u čitanje ovog rada.

Veliko hvala i mojoj obitelji, osobito mom suprugu Robertu, na bezgraničnoj potpori, strpljenju i ljubavi. Bez njihove pomoći ovo ne bi bilo moguće.

Sadržaj

Popis tablica

Predgovor

Predmet istraživanja ove doktorske disertacije je konstrukcija samodualnih kodova iz određenih kombinatoričkih dizajna, te pronalaženje PD-skupova za kodove povezane s nekim flag-tranzitivnim kombinatoričkim dizajnima.

Teorija dizajna dio je diskretne matematike koji se bavi proučavanjem konačnih incidencijskih struktura kao što su blokovni dizajni, Hadamardove matrice, latinski kvadrati, diferencijski skupovi i druge strukture. S razvojem računala naglo se razvila i teorija dizajna. Ona nalazi svoje primjene u raznim područjima, na primjer u rasporedima turnira, lutriji, matematičkoj biologiji, dizajniranju algoritama, tehnologiji umrežavanja, kriptografiji, te u raznim granama matematike [48]. Kombinatorički dizajni koji se koriste u konstrukcijama u ovom radu su blokovni dizajni te (grupovno) djeljivi dizajni.

Teorija kodiranja je grana matematike koja proučava prijenos kodiranih informacija od pošiljatelja do primatelja kroz komunikacijski kanal sa smetnjama, te načine njihovog dekodiranja. Bavi se dizajniranjem kodova s ispravljanjem pogrešaka koji omogućuju pouzdan prijenos podataka kroz bučni kanal, a naročito linearnim kodovima, koji zbog svojih svojstava dopuštaju efikasne algoritme kodiranja i dekodiranja [39]. Važna klasa linearnih kodova, koja je bila predmet jako puno istraživanja, su samodualni kodovi. Veliki dio ove disertacije bit će posvećen upravo konstrukciji samodualnih kodova.

Ova je disertacija tematski podijeljena u četiri poglavlja. Prvo, uvodno poglavlje, donosi nam osnovne pojmove iz teorije grupa, teorije kodiranja, teorije grafova i teorije dizajna, koji su nam potrebni za razumijevanje cijeloga rada. Zatim su drugo i treće poglavlje posvećeni konstrukciji samodualnih kodova iz nekih kombinatoričkih dizajna, točnije iz simetričnih (grupovno) djeljivih dizajna, te simetričnih i nesimetričnih blokovnih dizajna. Četvrto se poglavlje bavi pronalaženjem PD-skupova za kodove povezane s flag-tranzitivnim simetričnim dizajnima.

Incidencijska struktura s v točaka, b blokova i konstantnom veličinom blokova k u kojoj je svaka točka incidentna s točno r blokova je (grupovno) djeljivi dizajn (GDD) s parametrima $(v, b, r, k, \lambda_1, \lambda_2, m, n)$ ako se skup točaka može particionirati u m klasa veličine n, tako da su dvije točke iz iste klase sadržane zajedno u točno λ_1 blokova, a dvije točke iz različitih klasa sadržane su zajedno u točno λ_2 blokova. Neka svojstva grupovno djeljivih dizajna dana su u [7], [8] i [45].

O blokovnim dizajnima više se može pročitati u [5]. Iz definicije slijedi da je djeljivi

dizajn ujedno i blokovni dizajn ako i samo ako je ili $n = 1$ ili $\lambda_1 = \lambda_2$. Budući da se mogu promatrati kao poopćenje blokovnih dizajna, za djeljive se dizajne mogu pokušati generalizirati neke konstrukcije vezane uz blokovne dizajne. D. Crnković i S. Rukavina su u [17] dali konstrukciju samodualnih kodova iz proširenih orbitnih matrica simetričnih dizajna. Razvijanjem ideja koje su prezentirali Lander [35] i Wilson [52], te posebno onih u [17], dobiveni su rezultati o samodualnim kodovima iz djeljivih dizajna. Ti su rezultati opisani u drugom poglavlju ovog rada, te su objavljeni u [15]. Tamo su konstruirani samodualni kodovi razapeti retcima proširenih kvocijentnih matrica simetričnih (grupovno) djeljivih dizajna (SGDD) s dualnim svojstvom. Koristi se i lanac kodova da se kvocijentnoj matrici SGDD-a s dualnim svojstvom pridruži samodualan kod. U disertaciji su zatim pronađeni i primjeri samodualnih kodova u odnosu na određeni skalarni produkt, dobiveni iz SGDD-a s dualnim svojstvom povezanih s DDG-ovima i DDD-ovima (grafovima i digrafovima-djeljivim dizajnima). Ovi primjeri nisu objavljeni u spomenutom radu [15].

U trećem je poglavlju dano nekoliko konstrukcija samoortogonalnih i samodualnih kodova iz orbitnih matrica pridruženih blokovnim dizajnima, induciranih djelovanjem grupe automorfizama dizajna. Prvo su opisane konstrukcije samoortogonalnih i samodualnih kodova iz ne nužno simetričnih blokovnih dizajna, koje se provode uz pomoć njihovih proširenih orbitnih matrica. Dani su i konkretni primjeri tako dobivenih kodova. Ideje za ove konstrukcije proizašle su iz Wilsonovog rada [52] u kojemu se opisuje kako korištenjem matrica incidencije blokovnih dizajna možemo dobiti samodualne kodove.

Zatim su u nastavku trećeg poglavlja opisane još neke konstrukcije samodualnih kodova, posebno za simetrične blokovne dizajne i njihove orbitne matrice. Također, na sličan način kao za simetrične dizajne, tu su konstruirani i još neki samodualni kodovi pomoću kvocijentnih matrica SGDD-a s dualnim svojstvom. Ove su konstrukcije inspirirane teoremom Assmusa, Mezzarobe i Salwacha iz [2].

Posljednji dio rada govori o PD-skupovima. Razvoj tehnologije stvorio je potrebu za dobrim kodovima za ispravljanje pogrešaka te učinkovitim metodama kodiranja i dekodiranja. Permutacijsko dekodiranje uvela je 1964. Jessie MacWilliams u [38]. Algoritam permutacijskog dekodiranja koristi skupove automorfizama koda koji se nazivaju PD-skupovi. Ova se metoda može koristiti kada kod ima dovoljno veliku grupu automorfizama koja osigurava postojanje PD-skupa. Tehnika je opisana u MacWilliams, Sloane ([39, Chapter 16]) i Huffman ([30, Chapter 8]). Pregled permutacijskog dekodiranja korištenjem kodova dobivenih iz kombinatoričkih struktura dan je u [34]. Algoritam je to učinkovitiji što je manja veličina PD-skupa. Donju granicu za veličinu PD-skupa dao je Gordon [25]. Pitanje je postoje li uopće PD-skupovi za određeni kod, jer se ne mora nužno svaki kod moći permutacijski dekodirati.

Zadnje, četvrto poglavlje, bavi se pronalaženjem PD-skupova za određene kodove povezane s flag-tranzitivnim simetričnim dizajnima. U njemu se dokazuje postojanje PD-skupova za sve kodove generirane matricom incidencije incidencijskog grafa flag-

tranzitivnog simetričnog dizajna. Pri tome se koriste rezultati o kodovima iz matrica incidencije grafova iz rada Dankelmann, Key, Rodrigues [19]. Zatim su konstruirani konkretni primjeri takvih PD-skupova za kodove povezane s flag-tranzitivnim simetričnim dizajnima. Flag-tranzitivne projektivne ravnine i dvoravnine proučavali su W. Kantor [33] i E. O'Reilly-Regueiro [42]. U ovom radu se proučavaju neki primjeri kodova proizašlih iz tih flag-tranzitivnih simetričnih dizajna te se za njih nalaze i manji PD-skupovi za specifične informacijske skupove. Na kraju se rezultat o PD-skupovima poopćuje i za flag-tranzitivne simetrične (grupovno) djeljive dizajne s dualnim svojstvom. Svi rezultati prikazani u posljednjem poglavlju, osim teorema 4.9, dani su u [14].

Poglavlje 1

Osnovni pojmovi

Za razumijevanje rada pretpostavlja se da je čitatelj upoznat s osnovnim pojmovima iz linearne algebre. Ovaj odjeljak započinjemo iznošenjem nekih definicija iz teorije grupa koje će nam trebati u nastavku. Točnije, opisujemo pojmove permutacijske grupe, te djelovanja grupe na skup. Također prikazujemo osnove teorije kodiranja, teorije grafova i teorije dizajna potrebne za razumijevanje preostalih poglavlja. Za detaljnije čitanje o navedenim temama upućujemo čitatelja na [5], [11], [30] i [35]. Teorije kodiranja, grafova, te dizajna tri su važna područja diskretne matematike. Međusobno su čvrsto isprepletena i povezana, te svako od njih može imati koristi od preostalih (vidi npr. [11]).

1.1 Grupe

Pretpostavlja se poznavanje temeljnih pojmova teorije grupa koji se mogu naći na primjer u [46].

1.1.1 Permutacijske grupe

Permutacijske grupe su nam važne, budući da su grupe automorfizama proizvoljnih incidencijskih struktura (na primjer blokovnih i djeljivih dizajna, koje ćemo definirati kasnije), također permutacijske grupe.

Definicija 1.1. Permutacija nepraznog skupa Ω je svaka bijekcija $\sigma : \Omega \to \Omega$.
Skup svih permutacija skupa Ω je grupa s obzirom na kompoziciju funkcija koja se naziva **simetrična grupa skupa** Ω i označava se sa $S(\Omega)$.
Svaka podgrupa simetrične grupe $S(\Omega)$ naziva se **permutacijska grupa** na Ω.

Napomena 1.1. Za $|\Omega| = n$ ($n \in \mathbb{N}$) kažemo da je $S(\Omega)$ simetrična grupa **stupnja** n i označavamo je sa S_n. Vrijedi da je $|S_n| = n!$.

Definicija 1.2. Neka je $G \leq S(\Omega)$. Kažemo da je točka $x \in \Omega$ **fiksna točka** permutacije $g \in G$ ako vrijedi: $g(x) = x$.

1.1.2 Djelovanje grupe na skup

Definicija 1.3. Djelovanje grupe G na skup Ω je funkcija $G \times \Omega \to \Omega$ (u notaciji $(g, x) \mapsto gx$) takva da za svaki $x \in \Omega$ i $g_1, g_2 \in G$ vrijedi:

1. $1x = x$,
2. $(g_1 g_2)x = g_1(g_2 x)$.

Primjer 1.1. Simetrična grupa S_n djeluje na skup $\{1, 2, ..., n\}$ sa $(g, x) \mapsto g(x)$.

Napomena 1.2. Neka grupa G djeluje na neprazan skup Ω. Na Ω je dana binarna relacija $\sim$ sa:

$$x \sim y \Leftrightarrow (\exists g \in G)\ gx = y.$$

Relacija $\sim$ je relacija ekvivalencije na skupu Ω (za dokaz vidi npr. [31]).

Definicija 1.4. Neka grupa G djeluje na neprazan skup Ω. **G-orbita** elementa $x \in \Omega$ je klasa ekvivalencije od x s obzirom na relaciju ekvivalencije $\sim$ definiranu ranije. Označavamo je sa Gx, odnosno:

$$Gx = \{gx \mid g \in G\}.$$

Element x se naziva **predstavnik** orbite Gx, a broj elemenata G-orbite naziva se **duljina** te orbite.

Napomena 1.3. Duljina orbite dijeli red grupe (vidi npr. [21]).

Definicija 1.5. Kažemo da je djelovanje grupe G na neprazan skup Ω **tranzitivno** ako postoji element $x \in \Omega$ takav da je $Gx = \Omega$, odnosno ako je cijeli skup Ω jedna orbita.

Napomena 1.4. Permutacijska grupa G na skupu Ω djeluje tranzitivno na skup Ω ako i samo ako

$$(\forall \alpha, \beta \in \Omega)\,(\exists\ g \in G)\ \ g(\alpha) = \beta.$$

1.2 Kodovi

Teorija kodiranja ima svoj izvor u teoriji informacija, a začetnik joj je Claude E. Shannon. Najraniji radovi iz teorije kodiranja bili su Shannonov rad ([47]) iz 1948., te radovi Golaya ([24]) iz 1949. i Hamminga ([28]) iz 1950. Nastala je zbog potrebe za učinkovitom i pouzdanom komunikacijom, tj. prijenosom informacija, u okruženju koje je često neprijateljsko. Teorija kodiranja bavi se prijenosom kodiranih informacija od pošiljatelja do primatelja kroz komunikacijski kanal sa smetnjama, te dekodiranjem, odnosno određivanjem originalne iz primljene poruke. Pri dekodiranju je potrebno ispraviti pogreške nastale zbog smetnji.

Usporedno sa sve jačim razvojem računalne tehnologije nastala je i potreba za razvojem teorije kodiranja, što je dovelo do konstrukcije novih, boljih kodova primjenjivih u praksi. Kod konstrukcija kodova teži se dobiti kodove s malom duljinom, velikom dimenzijom i velikom minimalnom udaljenosti, kako bi prijenos podataka bio brz, broj mogućih poruka velik, te kapacitet za ispravljanje pogrešaka što veći.

U ovom ćemo se radu baviti linearnim kodovima, a osobito će nam biti važni samoortogonalni i samodualni kodovi. Najveći dio rada posvećen je upravo konstrukciji samodualnih kodova uz pomoć kombinatoričkih dizajna (djeljivih dizajna i blokovnih dizajna). Neki od najboljih poznatih kodova su samodualni, kao na primjer prošireni Hammingov kod i prošireni Golayev kod.

Definicija 1.6. Kod C duljine n nad alfabetom Q je podskup $C \subseteq Q^n$.
Elementi koda nazivaju se **riječi koda**.

Definicija 1.7. Neka je p potencija prostog broja. Kod C naziva se p-naran **linearni kod** dimenzije m ako je $Q = \mathbb{F}_p$ i ako je C m-dimenzionalan potprostor vektorskog prostora $\mathbb{F}_p^n$.
Posebno, za $Q = \mathbb{F}_2$ kod se naziva **binaran**.

Definicija 1.8. Neka su $x = (x_1, ..., x_n)$ i $y = (y_1, ..., y_n) \in \mathbb{F}_p^n$. **Hammingova udaljenost** između riječi x i y je broj:

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

Definicija 1.9. Minimalna udaljenost koda C je:

$$d = \min\{d(x, y) : x, y \in C,\ x \neq y\}.$$

Svake dvije riječi koda razlikuju se u barem d koordinatnih pozicija. Znači da je minimalna udaljenost d jednaka najmanjem broju pogrešaka potrebnom da bi se jedna kodna riječ promijenila u drugu riječ koda.

Definicija 1.10. Težina riječi koda x je $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$.

Za linearan kod minimalna udaljenost može se jednostavnije izračunati pomoću sljedeće propozicije koja se može naći u [39].

Propozicija 1.1. *Minimalna udaljenost linearnog koda jednaka je minimalnoj težini njegovih nenul riječi, odnosno:*

$$d = \min\{w(x) : x \in C, x \neq 0\}.$$

Napomena 1.5. Kod koji je p-naran linearan kod duljine n, dimenzije k i minimalne udaljenosti d naziva se $[n, k, d]_p$ kod ili samo $[n, k, d]$ kod kad je jasno o kojem se alfabetu

radi. Ako su poznate duljina n, te dimenzija k linearnog koda, možemo također reći da je to linearan $[n, k]$ kod.

Kažemo da kod C može **detektirati** najviše s pogrešaka ako promjenom jedne kodne riječi iz koda u najviše s koordinatnih pozicija ne možemo dobiti drugu riječ iz koda C.

Propozicija 1.2. *Linearan $[n, k, d]$ kod C može detektirati najviše $d-1$ pogrešaka u jednoj riječi koda.*

Dokaz. Ukoliko se pri prijenosu jedne riječi koda dogodi $d-1$ ili manje pogrešaka, znači da se primljena riječ razlikuje od poslane u manje od d koordinatnih pozicija. Odnosno, dobivena riječ sigurno nije iz koda C (jer on ima minimalnu udaljenost d), pa znamo da je došlo do pogreške. □

Kažemo da kod C može **ispraviti** najviše t pogrešaka ako promjenom t ili manje koordinatnih pozicija u kodnoj riječi x, kodna riječ koja ima najmanju udaljenost od dobivene riječi i dalje ostaje x.

Sljedeći je teorem dokazan u [39].

Teorem 1.1. *Linearan $[n, k, d]$ kod može ispraviti najviše*

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

pogrešaka.

Definicija 1.11. Parametar t iz prethodnog teorema naziva se **kapacitet za ispravljanje pogrešaka** danoga linearnog $[n, k, d]$ koda.

Definicija 1.12. Dva su linearna koda **ekvivalentna** ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda i množenjem pojedine koordinate s nekim nenul elementom polja.

Definicija 1.13. Dva su linearna koda **izomorfna** ako se jedan može dobiti iz drugoga permutacijom koordinatnih pozicija.
Automorfizam koda C je izomorfizam sa C u C, tj. permutacija koordinatnih pozicija koja preslikava riječi koda u riječi koda.
Skup svih automorfizama linearnog koda C čini grupu koju nazivamo **puna grupa automorfizama** koda i označavamo s $Aut(C)$.

Definicija 1.14. Generirajuća matrica linearnog $[n, k]$ koda je $k \times n$ matrica čiji su retci vektori baze koda.
Kažemo da je generirajuća matrica linearnog $[n, k]$ koda u **standardnom obliku** ako je oblika $[I_k, A]$, gdje je I_k jedinična matrica reda k i A neka $k \times (n-k)$ matrica.

Napomena 1.6. Svaki je linearan kod ekvivalentan linearnom kodu zadanom generirajućom matricom u standardnom obliku.

Napomena 1.7. Neka je p prost broj, te A cjelobrojna matrica. Pomoću matrice A možemo dobiti p-naran kod tako da uzmemo prostor razapet retcima od A ili pak stupcima od A modulo p. Dimenzija tako dobivenog koda jednaka je p-rangu od A. Uvodimo sljedeće oznake:

1. $row_p(A)$ - p-naran linearan kod razapet retcima od A,
2. $col_p(A)$ - p-naran linearan kod razapet stupcima od A.

Definicija 1.15. Kažemo da je linearan kod **dvostruko paran** ako mu je težina svake riječi djeljiva sa 4.

U nastavku ćemo definirati samoortogonalne i samodualne kodove. U tu svrhu podsjetit ćemo se definicije skalarnog produkta, koji se u slučaju vektorskih prostora nad konačnim poljima definira kao simetrična bilinearna forma.

Definicija 1.16. Neka je V vektorski prostor nad konačnim poljem $\mathbb{F}$. **Skalarni produkt** (ili **unutarnji produkt**) na V je preslikavanje $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ sa sljedećim svojstvima:

1. $\langle x_1 + x_2, y \rangle = \langle x_1, y \rangle + \langle x_2, y \rangle$, $\forall x_1, x_2, y \in V$,
2. $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$, $\forall \alpha \in \mathbb{F}$, $\forall x, y \in V$,
3. $\langle x, y \rangle = \langle y, x \rangle$, $\forall x, y \in V$.

Napomena 1.8. Standardni (euklidski) skalarni produkt vektora $x = (x_1, ..., x_n)$ i $y = (y_1, ..., y_n)$, za $x, y \in \mathbb{F}_p^n$, je skalar:

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

Definicija 1.17. Neka je $C \subseteq \mathbb{F}_p^n$ linearan kod. Njegov **dualan kod** je kod:

$$C^{\perp} = \{x \in \mathbb{F}_p^n \mid \langle x, c \rangle = 0, \ \forall c \in C\},$$

gdje je $\langle \cdot, \cdot \rangle$ standardni unutarnji produkt. Kod C naziva se:

a) **samoortogonalan** ako je $C \subseteq C^{\perp}$,

b) **samodualan** ako je $C = C^{\perp}$.

Napomena 1.9. Vrijede sljedeće činjenice o dimenzijama samodualnih i samoortogonalnih kodova.

a) Ako je C samodualan kod duljine n nad $\mathbb{F}_p$, tada je n paran i vrijedi:

$$\dim(C) = \frac{n}{2}.$$

To slijedi iz činjenice da je $\dim(C) + \dim(C^\perp) = n$.

b) Za samoortogonalan kod vrijedi $\dim(C) \leq \frac{n}{2}$.

Iz navedenih činjenica lako se dokazuju i sljedeće dvije tvrdnje propozicije.

Propozicija 1.3. *Neka je C linearan $[n, k, d]$ kod s generirajućom matricom G.*

1. *C je **samoortogonalan** ako i samo ako je $GG^T = 0$.*
2. *C je **samodualan** ako i samo ako je samoortogonalan i $k = \frac{n}{2}$.*

Primjer 1.2. Neka je C binaran $(8, 4, 4)$-kod s generirajućom matricom:

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

(C se naziva prošireni Hammingov kod reda 3). Kod C je samodualan, budući da je $GG^T = 0$.

Analogno kao za samodualan kod u odnosu na uobičajeni skalarni produkt, možemo definirati i kod koji je samodualan u odnosu na proizvoljan skalarni produkt.

Definicija 1.18. Neka je U simetrična nesingularna matrica nad poljem $\mathbb{F}_p$. Skalarni produkt $\langle \cdot, \cdot \rangle_U$ za retčane vektore u $\mathbb{F}_p^n$ dan je kao:

$$\langle a, c \rangle_U = aUc^T.$$

U-dualan kod linearnog koda C je kod

$$C^U = \{a \in \mathbb{F}_p^n \mid \langle a, c \rangle_U = 0, \ \forall c \in C\}.$$

Kod C naziva se:

a) **U-samoortogonalan**, ili samoortogonalan u odnosu na U, ako je $C \subseteq C^U$,

b) **U-samodualan**, ili samodualan u odnosu na U, ako je $C = C^U$.

Napomena 1.10. Za $U = I$ skalarni produkt u odnosu na U jednak je standardnom skalarnom produktu za vektore iz $\mathbb{F}_p^n$.

1.3 Grafovi

Teorija grafova ima svoje začetke u modeliranju mreža. Sam početak njenog razvoja povezuje se s Eulerovim rješavanjem problema Königsbergških mostova iz 1736. godine, objavljenom 1741. u radu [22].

U drugom ćemo poglavlju ovoga rada koristiti primjere grafova-djeljivih dizajna (DDG-ova) i digrafova-djeljivih dizajna (DDD-ova) za konstrukciju samodualnih kodova u odnosu na određeni skalarni produkt. U četvrtom poglavlju bavit ćemo se pronalaženjem PD-skupova za kodove razapete retcima matrica incidencije određenih grafova povezanih s dizajnima. Točnije bit će nam zanimljivi incidencijski grafovi simetričnih dizajna i simetričnih grupovno djeljivih dizajna.

U nastavku uvodimo osnove teorije grafova koje su nam potrebne.

Definicija 1.19. Graf Γ je uređena trojka (V, E, ψ), gdje je V neprazan skup **vrhova**, E skup **bridova** disjunktan s V i ψ funkcija incidencije koja svakom bridu pridružuje par (ne nužno različitih) vrhova.

Definicija 1.20. Ako su nekom bridu $e \in E$ grafa $\Gamma = (V, E, \psi)$ pridruženi vrhovi $u, v \in V$, kažemo da su u i v **krajevi** brida e. Također kažemo da su vrhovi u i v **susjedni** ukoliko su incidentni s istim bridom e. Analogno, dva su brida u grafu **susjedna** ako su incidentna s istim vrhom.

Definicija 1.21. Susjedstvo vrha v grafa Γ je skup svih vrhova grafa koji su susjedni s vrhom v.

Definicija 1.22. Brid u grafu koji je incidentan samo s jednim vrhom zove se **petlja**.

Definicija 1.23. Kažemo da je graf **jednostavan** ako ne sadrži petlje ni višestruke bridove.

Mi ćemo govoriti o grafovima koji su jednostavni, odnosno bez petlji (bridu se pridružuju dva različita vrha) i bez višestrukih bridova.

Definicija 1.24. Potpuni graf je jednostavan graf u kojem su svaka dva vrha susjedna. Potpuni graf s n vrhova označavat ćemo s K_n.

Definicija 1.25. Šetnja u grafu $\Gamma = (V, E, \psi)$ je netrivijalan konačan niz

$$W = v_0 e_1 v_1 e_2 v_2 \dots e_k v_k,$$

za $v_0, \dots v_k \in V$ i $e_1, \dots e_k \in E$, pri čemu su vrhovi v_{i-1} i v_i incidentni s bridom e_i, $i \in \{1, \dots, k\}$. Kaže se da je W šetnja od v_0 do v_k ili $(v_0, v_k)-$šetnja. Broj k se naziva **duljina šetnje** W.

Definicija 1.26. Šetnja $W = v_0e_1v_1e_2v_2 \dots e_kv_k$ je **zatvorena** ako ima pozitivnu duljinu i ako je $v_0 = v_k$.

Definicija 1.27. Ako su svi vrhovi $v_0, \dots v_k$ u šetnji W međusobno različiti onda kažemo da je W **put**.

Definicija 1.28. Ako u grafu Γ postoji put između vrhova u i v, tada kažemo da su u i v **povezani**. Za graf Γ kažemo da je **povezan** ako između svaka dva vrha u grafu postoji put.

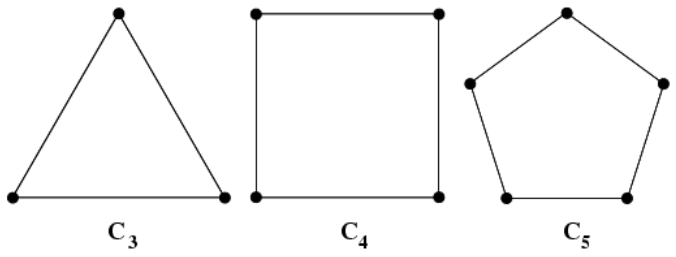
Definicija 1.29. Udaljenost između vrhova u i v grafa Γ je duljina najkraćeg puta između u i v ako su oni povezani, a ako ne postoji put između njih tada stavljamo da je udaljenost između njih jednaka ∞.

Definicija 1.30. Dijametar, diam(Γ), grafa Γ je maksimalna udaljenost između dva vrha od Γ.

Definicija 1.31. Zatvorena šetnja kod koje su svi vrhovi osim početnog i krajnjeg vrha međusobno različiti zove se **ciklus**.

Definicija 1.32. Struk grafa Γ je duljina najkraćeg ciklusa u Γ, a ako Γ nema ciklusa tada stavljamo da je struk jednak ∞.

Definicija 1.33. Ciklički graf C_n je graf sa n vrhova $v_0, ..., v_{n-1}$ i n bridova takav da je vrh v_i povezan sa dva susjedna vrha v_{i-1} i v_{i+1} (mod n).



Slika 1.1: Ciklički grafovi

Definicija 1.34. Stupanj vrha $u \in V$ je broj vrhova susjednih sa u.

Napomena 1.11. Minimalni stupanj vrha u grafu Γ označit ćemo sa $\delta(\Gamma)$.

Definicija 1.35. Graf je k**-regularan** ($k \in \mathbb{N}_0$) ako su mu svi vrhovi stupnja k.

Bose je 1963. godine uveo važnu klasu grafova pod nazivom jako regularni grafovi.

Definicija 1.36. Za graf Γ s v vrhova kažemo da je **jako regularan graf** s parametrima (v, k, λ, μ) ako je jednostavan, k-regularan i ako:

a) svaka dva susjedna vrha imaju točno λ zajedničkih susjednih vrhova,

b) svaka dva nesusjedna vrha imaju točno μ zajedničkih susjednih vrhova.

Napomena 1.12. Jako regularan graf s parametrima (v, k, λ, μ) označavat ćemo sa

$$SRG(v, k, \lambda, \mu).$$

Kratica SRG dolazi iz engleskog naziva *strongly regular graph*.

Nužan uvjet za egzistenciju $SRG(v, k, \lambda, \mu)$ dan je u sljedećem teoremu, čiji se dokaz može naći u [3].

Teorem 1.2. *Neka je* Γ *jako regularan graf* $SRG(v, k, \lambda, \mu)$*. Tada vrijedi:*

$$k(k - \lambda - 1) = (v - k - 1)\mu.$$

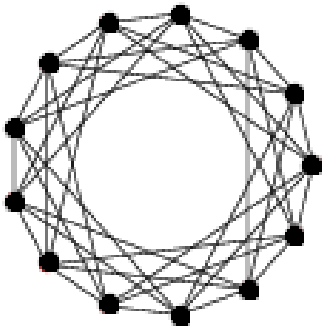
Definicija 1.37. Neka je q potencija prostog broja takva da je $q \equiv 1 (\text{mod } 4)$. **Paleyev graf** reda q, u oznaci $P(q)$ [1], je graf čiji je skup vrhova $V = \mathbb{F}_q$, pri čemu su dva vrha u i v susjedna ako je $u - v \in (\mathbb{F}_q^\times)^2$, odnosno ako im je razlika kvadrat u $\mathbb{F}_q$ različit od nule.

Primjer 1.3. Paleyev graf reda 13, $P(13)$, dan je na slici 1.2. Skup vrhova mu je:

$$V = \{0, 1, ..., 12\}.$$

Svaki vrh v povezan je sa šest susjednih vrhova:

$$v \pm 1 (\text{mod } 13),\ v \pm 3 (\text{mod } 13),\ v \pm 4 (\text{mod } 13).$$



Slika 1.2: Paleyev graf $P(13)$

[1] Paleyevi grafovi obično se označavaju s $P(q)$ ili $QR(q)$, gdje QR označava kvadratni ostatak, tj. engleski *quadratic residue* (vidi npr. [10]).

Napomena 1.13. Paleyev graf $P(q)$ je jako regularan graf s parametrima:

$$SRG\left(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1)\right).$$

Definicija 1.38. Neka je $\Gamma = (V, E, \psi)$ graf sa skupom vrhova $V = \{v_1, ..., v_\nu\}$ i skupom bridova $E = \{e_1, ..., e_\varepsilon\}$.

a) **Matrica susjedstva** grafa Γ je $|V| \times |V|$ matrica $A = [a_{ij}]$, gdje je:

$$a_{ij} = \begin{cases} 1 & \text{ako su vrhovi } v_i \text{ i } v_j \text{ susjedni,} \\ 0 & \text{inače.} \end{cases}$$

b) **Matrica incidencije** grafa Γ je $|V| \times |E|$ matrica $G = [g_{ij}]$, gdje je:

$$g_{ij} = \begin{cases} 1 & \text{ako je vrh } v_i \text{ incidentan s bridom } e_j, \\ 0 & \text{inače.} \end{cases}$$

Primjer 1.4. Pentagon $C_5 = P(5)$ je $SRG(5, 2, 0, 1)$ prikazan na slici 1.1, a njegova matrica susjedstva dana je sa:

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

Definicija 1.39. Dva su grafa $\Gamma_1 = (V_1, E_1, \psi_1)$ i $\Gamma_2 = (V_2, E_2, \psi_2)$ **izomorfna** ako postoje bijekcije $\theta : V_1 \to V_2$ i $\phi : E_1 \to E_2$ takve da:

$$\psi_1(e) = uv \text{ ako i samo ako } \psi_2(\phi(e)) = \theta(u)\theta(v).$$

Takav par preslikavanja (θ, ϕ) naziva se **izomorfizam** grafova Γ_1 i Γ_2.
Automorfizam grafa Γ je izomorfizam sa Γ u Γ.

Definicija 1.40. Graf $\Gamma = (V, E, \psi)$ je **bipartitan** ako se V može particionirati u dvije klase takve da svaki brid ima krajeve u različitim klasama.
Potpun bipartitan graf je bipartitan graf u kojem su svaka dva vrha iz različitih klasa povezana bridom.

U posljednjem poglavlju koristit ćemo i sljedećih nekoliko pojmova.

Definicija 1.41. Povezanost bridovima $\lambda(\Gamma)$ povezanog grafa Γ je minimalan broj bridova čijim uklanjanjem graf postaje nepovezan.
Most povezanog grafa je brid čijim uklanjanjem dobijemo nepovezan graf.

Napomena 1.14. Vrijede sljedeće tvrdnje:

a) Graf Γ ima most ako i samo ako je $\lambda(\Gamma) = 1$.

b) Za svaki graf Γ je $\lambda(\Gamma) \leq \delta(\Gamma)$. Ovo slijedi direktno iz činjenice da uklanjanje bridova incidentnih s vrhom stupnja $\delta(\Gamma)$ ostavlja graf koji je nepovezan.

Definicija 1.42. Graf Γ je **super-λ** ako $\lambda(\Gamma) = \delta(\Gamma)$ i jedini skupovi bridova kardinalnosti $\lambda(\Gamma)$ čije uklanjanje daje nepovezan graf su skupovi bridova incidentnih s vrhom stupnja $\delta(\Gamma)$.

Definicija 1.43. Kažemo da je graf Γ **tranzitivan na vrhovima (odnosno bridovima)** ako njegova puna grupa automorfizama $Aut(G)$ djeluje tranzitivno na skup vrhova grafa (odnosno skup bridova).

1.4 Dizajni

Osnove teorije dizajna imaju svoje izvore u statistici, gdje su se počele koristiti u dizajnu bioloških eksperimenata u radu Ronalda Fishera u 1920-ima.

Teorija dizajna bavi se pitanjima o mogućnosti raspoređivanja elemenata konačnog skupa u podskupove na način da određena svojstva "ravnoteže" budu zadovoljena [48]. Između ostaloga bavi se blokovnim dizajnima, Hadamardovim matricama, latinskim kvadratima, diferencijskim skupovima i drugim strukturama. Nama će u nastavku rada od posebne važnosti biti upravo blokovni dizajni, te (grupovno) djeljivi dizajni. U poglavljima koja slijede nakon uvodnog dijela, te će nam dvije vrste kombinatoričkih dizajna poslužiti za konstrukciju samodualnih kodova, te za pronalaženje određenih PD-skupova.

Blokovne i djeljive dizajne definirat ćemo uz pomoć pojma incidencijske strukture.

Definicija 1.44. 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 **točkama**, elemente skupa $\mathcal{B}$ **blokovima**, a relaciju $\mathcal{I}$ nazivamo **relacijom incidencije**.
Kažemo da je incidencijska struktura **konačna** ako su skupovi $\mathcal{P}$ i $\mathcal{B}$ konačni.

Definicija 1.45. U incidencijskoj strukturi $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, 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 1.4. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura s v točaka i b blokova, te neka su stupnjevi točaka $r_1, ..., r_v$ i stupnjevi blokova $k_1, ..., k_b$. Tada vrijedi:*

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

Dokaz. Tvrdnja se dokazuje prebrojavanjem na dva načina elemenata skupa

$$\{(P, x) \in \mathcal{P} \times \mathcal{B} \mid (P, x) \in \mathcal{I}\}.$$

□

Kao posljedicu dobivamo sljedeći korolar.

Korolar 1.1. *Ako je u incidencijskoj strukturi s v točaka i b blokova svaka točka stupnja r i svaki blok stupnja k, tada vrijedi:*

$$vr = bk.$$

Definicija 1.46. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura. **Dualna struktura** strukture $\mathcal{D}$ je struktura $\mathcal{D}^* = (\mathcal{P}^*, \mathcal{B}^*, \mathcal{I}^*)$, gdje je $\mathcal{P}^* = \mathcal{B}$, $\mathcal{B}^* = \mathcal{P}$, a relacija incidencije dana je sa:

$$\mathcal{I}^* = \{(x, P) \mid (P, x) \in \mathcal{I}\}.$$

Definicija 1.47. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura. **Komplementarna struktura** strukture $\mathcal{D}$ je struktura $\mathcal{D}' = (\mathcal{P}, \mathcal{B}, \mathcal{I}')$, gdje je $\mathcal{I}' = \mathcal{P} \times \mathcal{B} \setminus \mathcal{I}$.

Definicija 1.48. Izomorfizam incidencijskih struktura $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, \mathcal{I}_1)$ i $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2, \mathcal{I}_2)$ je bijektivno preslikavanje $f : \mathcal{P}_1 \cup \mathcal{B}_1 \to \mathcal{P}_2 \cup \mathcal{B}_2$ takvo da:

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

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

Definicija 1.49. Skup svih automorfizama incidencijske strukture $\mathcal{D}$ je grupa s obzirom na kompoziciju funkcija i naziva se **puna grupa automorfizama** strukture $\mathcal{D}$ i označavamo ju sa $Aut(\mathcal{D})$.
Svaka njezina podgrupa naziva se **grupa automorfizama** od $\mathcal{D}$.

U nastavku ćemo definirati posebnu vrstu konačne incidencijske strukture pod nazivom blokovni dizajn.

Definicija 1.50. Blokovni dizajn ili $2-(v, k, \lambda)$ **dizajn** je konačna incidencijska struktura $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ takva da vrijedi:

1. $|\mathcal{P}| = v$,
2. svaki blok je incidentan s točno k točaka,
3. svaki par točaka je incidentan s točno λ blokova.

Ako je $v = b$, onda kažemo da je blokovni dizajn **simetričan**.

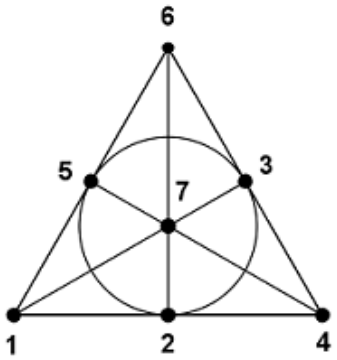
Napomena 1.15. Blokovni dizajni, odnosno 2-dizajni se često još nazivaju i balansirani nepotpuni blok dizajni ili BIBD (*balanced incomplete block designs*)[2].

Primjer 1.5. Fanova ravnina prikazana na slici 1.3 je simetrični $2-(7,3,1)$ dizajn zadan skupom točaka

$$\mathcal{P} = \{1,2,3,4,5,6,7\},$$

te skupom blokova

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



Slika 1.3: Simetrični 2-$(7,3,1)$ dizajn

Sljedeća tri teorema dokazana su u [48].

Teorem 1.3. *U* $2-(v,k,\lambda)$ *dizajnu svaka je točka incidentna s točno*

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

blokova.

Teorem 1.4. *Broj blokova* $2-(v,k,\lambda)$ *dizajna jednak je:*

$$b = \frac{vr}{k} = \frac{\lambda(v^2-v)}{k^2-k}.$$

Teorem 1.5. *U* $2-(v,k,\lambda)$ *dizajnu vrijedi:* $b \geq v$.

Nejednakost iz prethodnog teorema naziva se **Fisherova nejednakost**.

Definicija 1.51. Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn. **Red** dizajna $\mathcal{D}$ je broj $n = r - \lambda$.

[2]Vidi npr. [48].

Sljedeći važan teorem daje nužan uvjet za postojanje simetričnog (v, k, λ)-dizajna, a dokaz mu se može naći npr. u [27]. Poznat je kao Bruck-Ryser-Chowla teorem.

Teorem 1.6. *Ako postoji simetričan (v, k, λ)-dizajn, gdje je $n = k - \lambda$, tada:*

1. *ako je v paran, n je kvadrat,*

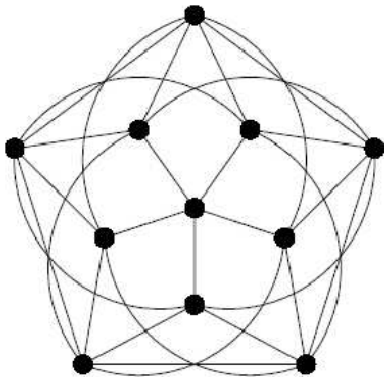
2. *ako je v neparan, tada jednadžba*

$$x^2 = ny^2 + (-1)^{\frac{v-1}{2}} \lambda z^2,$$

ima rješenje u cijelim brojevima x, y, z, koji nisu svi jednaki 0.

Definicija 1.52. Simetričan $(v, k, 1)$-dizajn se naziva **projektivna ravnina** reda $k - 1$, a simetričan $(v, k, 2)$-dizajn se naziva **dvoravnina**.

Primjer 1.6. (**Paleyeva dvoravnina**) Primjer $2 - (11, 5, 2)$ dizajna je Paleyeva dvoravnina prikazana na slici 1.4. To je do na izomorfizam jedina dvoravnina s navedenim parametrima.



Slika 1.4: Paleyeva dvoravnina

Definicija 1.53. Za blokovni dizajn kažemo da je **jednostavan** ako ne sadrži ponovljene blokove.

U ovom ćemo radu promatrati samo jednostavne blokovne dizajne.

Svakom blokovnom dizajnu možemo pridružiti matricu na sljedeći način.

Definicija 1.54. Neka je $\mathcal{P} = \{x_1, ..., x_v\}$ i $\mathcal{B} = \{B_1, ..., B_b\}$. **Matrica incidencije** blokovnog dizajna $\mathcal{D} = \{\mathcal{P}, \mathcal{B}, \mathcal{I}\}$ je $v \times b$ matrica $A = [a_{ij}]$, gdje je

$$a_{ij} = \begin{cases} 1, & \text{ako je } (x_i, B_j) \in \mathcal{I}, \\ 0, & \text{ako } (x_i, B_j) \notin \mathcal{I}. \end{cases}$$

Primjer 1.7. Matrica incidencije Fanove ravnine dana je sa:

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

Dokaz sljedećeg teorema može se naći u [48].

Teorem 1.7. *Neka je M $(0,1)$-matrica dimenzije $v \times b$. M je matrica incidencije $2-(v,k,\lambda)$ dizajna ako i samo ako vrijedi:*

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

gdje je I_v jedinična matrica reda v, J_v matrica reda v čiji su svi elementi jednaki 1, a j_v i j_b vektori čiji su svi elementi jednaki 1 duljine v, odnosno b.

Napomena 1.16. Ako je M matrica incidencije blokovnog dizajna $\mathcal{D}$, tada je matrica incidencije njemu komplementarnog dizajna $\mathcal{D}'$ matrica $J - M$.

Sljedeći teorem dokazan je u [1].

Teorem 1.8. *Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn s $v-k \geq 2$. Tada je njegov komplementarni dizajn $\mathcal{D}'$ $2-(v,v-k,\lambda')$ dizajn, gdje je:*

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

U nastavku uvodimo pojam taktičke dekompozicije matrice, te taktičke dekompozicije blokovnog dizajna.

Definicija 1.55. Neka je M $v \times b$ matrica. **Dekompozicija** od M je particija $P_1, ..., P_n$ redaka od M i particija $B_1, ..., B_m$ stupaca od M. Stavimo da je:

$$|P_i| = \omega_i,\ |B_j| = \Omega_j,\ \text{ za } 1 \leq i \leq n,\ 1 \leq j \leq m.$$

Sa $M_{i,j}$ označimo $\omega_i \times \Omega_j$ matricu koja se sastoji od elemenata iz presjeka redaka iz P_i i stupaca iz B_j. Kažemo da je dekompozicija matrice M:

a) **taktička po retcima** ako je za $i = 1, ..., n$ i $j = 1, ..., m$ suma elemenata u svakom retku matrice $M_{i,j}$ konstantna,

b) **taktička po stupcima** ako je za $i = 1, ..., n$ i $j = 1, ..., m$ suma elemenata u svakom stupcu matrice $M_{i,j}$ konstantna,

c) **taktička** ako je taktička po retcima i po stupcima.

Definicija 1.56. Kažemo da je particija skupa točaka i skupa blokova blokovnog dizajna $\mathcal{D}$ **taktička** ako odgovara taktičkoj dekompoziciji njegove matrice incidencije.

Primjer 1.8. Trivijalni primjeri taktičkih dekompozicija skupova točaka i blokova blokovnih dizajna:

a) dekompozicija u kojoj su sve točke dizajna u jednoj klasi i svi blokovi dizajna zajedno u jednoj klasi,

b) dekompozicija u kojoj su sve klase točaka i sve klase blokova jednočlane.

Napomena 1.17. Kasnije ćemo pokazati kako djelovanje grupe automorfizama dizajna na blokovni dizajn inducira taktičku dekompoziciju dizajna.

Poglavlje 2

Simetrični grupovno djeljivi dizajni

U ovom poglavlju uvest ćemo konstrukciju samodualnih kodova iz proširenih kvocijentnih matrica simetričnih (grupovno) djeljivih dizajna (SGDD-a) s dualnim svojstvom. Konstrukcija je objavljena u članku [15]. Rezultati su dobiveni razvijanjem ideja prezentiranih u [35] i [52], te posebno u [17] gdje je dana konstrukcija samodualnih kodova iz proširenih orbitnih matrica simetričnih dizajna u odnosu na djelovanje grupe automorfizama koja djeluje sa svim orbitama iste duljine.

Također, u nastavku ćemo naći i primjere SGDD-a s dualnim svojstvom dobivene iz grafova-djeljivih dizajna (DDG-ova) i digrafova-djeljivih dizajna (DDD-ova), te pomoću njihovih kvocijentnih matrica konstruirati samodualne kodove.

2.1 Simetrični grupovno djeljivi dizajni

Definicija djeljivog dizajna (također često zvanog grupovno djeljivi dizajn) varira. Ovdje koristimo definiciju analognu onoj koju daje Bose u [7].

Djeljivi su dizajni proučavani zbog primjene u statistici te zbog njihove univerzalne primjene na konstrukciju novih dizajna ([40], [49], [50]).

Definicija 2.1. Incidencijska struktura s v točaka, b blokova i konstantnom veličinom blokova k u kojoj je svaka točka incidentna s točno r blokova je **(grupovno) djeljivi dizajn** (GDD) s parametrima $(v, b, r, k, \lambda_1, \lambda_2, m, n)$, u oznaci $\mathcal{D}(v, b, r, k, \lambda_1, \lambda_2, m, n)$, ako se skup točaka može particionirati u m klasa veličine n, tako da su:

1. dvije točke iz iste klase sadržane zajedno u točno λ_1 blokova,

2. dvije točke iz različitih klasa sadržane zajedno u točno λ_2 blokova.

Napomena 2.1. Za djeljivi dizajn $\mathcal{D}(v, b, r, k, \lambda_1, \lambda_2, m, n)$ očito je da vrijedi:

a) $v = mn$, jer m klasa od po n točaka particioniraju skup od v točaka,

b) $vr = bk$, zbog korolara 1.1.

Propozicija 2.1. *Za djeljivi dizajn s parametrima* $(v, b, r, k, \lambda_1, \lambda_2, m, n)$ *vrijedi sljedeća jednakost:*

$$(n-1)\lambda_1 + n(m-1)\lambda_2 = r(k-1).$$

Dokaz. Neka je skup točaka djeljivog dizajna označen sa $\mathcal{P}$. Neka je P neka točka iz $\mathcal{P}$. Točka P nalazi se u r blokova, od kojih svaki sadrži još po $k-1$ preostalih točaka. Time dobivamo $r(k-1)$ parova točaka čiji jedan član je P, a zajedno se nalaze u bloku. S druge strane, za svaku od $n-1$ točaka iz iste klase kao P imamo λ_1 odgovarajućih parova, dok u $m-1$ ostalih klasa svaka od n točaka daje po λ_2 odgovarajućih parova sa P. □

Dokaz sljedeće propozicije može se naći u [8].

Propozicija 2.2. *Neka je* $\mathcal{D}(v, b, r, k, \lambda_1, \lambda_2, m, n)$ *djeljivi dizajn. Tada vrijedi:*

$$rk \geq v\lambda_2.$$

Napomena 2.2. Iz definicije slijedi da je djeljivi dizajn blokovni dizajn ako i samo ako je ili $n = 1$ ili $\lambda_1 = \lambda_2$ ([32]).

Definicija 2.2. Ako je $n \neq 1$ i $\lambda_1 \neq \lambda_2$, tada se djeljivi dizajn naziva **pravi**.

Napomena 2.3. Za matricu incidencije N grupovno djeljivog dizajna, determinanta od NN^T dana je sa

$$\det(NN^T) = rk(r-\lambda_1)^{m(n-1)}(rk - v\lambda_2)^{m-1},$$

i vlastite vrijednosti od NN^T su

$$rk,\ r-\lambda_1,\ rk-v\lambda_2$$

s kratnostima 1, $m(n-1)$ i $m-1$, redom (vidi [45]).

Definicija 2.3. Bose i Connor ([8]) klasificirali su djeljive dizajne u tri tipa u terminima vlastitih vrijednosti:

1. **singularan** ako je $r - \lambda_1 = 0$,
2. **nesingularan** ako je $r - \lambda_1 > 0$
   a) **semi-regularan** ako je $rk - v\lambda_2 = 0$,
   b) **regularan** ako je $rk - v\lambda_2 > 0$.

Definicija 2.4. GDD se naziva **simetričan** GDD (SGDD) ako je $v = b$ (ili, ekvivalentno, $r = k$). Tada se označava sa $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ i slijedi:

$$v = mn, \quad (n-1)\lambda_1 + n(m-1)\lambda_2 = k(k-1), \quad k^2 \geq v\lambda_2.$$

Definicija 2.5. Kažemo da SGDD $\mathcal{D}$ ima **dualno svojstvo** ako je dual od $\mathcal{D}$ opet djeljivi dizajn s istim parametrima kao $\mathcal{D}$.

Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom. Tada se blokovi od $\mathcal{D}$ mogu podijeliti u skupove $S_1, ..., S_m$, od kojih svaki sadrži n blokova, tako da se svaka dva bloka koja pripadaju istom skupu sijeku u λ_1 točaka, a svaka dva bloka koja pripadaju različitim skupovima sijeku se u λ_2 točaka.

Primjer 2.1. SGDD s dualnim svojstvom $\mathcal{D}(6, 3, 2, 1, 3, 2)$ dan je skupom točaka $\mathcal{P} = \{0, 1, 2, 3, 4, 5\}$, skupom blokova

$$\mathcal{B} = \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 0\}, \{4, 5, 1\}, \{5, 0, 2\}\}$$

te klasama točaka $\{0, 3\}$, $\{1, 4\}$, $\{2, 5\}$.

Ističemo da se ono što mi zovemo "s dualnim svojstvom" katkad naziva "simetričan", "simetričan" u našem smislu ($v = b$) se tada zove "kvadratan" (vidi na primjer [32]).

2.2 Kodovi iz kvocijentnih matrica simetričnih grupovno djeljivih dizajna s dualnim svojstvom

Particije točaka i blokova iz definicije SGDD-a s dualnim svojstvom daju particiju (koju ćemo zvati **kanonska particija**) matrice incidencije

$$N = \begin{bmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{bmatrix},$$

gdje su A_{ij} kvadratne podmatrice reda n.

Sa I_n ćemo označiti $n \times n$ jediničnu matricu, a sa J_n označimo $n \times n$ matricu čiji su svi elementi jednaki jedan. Tada se matrica NN^T može zapisati na sljedeći način:

$$NN^T = \begin{bmatrix} B_{11} & \cdots & B_{1m} \\ \vdots & \ddots & \vdots \\ B_{m1} & \cdots & B_{mm} \end{bmatrix},$$

gdje je

$$B_{ij} = [(k - \lambda_1)I_n + (\lambda_1 - \lambda_2)J_n]\delta_{ij} + \lambda_2 J_n,$$

i δ_{ij} je Kroneckerov delta simbol.

Teorem 2.1. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom i neka je N matrica incidencije od $\mathcal{D}$. Ako je p prost broj takav da $p \mid \lambda_1$, $p \mid k$ i $p \mid \lambda_2$, tada retci od N razapinju samoortogonalan kod duljine v nad $\mathbb{F}_p$.*

Dokaz. Tvrdnja slijedi iz činjenice da je NN^T nul-matrica modulo p, budući da njezini elementi poprimaju vrijednosti iz skupa $\{k, \lambda_1, \lambda_2\}$. □

Bose je pokazao u [7] da opisana kanonska particija matrice incidencije N daje taktičku dekompoziciju, odnosno da svaki blok A_{ij} ima konstantnu sumu redaka (i stupaca). To nam omogućuje da definiramo kvocijentnu matricu SGDD-a na sljedeći način.

Definicija 2.6. Kažemo da je $m \times m$ matrica $R = [r_{ij}]$ **kvocijentna matrica** SGDD-a s dualnim svojstvom ako je svaki element r_{ij} jednak retčanoj sumi bloka A_{ij} iz kanonske particije matrice incidencije.

Napomena 2.4. Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom s kvocijentnom matricom $R = [r_{ij}]$. Označimo klase točaka od $\mathcal{D}$ sa $T_1, ..., T_m$, a klase blokova od $\mathcal{D}$ sa $S_1, ..., S_m$. Tada je svaka točka iz T_i sadržana u točno r_{ij} blokova iz S_j i svaki blok iz S_j sadrži točno r_{ij} točaka iz T_i.

	{0,1,3}	{0,3,4}	{1,2,4}	{1,4,5}	{0,2,5}	{2,3,5}
0	1	1	0	0	1	0
3	1	1	0	0	0	1
1	1	0	1	1	0	0
4	0	1	1	1	0	0
2	0	0	1	0	1	1
5	0	0	0	1	1	1

Tablica 2.1: Incidencija točaka i blokova za SGDD $\mathcal{D}(6, 3, 2, 1, 3, 2)$ iz primjera 2.1

Primjer 2.2. Neka je $\mathcal{D}$ SGDD iz primjera 2.1. Ako poredamo točke i blokove od $\mathcal{D}$ kao što je prikazano u tablici 2.1, dobivamo da je matrica incidencije djeljivog dizajna $\mathcal{D}$ dana sa:

$$N = \left[\begin{array}{cc|cc|cc} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right].$$

Slijedi da je kvocijentna matrica od $\mathcal{D}$ jednaka:

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

Napomena 2.5. Kvocijentna matrica zadovoljava (Bose [7]) sljedeće uvjete:

$$RR^T = [(k - \lambda_1) + n(\lambda_1 - \lambda_2)]I_m + n\lambda_2 J_m = (k^2 - v\lambda_2)I_m + n\lambda_2 J_m, \tag{2.1}$$

$$RJ_m = J_m R = kJ_m, \tag{2.2}$$

što znači da je suma svakog retka i svakog stupca od R jednaka k.

Nadalje, budući da je $\det(RR^T) = k^2 \left(k^2 - v\lambda_2\right)^{m-1}$, slijedi da je determinanta od R dana sa:

$$|\det(R)| = k\left(k^2 - v\lambda_2\right)^{\frac{m-1}{2}}. \tag{2.3}$$

Teorem 2.2. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom i neka je R kvocijentna matrica od $\mathcal{D}$. Ako je p prost broj takav da $p \nmid (k^2 - v\lambda_2)$ i $p \nmid k$, tada linearan kod nad $\mathbb{F}_p$ razapet retcima od R ima dimenziju m.*

Dokaz. Budući da $|det(R)| = k\left(k^2 - v\lambda_2\right)^{\frac{m-1}{2}}$, matrica R je invertibilna nad $\mathbb{F}_p$. Dakle, slijedi da je p-rang od R jednak m. □

Napomena 2.6. Neka je A $a \times b$ matrica, te B $b \times c$ matrica. Tada je

$$r(AB) \leq min\{r(A), r(B)\}.$$

Specijalno, za matricu A vrijedi:

$$r(AA^T) \leq min\{r(A), r(A^T)\} = r(A).$$

Ova činjenica će se koristiti u dokazu sljedećeg teorema.

Teorem 2.3. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom i R kvocijentna matrica od $\mathcal{D}$. Ako je p prost broj takav da $p \nmid (k^2 - v\lambda_2)$ i $p \mid k$, tada linearan kod nad $\mathbb{F}_p$ razapet retcima od R ima dimenziju $m - 1$.*

Dokaz. Budući da matrica RR^T ima $m - 1$ vlastitih vrijednosti jednakih $k^2 - v\lambda_2$ i jednu vlastitu vrijednost koja je jednaka k^2, ima samo jednu vlastitu vrijednost jednaku 0 u $\mathbb{F}_p$. Slijedi da je $r_p(RR^T) = m - 1$ (jer je za simetričnu matricu rang jednak broju nenul vlastitih vrijednosti), pa je zato $r_p(R) \geq m - 1$. S druge strane, budući da je $\det(R) \equiv 0 \pmod{p}$, slijedi da je $r_p(R) \leq m - 1$, pa je time $r_p(R) = m - 1$. □

Teoremi 2.2 i 2.3 pokazuju da je kod nad $\mathbb{F}_p$ razapet kvocijentnom matricom $SGDD$-a s dualnim svojstvom prilično nezanimljiv za $p \nmid (k^2 - v\lambda_2)$, budući da u tom slučaju dobiveni kod ima dimenziju m ili $m-1$. Zato ćemo se fokusirati na kodove nad $\mathbb{F}_p$ takve da $p \mid (k^2 - v\lambda_2)$. Primijetimo da u slučaju semi-regularnog simetričnog $(v, k, \lambda_1, \lambda_2, m, n)$ djeljivog dizajna svaki prosti broj p dijeli $k^2 - v\lambda_2$.

Teorem 2.4. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom i neka je R kvocijentna matrica od $\mathcal{D}$. Ako je p prost broj takav da $p \mid (k^2 - v\lambda_2)$ i $p \mid n\lambda_2$, tada retci od R razapinju samoortogonalan kod duljine m nad $\mathbb{F}_p$.*

Dokaz. Tvrdnja slijedi iz činjenice da je $RR^T = (k^2 - v\lambda_2)I_m + n\lambda_2 J_m$. □

2.3 Samodualni kodovi iz proširenih kvocijentnih matrica

Napomena 2.7. Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ $SGDD$ s dualnim svojstvom i neka je R kvocijentna matrica od $\mathcal{D}$. Ako prost broj p ne dijeli $n\lambda_2$, tada za dobivanje samoortogonalnih kodova nad $\mathbb{F}_p$ možemo koristiti malo drugačiji kod od onog razapetog kvocijentnom matricom R.

Neka je p prost broj takav da $p \nmid n\lambda_2$. Kvocijentnu matricu R možemo proširiti na sljedeći način:

$$R^{ext} = \left[\begin{array}{ccc|c} & & & 1 \\ & R & & \vdots \\ & & & 1 \\ \hline n\lambda_2 & \cdots & n\lambda_2 & k \end{array}\right].$$

Ovako dobivenu matricu R^{ext} nazvat ćemo **proširena kvocijentna matrica**. Kod nad $\mathbb{F}_p$ razapet retcima od R^{ext} označit ćemo sa C^{ext}, te ćemo ga nazivati **prošireni kod**.

Za $x = (x_1, ..., x_{m+1})$ i $y = (y_1, ..., y_{m+1})$ uvodimo skalarni produkt ψ sa

$$\psi(x, y) = x_1y_1 + ... + x_my_m - n\lambda_2 x_{m+1}y_{m+1}.$$

Znamo da $p \nmid n\lambda_2$, pa je ψ nedegenerirana forma na $\mathbb{F}_p$ (njezina matrica je regularna).

Lema 2.1. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom, R kvocijentna matrica od $\mathcal{D}$, te R^{ext} proširena kvocijentna matrica. Ako je p prost broj takav da $p \mid (k^2 - v\lambda_2)$, tada je prošireni kod C^{ext} nad $\mathbb{F}_p$ samoortogonalan u odnosu na ψ.*

Dokaz. Neka su x i y retci od R^{ext}. Tada je $\psi(x, y) \in \{0, k^2 - v\lambda_2, -n\lambda_2(k^2 - v\lambda_2)\}$. □

Ako je b bilinearna forma i B njezina matrica, tada je determinanta od b dana sa $\det(b) = \det(B)$. Matrica bilinearne forme ψ je $(m+1) \times (m+1)$ matrica

$$\Psi = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & -n\lambda_2 \end{bmatrix}.$$

Budući da je $\det(R^{ext}\Psi(R^{ext})^T) = \det(\psi)[\det(R^{ext})]^2 = -n\lambda_2(k^2 - v\lambda_2)^{m+1}$ i $\det(\psi) = -n\lambda_2$, slijedi da je $(\det(R^{ext}))^2 = (k^2 - v\lambda_2)^{m+1}$, i zato je

$$|\det(R^{ext})| = (k^2 - v\lambda_2)^{\frac{1}{2}(m+1)}.$$

Teorem 2.5. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom, R kvocijentna matrica od $\mathcal{D}$ i neka je C kod nad $\mathbb{F}_p$ razapet retcima od R. Ako je p prost broj takav da $p \mid (k^2 - v\lambda_2)$, tada je* $\dim(C) \leq \frac{m+1}{2}$.

Dokaz. Ako $p \mid n\lambda_2$ tada je C samoortogonalan prema teoremu 2.4, pa je $\dim(C) \leq \frac{m}{2}$. Ako $p \nmid n\lambda_2$ tada je C^{ext} samoortogonalan u odnosu na ψ i $\dim(C^{ext}) \leq \frac{m+1}{2}$. Dokazat ćemo da ako $p \mid (k^2 - v\lambda_2)$ i $p \nmid n\lambda_2$, tada je $\dim(C) = \dim(C^{ext})$. Zadnji stupac od R^{ext} jednak je (mod p) k^{-1} pomnoženo sa sumom ostalih m stupaca. Zadnji red od R^{ext} jednak je (mod p) $n\lambda_2 k^{-1}$ pomnoženo sa sumom prvih m redaka. Slijedi da R i R^{ext} imaju isti rang nad $\mathbb{F}_p$. □

Dokaz sljedećeg teorema može se naći u [35, Appendix C].

Teorem 2.6. *Neka je A $m \times m$ matrica s cjelobrojnim elementima. Tada postoje cjelobrojne unimodularne matrice (tj. cjelobrojne matrice s determinantama jednakim ± 1) P i Q takve da vrijedi:*

1. *PAQ je dijagonalna matrica, $PAQ = diag(d_1, ..., d_m)$,*
2. *d_i dijeli d_{i+1}, za $i = 1, ..., m-1$.*

*Štoviše, elementi d_i su određeni do na predznak i nazivaju se **invarijantni faktori** od A ili **elementarni djelitelji** od A.*

Jedinstvena dijagonalna matrica $PAQ = \mathrm{diag}(d_1, ..., d_m)$ naziva se **cjelobrojna Smithova normalna forma**, ili samo Smithova forma, od A. O Smithovoj formi i njezinoj primjeni u teoriji kombinatoričkih dizajna može se više pročitati u [52].

Napomena 2.8. Za cjelobrojnu matricu A vrijedi da je njezin p-rang jednak broju invarijantnih faktora od A koji nisu djeljivi s p.

Teorem 2.7. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom, R kvocijentna matrica od $\mathcal{D}$ i C^{ext} odgovarajući prošireni kod nad $\mathbb{F}_p$. Ako je p prost broj takav da $p \nmid n\lambda_2$, $p \mid (k^2 - v\lambda_2)$, ali $p^2 \nmid (k^2 - v\lambda_2)$, tada je C^{ext} samodualan u odnosu na ψ.*

Dokaz. Moramo dokazati da je $\dim(C^{ext}) = \frac{1}{2}(m+1)$. Nejednakost $\dim(C^{ext}) \leq \frac{1}{2}(m+1)$ slijedi iz činjenice da je C^{ext} samoortogonalan. Da bi dokazali da je $\frac{1}{2}(m+1) \leq \dim(C^{ext})$, pokazat ćemo da R^{ext} ima $\mathbb{F}_p$-rang barem $\frac{1}{2}(m+1)$. Budući da je R^{ext} kvadratna matrica reda $m+1$ s cjelobrojnim elementima, postoje cjelobrojne unimodularne matrice P i Q, takve da je $PR^{ext}Q$ dijagonalna matrica $PR^{ext}Q = \text{diag}(d_1, ..., d_{m+1})$ i d_i dijeli d_{i+1}, za $i = 1, ..., m$. Iz $|\det(PR^{ext}Q)| = |\det(R^{ext})| = (k^2 - v\lambda_2)^{\frac{1}{2}(m+1)}$, $p \mid (k^2 - v\lambda_2)$ i $p^2 \nmid (k^2 - v\lambda_2)$, slijedi da najviše $\frac{1}{2}(m+1)$ elemenata d_i su višekratnici od p. Zato $PR^{ext}Q$ ima $\mathbb{F}_p$-rang najmanje $\frac{1}{2}(m+1)$. Množenje matrice zdesna ili slijeva s unimodularnom matricom ne mijenja njezin rang modulo p, pa R^{ext} također ima $\mathbb{F}_p$-rang barem $\frac{1}{2}(m+1)$. Slijedi da je $\dim(C^{ext}) = \frac{1}{2}(m+1)$. □

O povezanosti samodualnih kodova i kvadrata u $\mathbb{F}_p$ govori sljedeći Wittov teorem čiji se dokaz može naći u [52].

Teorem 2.8. *Za danu simetričnu nesingularnu matricu U reda n nad $\mathbb{F}_p$, p neparan prost broj, postoji p-naran kod duljine n koji je samodualan u odnosu na U ako i samo ako je $(-1)^{n/2}det(U)$ kvadrat u $\mathbb{F}_p$.*

Direktna posljedica teorema 2.7 i 2.8 je sljedeći teorem.

Teorem 2.9. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom, R kvocijentna matrica od $\mathcal{D}$, C^{ext} odgovarajući prošireni kod nad $\mathbb{F}_p$. Ako je p neparan prost broj takav da $p \nmid n\lambda_2$, $p \mid (k^2 - v\lambda_2)$, ali $p^2 \nmid (k^2 - v\lambda_2)$, tada je $-\lambda_2 n(-1)^{\frac{m+1}{2}}$ kvadrat u $\mathbb{F}_p$.*

Ako $p^2 \mid (k^2 - v\lambda_2)$ ponekad možemo koristiti lanac kodova za dobivanje samodualnog koda iz kvocijentne matrice.

Za danu $m \times n$ cjelobrojnu matricu A, sa $row_{\mathbb{F}}(A)$ označimo linearan kod nad poljem $\mathbb{F}$ razapet sa retcima od A. Sa $row_p(A)$ označimo p-naran linearan kod razapet sa retcima od A. Također za danu matricu A definiramo, za bilo koji prost broj p i nenegativan cijeli broj i,

$$\mathcal{M}_i(A) = \{x \in \mathbb{Z}^n : p^i x \in row_{\mathbb{Z}}(A)\}.$$

Imamo $\mathcal{M}_0(A) = row_{\mathbb{Z}}(A)$ i

$$\mathcal{M}_0(A) \subseteq \mathcal{M}_1(A) \subseteq \mathcal{M}_2(A) \subseteq ... .$$

Neka je

$$C_i(A) = \pi_p(\mathcal{M}_i(A))$$

gdje je π_p homomorfizam (projekcija) sa $\mathbb{Z}^n$ na $\mathbb{F}_p^n$ dan uzimanjem svih koordinata modulo p. Tada je svaki $C_i(A)$ p-naran linearan kod duljine n, $C_0(A) = row_p(A)$, i

$$C_0(A) \subseteq C_1(A) \subseteq C_2(A) \subseteq ... .$$

Teorem koji slijedi i njegov dokaz mogu se naći u [52].

Teorem 2.10. *Neka je D dijagonalna forma za A s dijagonalnim elementima $d_1, d_2, ..., d_n$, gdje je n broj stupaca od A. Dimenzija p-narnog koda $C_j(A)$ je broj dijagonalnih elemenata d_i koji nisu djeljivi sa p^{j+1}.*

Sljedeći teorem iz [52] pokazuje kako se lanac kodova može iskoristiti za dobivanje samodualnog koda.

Teorem 2.11. *Pretpostavimo da je A $n \times n$ cjelobrojna matrica takva da je $AUA^T = p^eV$ za neki cijeli broj e, gdje su U i V kvadratne matrice s determintama relativno prostim s p. Tada je $C_e(A) = \mathbb{F}_p^n$ i*

$$C_j(A)^U = C_{e-j-1}(A), \quad za\ j = 0, 1, ..., e-1.$$

Posebno, ako je $e = 2f + 1$, tada je $C_f(A)$ U-samodualan p-naran kod duljine n.

Ovaj rezultat se može iskoristiti za pridruživanje samodualnog koda kvocijentnoj matrici djeljivog dizajna.

Teorem 2.12. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom. Pretpostavimo da je $k^2 - v\lambda_2$ točno djeljiv s neparnom potencijom prostog broja p[1] i da je λ_2 točno djeljiv s parnom potencijom od p, to jest $k^2 - v\lambda_2 = p^e n_0$, $\lambda_2 = p^{2a}\lambda_0$, gdje je e neparan, $a \geq 0$ i $(n_0, p) = (\lambda_0, p) = 1$. Ako $p \nmid n$ tada postoji samodualan p-naran kod duljine $m + 1$ u odnosu na skalarni produkt koji odgovara matrici $U = diag(1, ..., 1, -n\lambda_0)$.*

Dokaz. Neka je R_1 kvocijentna matrica od $\mathcal{D}$. Definirajmo matricu R_1^{ext} sa

$$R_1^{ext} = \left[\begin{array}{ccc|c} & & & p^a \\ & R_1 & & \vdots \\ & & & p^a \\ \hline p^a n\lambda_0 & \cdots & p^a n\lambda_0 & k \end{array}\right].$$

Slijedi da je $R_1^{ext}U(R_1^{ext})^T = (k^2 - v\lambda_2)U = p^e n_0 U = p^e V$, za $V = n_0 U$. Determinante od U i V su relativno proste sa p, pa možemo primijeniti teorem 2.11 da dobijemo U-samodualan kod. □

Kao posljedicu teorema 2.8 i 2.12 dobivamo sljedeći teorem.

Teorem 2.13. *Neka je $\mathcal{D}(v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom. Pretpostavimo da je p neparan prost broj takav da $k^2 - v\lambda_2 = p^e n_0$, $\lambda_2 = p^b\lambda_0$, gdje je e neparan, b paran i $(n_o, p) = (\lambda_0, p) = 1$. Ako $p \nmid n$, tada je $-n\lambda_0(-1)^{\frac{m+1}{2}}$ kvadrat u $\mathbb{F}_p$.*

[1] Kažemo da je broj x točno djeljiv s brojem y ako $y|x$ ali $y^2 \nmid x$.

Napomena 2.9. Uočimo da se teoremi 2.7, 2.9, 2.12 i 2.13 ne mogu primijeniti na semi-regularan simetričan $(v, k, \lambda_1, \lambda_2, m, n)$ djeljivi dizajn, budući da je u tom slučaju $k^2 - v\lambda_2$ djeljiv sa p^e, za svaki prost broj p i svaki nenegativan cijeli broj e.

2.4 Primjeri

U nastavku ćemo opisati primjere samodualnih kodova dobivenih na temelju prethodno opisanih rezultata uz pomoć proširenih kvocijentnih matrica SGDD-a s dualnim svojstvom. Djeljivi dizajni koji će se koristiti u primjerima bit će dobiveni iz određenih grafova, točnije iz grafova-djeljivih dizajna i digrafova-djeljivih dizajna, koje ćemo definirati u sljedećim potpoglavljima.

2.4.1 Samodualni kodovi iz grafova-djeljivih dizajna

Definicija 2.7. Dizajn susjedstva grafa Γ je dizajn čije su točke vrhovi od Γ, a blokovi su dani kao susjedstva vrhova od Γ.

Napomena 2.10. Matrica susjedstva grafa Γ je matrica incidencije pripadnog dizajna susjedstva.

U ovom potpoglavlju opisat ćemo grafove sa svojstvom da je njihov dizajn susjedstva djeljivi dizajn, pod nazivom grafovi-djeljivi dizajni ili DDG-ovi [2]. Uveli su ih Haemers, Kharaghani i Meulenberg u [26] kao generalizaciju (v, k, λ)-grafova.

Definicija 2.8. Za jako regularan graf s parametrima (v, k, λ, λ) kažemo da je (v, k, λ)-**graf**. Dizajn susjedstva (v, k, λ)-grafa je simetričan $2 - (v, k, \lambda)$ dizajn.

Definicija 2.9. Kažemo da je k-regularan graf s v vrhova **graf-djeljivi dizajn (DDG)** s parametrima $(v, k, \lambda_1, \lambda_2, m, n)$ ako se skup vrhova može particionirati u m klasa veličine n, tako da:

1. dva vrha iz iste klase imaju točno λ_1 zajedničkih susjeda,

2. dva vrha iz različitih klasa imaju točno λ_2 zajedničkih susjeda.

Napomena 2.11. Iz definicije DDG-a očito je da je dizajn susjedstva DDG-a uvijek simetrični djeljivi dizajn s dualnim svojstvom.

Obratno, vrijedi da je djeljivi dizajn sa simetričnom matricom incidencije s nulama na dijagonali, dizajn susjedstva DDG-a.

Definicija 2.10. DDG sa $m = 1$, $n = 1$ ili $\lambda_1 = \lambda_2$ je (v, k, λ)-graf i takav DDG nazivamo **nepravi**, a inače **pravi**.

[2]Kratica DDG dolazi od engleskog naziva *divisible design graph*.

Tablica sa mogućim skupovima parametara za prave DDG-ove sa svojstvima $v \leq 27$, $0 < \lambda_2 < 2k - v$, $\lambda_1 < k$, dana je u [26]. Za one skupove parametara za koje je dokazano postojanje DDG-a tamo je dana i konstrukcija. U deset slučajeva postojanje DDG-a s navedenim parametrima ostalo je otvoreni problem. Zatim su D. Crnković i W. Haemers u [12] riješili devet od deset preostalih slučajeva. Proučili smo djeljive dizajne dobivene kao dizajne susjedstva navedenih DDG-ova iz tablice iz [26], te pomoću njihovih kvocijentnih matrica našli primjere samodualnih kodova primjenom teorema 2.7. Dobiveni samodualni kodovi prikazani su u tablici 2.2 i opisani u nastavku.

v	k	λ_1	λ_2	m	n	$k^2 - v\lambda_2$	$n\lambda_2$	dobiveni samodualni kodovi pomoću T.2.7
8	4	0	2	4	2	0	4	-
10	5	4	2	5	2	5	4	samodualan kod duljine 6 nad $\mathbb{F}_5$ (Pr. 2.6)
12	5	0	2	6	2	1	4	-
12	5	1	2	4	3	1	6	-
12	6	2	3	3	4	0	12	-
12	7	3	4	4	3	1	12	-
15	4	0	1	5	3	1	3	-
18	9	6	4	6	3	9	12	-
18	9	8	4	9	2	9	8	-
20	7	3	2	4	5	9	10	-
20	7	6	2	10	2	9	4	-
20	9	0	4	10	2	1	8	-
20	13	9	8	4	5	9	40	-
20	13	12	8	10	2	9	16	-
24	6	2	1	3	8	12	8	samodualan kod duljine 4 nad $\mathbb{F}_3$ (Pr. 2.4)
24	7	0	2	8	3	1	6	-
24	8	4	2	4	6	16	12	-
24	10	2	4	12	2	4	8	-
24	10	3	4	8	3	4	12	-
24	10	6	3	3	8	28	24	samodualan kod duljine 4 nad $\mathbb{F}_7$ (Pr. 2.5)
24	14	6	8	12	2	4	16	-
24	14	7	8	8	3	4	24	-
24	16	12	10	4	6	16	60	-
26	13	12	6	13	2	13	12	samodualan kod duljine 14 nad $\mathbb{F}_{13}$ (Pr. 2.7)
27	16	12	9	9	3	13	27	otvoreni problem (Pr. 2.8)
27	18	9	12	9	3	0	36	-

Tablica 2.2: Mogući parametri za prave DDG-ove sa $v \leq 27$, $0 < \lambda_2 < 2k - v$, $\lambda_1 < k$ i dobiveni kodovi

U [26] su neki primjeri DDG-ova dobiveni iz regularnih grafičkih Hadamardovih matrica. Prije opisa te konstrukcije definirat ćemo potrebne pojmove vezane uz Hadamardove matrice.

Definicija 2.11. Kažemo da je $m \times m$ matrica H **Hadamardova matrica** reda m ako su joj svi elementi jednaki 1 ili -1 i ako je $HH^T = mI_m$.

Napomena 2.12. Primijetimo da množenje elemenata u jednom retku (ili stupcu) Hadamardove matrice sa -1 opet daje Hadamardovu matricu.

Primjer 2.3. Sljedeće matrice su primjeri Hadamardovih matrica reda 1, 2 i 4:

$$[1]\,, \quad [-1]\,, \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Sljedeći rezultat daje nužan uvjet za postojanje Hadamarove matrice reda n, a dokaz se može naći u [48].

Teorem 2.14. *Ako postoji Hadamardova matrica reda $n > 2$, tada je:*

$$n \equiv 0 (mod\ 4).$$

Definicija 2.12. Hadamardova matrica H se naziva:

a) **grafička** ako je H simetrična s konstantnom dijagonalom,

b) **regularna** ako su joj sve sume redaka i stupaca jednake (recimo jednake broju l).

Slijedi opis konstrukcije DDG-ova iz regularnih grafičkih Hadamardovih matrica dan u [26].

Teorem 2.15. ([*26, Construction* 4.9]) *Neka je H regularna grafička Hadamardova matrica reda $l^2 \geq 4$ s dijagonalnim elementima -1 i retčanom sumom l. Tada je graf s matricom susjedstva*

$$A = \begin{bmatrix} M & N & 0 \\ N & 0 & M \\ 0 & M & N \end{bmatrix}, \quad \textit{gdje je}$$

$$M = \frac{1}{2}\begin{bmatrix} J+H & J+H \\ J+H & J+H \end{bmatrix} \quad i \quad N = \frac{1}{2}\begin{bmatrix} J+H & J-H \\ J-H & J+H \end{bmatrix}$$

DDG s parametrima $(6l^2, 2l^2 + l, l^2 + l, (l^2 + l)/2, 3, 2l^2)$.

Primjer 2.4. Uzmimo regularnu grafičku Hadamardovu matricu H_1, te primijenimo opisanu konstrukciju za dobivanje DDG-a Γ_1 s parametrima $(24, 6, 2, 1, 3, 8)$, gdje je

$$H_1 = \begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix}.$$

Matrica susjedstva grafa Γ_1 dana je kao:

$$A_1 = \left[\begin{array}{cccc:cccc|cccc:cccc|cccc:cccc}
0&0&0&1&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&1&1&0&1&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&1&0&1&1&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0\\
\hdashline
0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&1&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&0&1&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&1&0&0&1&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1\\
\hdashline
1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0\\
1&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&1&1&1\\
\hdashline
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&1&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&1&0&1&1&0&1&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0
\end{array}\right].$$

Pripadni dizajn susjedstva je djeljivi dizajn $\mathcal{D}_1$ s matricom incidencije A_1.

Kvocijentna matrica koja se dobije iz matrice A_1 jednaka je:

$$R_1 = \begin{bmatrix} 2 & 4 & 0 \\ 4 & 0 & 2 \\ 0 & 2 & 4 \end{bmatrix} \equiv \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{bmatrix} \pmod 3.$$

Iz dizajna $\mathcal{D}_1$ primjenom teorema 2.7 dobivamo samodualan kod C_1^{ext} duljine 4 nad $\mathbb{F}_3$ u odnosu na ψ. Kod je razapet retcima matrice:

$$R_1^{ext} = \left[\begin{array}{ccc|c} 2 & 1 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 2 & 1 & 1 \\ \hline 2 & 2 & 2 & 0 \end{array}\right] \pmod 3.$$

Primjer 2.5. Regularna grafička Hadamardova matrica H_2 pomoću iste konstrukcije daje DDG Γ_2 s parametrima $(24, 10, 6, 3, 3, 8)$.

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

Matrica susjedstva grafa Γ_2 dana je kao:

$$A_2 = \left[\begin{array}{cccc:cccc:cccc:cccc:cccc:cccc}
0&1&1&1&0&1&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&1&1&0&1&1&1&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&0&1&1&1&0&1&1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0\\
1&1&1&0&1&1&1&0&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0\\
\hdashline
0&1&1&1&0&1&1&1&1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0\\
1&0&1&1&1&0&1&1&0&1&0&0&1&0&1&1&0&0&0&0&0&0&0&0\\
1&1&0&1&1&1&0&1&0&0&1&0&1&1&0&1&0&0&0&0&0&0&0&0\\
1&1&1&0&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0\\
\hdashline
0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1\\
1&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&1&1\\
1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1\\
1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0\\
\hdashline
1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1\\
0&1&0&0&1&0&1&1&0&0&0&0&0&0&0&0&1&0&1&1&1&0&1&1\\
0&0&1&0&1&1&0&1&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1\\
0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0\\
\hdashline
0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&1&1&1&1&0&0&0\\
0&0&0&0&0&0&0&0&1&0&1&1&1&0&1&1&1&0&1&1&0&1&0&0\\
0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&1&1&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&1&1&1&0&0&0&0&1\\
\hdashline
0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&1&0&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&1&0&1&1&1&0&1&1&0&1&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&0&0&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&0&1&1&1&1&0
\end{array}\right].$$

Pripadni dizajn susjedstva je djeljivi dizajn $\mathcal{D}_2$ s matricom incidencije A_2.
Kvocijentna matrica koja se dobije iz matrice A_2 jednaka je:

$$R_2 = \begin{bmatrix} 6 & 4 & 0 \\ 4 & 0 & 6 \\ 0 & 6 & 4 \end{bmatrix}.$$

Iz dizajna $\mathcal{D}_2$ primjenom teorema 2.7 dobivamo samodualan kod C_2^{ext} duljine 4 nad

$\mathbb{F}_7$ u odnosu na ψ. Kod je razapet retcima matrice:

$$R_2^{ext} = \left[\begin{array}{ccc|c} 6 & 4 & 0 & 1 \\ 4 & 0 & 6 & 1 \\ 0 & 6 & 4 & 1 \\ \hline 3 & 3 & 3 & 3 \end{array}\right] \pmod 7.$$

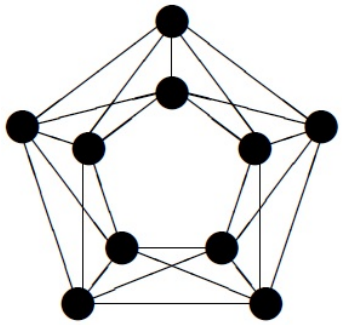
Sljedeća konstrukcija, također iz [26], daje primjere DDG-ova dobivenih pomoću jako regularnih grafova. Trebat će nam i sljedeća definicija.

Definicija 2.13. Neka je Γ_1 graf s matricom susjedstva A, te Γ_2 graf s matricom susjedstva B. **Jaki produkt** grafova Γ_1 i Γ_2 je graf čija je matrica susjedstva dana kao:

$$(A + I) \otimes (B + I) - I.$$

Teorem 2.16. ([*26, Construction* 4.10]) *Neka je Γ' jako regularan graf s parametrima $(m, k', \lambda, \lambda + 1)$. Tada je jaki produkt od K_2 sa Γ' DDG s parametrima jednakim: $n = 2$, $\lambda_1 = k - 1 = 2k'$ i $\lambda_2 = 2\lambda + 2$.*

Primjer 2.6. Neka je $\Gamma' = C_5$ pentagon, tj. jako regularni graf s parametrima $(5, 2, 0, 1)$. Prethodnom konstrukcijom iz njega dobivamo DDG Γ s parametrima $(10, 5, 4, 2, 5, 2)$ kao jaki produkt K_2 i C_5. Γ je prikazan na slici 2.1. Njemu odgovarajući djeljivi dizajn zadovoljava uvjete teorema 2.7 te daje samodualan kod duljine šest nad $\mathbb{F}_5$ u odnosu na ψ.



Slika 2.1: DDG(10,5,4,2,5,2)

Primjer 2.7. Neka je $\Gamma' = P(13)$ Paleyev graf reda 13. To je jako regularan graf s parametrima $(13, 6, 2, 3)$. Tada pomoću njega dobivamo DDG Γ s parametrima $(26, 13, 12, 6, 13, 2)$ kao jaki produkt K_2 i $P(13)$. Njemu odgovarajući djeljivi dizajn zadovoljava uvjete teorema 2.7 te daje samodualan kod duljine 14 nad $\mathbb{F}_{13}$ u odnosu na ψ.

Primjer 2.8. Postojanje DDG-a s parametrima $(27, 16, 12, 9, 9, 3)$ otvoreni je problem, odnosno takav DDG nije pronađen niti je dokazano da ne postoji DDG s tim parametrima.

Ako takav DDG postoji, pripadni dizajn susjedstva je djeljivi dizajn koji zadovoljava pretpostavke teorema 2.7. U tom slučaju postojao bi samodualan kod duljine 10 nad $\mathbb{F}_{13}$ u odnosu na ψ.

2.4.2 Samodualni kodovi iz digrafova-djeljivih dizajna

U [13] su D. Crnković i H. Kharaghani definirali i proučavali usmjerenu verziju DDG-ova pod nazivom digrafovi-djeljivi dizajni ili skraćeno DDD[3]. Tamo su također dani nužni uvjeti za postojanje DDD-a s određenim parametrima te neke konstrukcije.
U nastavku ćemo definirati DDD-ove te vidjeti kako pomoću njih možemo dobiti SGDD-e. Započinjemo s definicijom usmjerenog grafa.

Definicija 2.14. Usmjereni graf ili **digraf** je par $\Gamma = (V, E)$, gdje je V konačan neprazan skup vrhova i E skup uređenih parova (x, y) koje nazivamo **lukovi** takvih da $x, y \in V$ i $x \neq y$.
Ako je (x, y) luk, tada kažemo da x **dominira** nad y, odnosno da je y **dominiran** sa x.

Definicija 2.15. Kažemo da je digraf $\Gamma = (V, E)$:

a) **asimetričan** ako iz $(x, y) \in E$ slijedi $(y, x) \notin E$,

b) **regularan stupnja** k ili k**-regularan** ako svaki vrh od Γ dominira nad točno k vrhova i dominiran je s točno k vrhova.

Sada možemo definirati digraf-djeljivi dizajn.

Definicija 2.16. Za k-regularan asimetričan digraf s v vrhova kažemo da je **digraf-djeljivi dizajn (DDD)** s parametrima $(v, k, \lambda_1, \lambda_2, m, n)$, ako se skup vrhova može particionirati u m klasa veličine n, tako da je:

1. za svaka dva različita vrha x i y iz iste klase, broj vrhova koji dominiraju nad x i y i broj vrhova koji su dominirani s x i y jednak λ_1,

2. za svaka dva različita vrha x i y iz različitih klasa, broj vrhova koji dominiraju nad x i y i broj vrhova koji su dominirani s x i y jednak λ_2.

Digraf se može karakterizirati svojom matricom susjedstva.

Definicija 2.17. Neka je $\Gamma = (V, E)$ digraf sa skupom vrhova $V = \{x_1, ..., x_v\}$. **Matrica susjedstva** za Γ je $v \times v$ matrica $A = [a_{ij}]$ takva da je

$$a_{ij} = \begin{cases} 1, & \text{ako je } (x_i, x_j) \in E \\ 0, & \text{inače} \end{cases}.$$

[3]Kratica DDD dolazi iz engleskog naziva *divisible design digraphs*.

Definicija 2.18. Kažemo da je $(0,1)$-matrica X **kososimetrična** ako je $X + X^T$ $(0,1)$-matrica.

Napomena 2.13. Za matricu susjedstva DDD-a vrijedi da je ona uvijek kososimetrična matrica.

Lako se pokazuje iz definicije DDD-a da vrijedi sljedeći teorem iz [13].

Teorem 2.17. *Ako je Γ DDD s parametrima $(v, k, \lambda_1, \lambda_2, m, n)$, tada je njegov dizajn susjedstva simetričan djeljivi dizajn s dualnim svojstvom s parametrima $(v, k, \lambda_1, \lambda_2, m, n)$.*

Napomena 2.14. Prethodni teorem osigurava da će matrica susjedstva DDD-a biti matrica incidencije za SGDD s dualnim svojstvom s istim parametrima.
Obratno, ako je $\mathcal{D}$ SGDD s dualnim svojstvom s parametrima $(v, k, \lambda_1, \lambda_2, m, n)$ koji ima kososimetričnu matricu incidencije, tada je $\mathcal{D}$ dizajn susjedstva za DDD s istim parametrima $(v, k, \lambda_1, \lambda_2, m, n)$.

U nastavku ćemo opisati dvije konstrukcije DDD-a uz pomoć Hadamardovih dizajna s kososimetričnim matricama incidencije. Konstrukcije su iz [13]. Iskoristit ćemo ih za dobivanje samodualnih kodova pomoću odgovarajućih dizajna susjedstva konstruiranih DDD-a.

Definicija 2.19. Simetričan dizajn s parametrima $(4n-1, 2n-1, n-1)$ ili $(4n-1, 2n, n)$ naziva se **Hadamardov dizajn** reda n.

Primjer 2.9. Simetričan $2-(7,3,1)$ dizajn je ujedno i projektivna ravnina reda 2 i Hadamardov dizajn reda 2.

Napomena 2.15. Neka je $\mathcal{D}$ $(4n-1, 2n-1, n-1)$ Hadamardov dizajn. Tada je njegov komplementarni dizajn $(4n-1, 2n, n)$ Hadamardov dizajn. To slijedi iz teorema 1.8.

Sljedeća lema dokazana je u [13] i opisuje prvu od spomenutih konstrukcija DDD-a pomoću Hadamardovih dizajna.

Lema 2.2. ([*13, Lemma* 4.4]) *Pretpostavimo da postoji Hadamardov $(4l+3, 2l+1, l)$ dizajn*[4] *s kososimetričnom matricom incidencije. Tada postoji DDD s parametrima*

$$(28l+21, 8l+7, 4l+3, 2l+2, 7, 4l+3).$$

[4]Hadamardov $(4l+3, 2l+1, l)$ dizajn je zapravo Hadamardov $(4n-1, 2n-1, n-1)$ dizajn za koji je $n = l+1$.

Dokaz. Neka je D sljedeća matrica incidencije Hadamardovog $(7,3,1)$ dizajna:

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

te neka je D_1 kososimetrična matrica incidencije Hadamardovog $(4l+3, 2l+1, l)$ dizajna. Stavimo da je $\overline{D}_1$ matrica koja se dobije iz D_1 zamjenom 0 i 1, tj. $\overline{D}_1 = J_{4l+3} - D_1$. Tada je matrica A definirana kao:

$$A = D \otimes \overline{D}_1 + I_7 \otimes D_1,$$

matrica susjedstva za DDD s parametrima $(28l+21, 8l+7, 4l+3, 2l+2, 7, 4l+3)$. □

Napomena 2.16. Primijetimo da matrica D_1 iz prethodne leme može biti i matrica incidencije trivijalnog dizajna.

Primjer 2.10. Neka je D_1 matrica incidencije simetričnog $(3,1,0)$ dizajna dana kao:

$$D_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Tada je D_1 kososimetrična matrica incidencije Hadamardovog $(4l+3, 2l+1, l)$ dizajna za $l = 0$. Odgovarajuća matrica $\overline{D}_1$ jednaka je:

$$\overline{D}_1 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Primjenom konstrukcije iz leme 2.2 dobivamo matricu susjedstva A za $DDD(21, 7, 3, 2, 7, 3)$ kao:

$$A = \begin{bmatrix} D_1 & \overline{D}_1 & \overline{D}_1 & 0 & \overline{D}_1 & 0 & 0 \\ 0 & D_1 & \overline{D}_1 & \overline{D}_1 & 0 & \overline{D}_1 & 0 \\ 0 & 0 & D_1 & \overline{D}_1 & \overline{D}_1 & 0 & \overline{D}_1 \\ \overline{D}_1 & 0 & 0 & D_1 & \overline{D}_1 & \overline{D}_1 & 0 \\ 0 & \overline{D}_1 & 0 & 0 & D_1 & \overline{D}_1 & \overline{D}_1 \\ \overline{D}_1 & 0 & \overline{D}_1 & 0 & 0 & D_1 & \overline{D}_1 \\ \overline{D}_1 & \overline{D}_1 & 0 & \overline{D}_1 & 0 & 0 & D_1 \end{bmatrix}.$$

Pripadni dizajn susjedstva ovog DDD-a je djeljivi dizajn $\mathcal{D}$ s matricom incidencije A. Iz matrice A dobivamo sljedeću kvocijentnu matricu:

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

Dizajn $\mathcal{D}$ primjenom teorema 2.7 daje samodualan $[8, 4]$ kod C^{ext} nad $\mathbb{F}_7$ u odnosu na ψ. Kod razapinju retci matrice:

$$R^{ext} = \left[\begin{array}{ccccccc|c} 1 & 2 & 2 & 0 & 2 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 0 & 2 & 1 \\ 2 & 0 & 0 & 1 & 2 & 2 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 & 2 & 2 & 1 \\ 2 & 0 & 2 & 0 & 0 & 1 & 2 & 1 \\ 2 & 2 & 0 & 2 & 0 & 0 & 1 & 1 \\ \hline 6 & 6 & 6 & 6 & 6 & 6 & 6 & 0 \end{array}\right] \pmod 7.$$

Slijedi i druga konstrukcija DDD-a pomoću Hadamardovih dizajna, također dokazana u [13] kao i prethodna.

Lema 2.3. ([*13, Lemma* 4.5]) *Neka je D kososimetrična matrica incidencije Hadamardovog dizajna s parametrima $(4l+3, 2l+1, l)$ i neka je D_1 kososimetrična matrica incidencije simetričnog (v_1, k_1, λ_1) dizajna. Tada je matrica*

$$A = D \otimes J_{v_1} + I_v \otimes D_1,$$

matrica susjedstva za DDD s parametrima $((4l+3)v_1, (2l+1)v_1 + k_1, (2l+1)v_1 + \lambda_1, v_1 l + k_1, 4l+3, v_1)$.

Primjer 2.11. Neka su i D i D_1 kososimetrične matrice incidencije simetričnog $(3, 1, 0)$ dizajna, tj. točnije neka je:

$$D = D_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Primjenom konstrukcije iz leme 2.3 dobivamo matricu susjedstva A za DDD s parametrima

$(9, 4, 3, 1, 3, 3)$ kao:

$$A = \begin{bmatrix} D_1 & I_3 & 0 \\ 0 & D_1 & I_3 \\ I_3 & 0 & D_1 \end{bmatrix}.$$

Matrica A je ujedno i matrica incidencije za pripadni dizajn susjedstva $\mathcal{D}$ ovog DDD-a.
Iz matrice A dobivamo sljedeću kvocijentnu matricu:

$$R = \begin{bmatrix} 1 & 3 & 0 \\ 0 & 1 & 3 \\ 3 & 0 & 1 \end{bmatrix}.$$

Pomoću dizajna $\mathcal{D}$ primjenom teorema 2.7 dobivamo samodualan $[4, 2]$ kod C^{ext} nad $\mathbb{F}_7$ u odnosu na ψ. Kod je razapet retcima matrice:

$$R^{ext} = \left[\begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 0 & 1 & 3 & 1 \\ 3 & 0 & 1 & 1 \\ \hline 3 & 3 & 3 & 4 \end{array}\right].$$

Primjer 2.12. Neka je D kososimetrična matrica incidencije Hadamardovog $(3, 1, 0)$ dizajna, te D_1 kososimetrična matrica incidencije simetričnog $(4, 1, 0)$ dizajna, odnosno neka je:

$$D = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad D_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Lema 2.3 daje matricu susjedstva A za DDD s parametrima $(12, 5, 4, 1, 3, 4)$ kao:

$$A = \begin{bmatrix} D_1 & I_4 & 0 \\ 0 & D_1 & I_4 \\ I_4 & 0 & D_1 \end{bmatrix}.$$

A je matrica incidencije pripadnog dizajna susjedstva $\mathcal{D}$ ovog DDD-a.
Iz matrice A dobivamo kvocijentnu, te proširenu kvocijentnu matricu:

$$R = \begin{bmatrix} 1 & 4 & 0 \\ 0 & 1 & 4 \\ 4 & 0 & 1 \end{bmatrix} \quad \text{i} \quad R^{ext} = \left[\begin{array}{ccc|c} 1 & 4 & 0 & 1 \\ 0 & 1 & 4 & 1 \\ 4 & 0 & 1 & 1 \\ \hline 4 & 4 & 4 & 5 \end{array}\right].$$

Pomoću dizajna $\mathcal{D}$ primjenom teorema 2.7 dobivamo samodualan $[4, 2]$ kod C^{ext} nad

$\mathbb{F}_{13}$ u odnosu na ψ, razapet retcima matrice R^{ext}.

Definicija 2.20. DDD sa $m = 1$, $n = 1$ ili $\lambda_1 = \lambda_2$ nazivamo **nepravi**, a inače **pravi**.

Crnković i Kharaghani su u [13] dali tablicu s mogućim skupovima parametara za prave DDD-ove sa svojstvima $v \leq 27$, $0 < \lambda_2 < k$, $\lambda_1 < k$. Postojanje DDD-a s navedenim parametrima ostalo je otvoreni problem u dvadeset slučajeva od ukupno 94 moguća. Za 24 skupa parametara dokazano je postojanje DDD-a i navedena je konstrukcija koja se koristi. U sljedećoj tablici proučili smo ta 24 skupa parametara koji daju DDD-ove, te vidjeli za koje od njih pripadni djeljivi dizajni daju samodualne kodove primjenom teorema 2.7.

v	k	λ_1	λ_2	m	n	$k^2 - v\lambda_2$	$n\lambda_2$	dobiveni samodualni kodovi pomoću T.2.7
8	3	0	1	4	2	1	2	-
9	4	3	1	3	3	7	3	samodualan $[4, 2]$ kod nad $\mathbb{F}_7$ (Pr.2.11)
9	3	0	1	3	3	0	3	-
12	5	1	2	4	3	1	6	-
12	5	4	1	3	4	13	4	samodualan $[4, 2]$ kod nad $\mathbb{F}_{13}$ (Pr.2.12)
12	4	2	1	6	2	4	2	-
15	4	0	1	5	3	1	3	-
15	6	5	1	3	5	21	5	samodualan $[4, 2]$ kod nad $\mathbb{F}_3$ i $\mathbb{F}_7$
16	7	0	3	8	2	1	6	-
16	7	2	3	4	4	1	12	-
16	4	0	1	4	4	0	4	-
18	6	0	2	6	3	0	6	-
18	7	6	1	3	6	31	6	samodualan $[4, 2]$ kod nad $\mathbb{F}_{31}$
20	7	3	2	4	5	9	10	-
21	10	9	4	7	3	16	12	-
21	7	3	2	7	3	7	6	samodualan $[8, 4]$ kod nad $\mathbb{F}_7$ (Pr.2.10)
21	10	8	3	3	7	37	21	samodualan $[4, 2]$ kod nad $\mathbb{F}_{37}$
21	8	7	1	3	7	43	7	samodualan $[4, 2]$ kod nad $\mathbb{F}_{43}$
24	11	0	5	12	2	1	10	-
24	10	2	4	12	2	4	8	-
24	5	0	1	6	4	1	4	-
24	9	8	1	3	8	57	8	samodualan $[4, 2]$ kod nad $\mathbb{F}_3$ i $\mathbb{F}_{19}$
25	5	0	1	5	5	0	5	-
27	10	9	1	3	9	73	9	samodualan $[4, 2]$ kod nad $\mathbb{F}_{73}$

Tablica 2.3: Mogući parametri za prave DDD-ove sa $v \leq 27$, $0 < \lambda_2 < k$, $\lambda_1 < k$ i dobiveni kodovi

Napomena 2.17. Svi samodualni kodovi navedeni u tablici 2.3 dobiveni su konstrukcijom iz leme 2.3, osim koda iz primjera 2.10, koji je dobiven pomoću leme 2.2.

Poglavlje 3

Samodualni kodovi iz blokovnih dizajna

U ovom poglavlju uvest ćemo pojam orbitnih matrica, te zatim opisati konstrukcije samoortogonalnih i samodualnih kodova nad $\mathbb{F}_p$, u odnosu na određene skalarne produkte, uz pomoć orbitnih matrica blokovnih dizajna induciranih djelovanjem grupe automorfizama dizajna. Konstruirat ćemo i neke primjere samodualnih kodova dobivenih pomoću orbitnih matrica blokovnih dizajna.

Nakon konstrukcija koje se odnose općenito na blokovne dizajne, prikazat ćemo i dodatne konstrukcije posebno za simetrične blokovne dizajne i njihove orbitne matrice. Također, na sličan način kao za simetrične dizajne, konstruirat ćemo samodualne kodove i pomoću kvocijentnih matrica simetričnih grupovno djeljivih dizajna (SGDD-a) s dualnim svojstvom. Kao poseban slučaj konstrukcija iz simetričnih dizajna, promotrit ćemo i konstrukcije uz pomoć Hadamardovih dizajna. Na kraju ćemo vidjeti kako nam Kroneckerov produkt može pomoći u dobivanju novih samodualnih kodova.

3.1 Orbitne matrice blokovnih dizajna

U nastavku ćemo definirati orbitne matrice pridružene blokovnim dizajnima. Najčešća primjena orbitnih matrica je za konstrukciju blokovnih dizajna koji dopuštaju djelovanje pretpostavljene grupe automorfizama (vidi npr. [16]). Mi ćemo ih koristiti za konstrukciju samodualnih kodova.

Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ $2-(v,k,\lambda)$ dizajn i neka je $G \leq Aut(\mathcal{D})$. Označimo sa $P_1, ..., P_n$ G-orbite točaka, sa $B_1, ..., B_m$ G-orbite blokova te neka je:

$$|P_i| = \omega_i, \quad |B_j| = \Omega_j, \quad \text{gdje je } 1 \leq i \leq n,\ 1 \leq j \leq m.$$

Napomena 3.1. Za $b = |\mathcal{B}|$ očito je da vrijedi:

$$\sum_{i=1}^{n} \omega_i = v, \quad \sum_{j=1}^{m} \Omega_j = b.$$

Dokaz sljedeće propozicije može se naći i u [4].

Propozicija 3.1. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ $2-(v,k,\lambda)$ dizajn i $G \leq Aut(\mathcal{D})$. G-orbite točaka i blokova daju taktičku dekompoziciju dizajna $\mathcal{D}$.*

Dokaz. Neka su $P, Q \in P_i$ dvije različite točke iz orbite točaka P_i, te $x_i, ..., x_k \in B_j$ blokovi dizajna incidentni s točkom P. Znamo da postoji $g \in G$ takav da je $gP = Q$. Slijedi da su blokovi $gx_1, ..., gx_k$ blokovi iz orbite B_j incidentni s točkom Q. Slijedi da je svaka točka iz P_i incidentna s konstantnim brojem blokova iz B_j. To znači da je dekompozicija dizajna $\mathcal{D}$ taktička po točkama. Analogno se pokaže da je taktička po blokovima. □

Uvedimo za blok $x \in \mathcal{B}$ i točku $Q \in \mathcal{P}$ sljedeće oznake:

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

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

Neka je $Q \in P_i$, $x \in B_j$. Označimo sada:

$$\gamma_{ij} = |\langle x \rangle \cap P_i|,$$

$$\Gamma_{ij} = |\langle Q \rangle \cap B_j|.$$

Budući da je dekompozicija dizajna taktička, brojevi γ_{ij} ne ovise o izboru bloka x, kao što ni brojevi Γ_{ij} ne ovise o izboru točke Q kao predstavnika točkovne orbite P_i.

Napomena 3.2. Broj γ_{ij} jednak je broju točaka iz orbite točaka P_i incidentnih s blokom iz orbite blokova B_j. Slično, Γ_{ij} je jednak broju blokova iz orbite blokova B_j incidentnih s točkom iz orbite točaka P_i. Zato vrijedi:

a) $\sum_{i=1}^{n} \gamma_{ij} = k, \ \forall j \in \{1, ..., m\}$;

b) $\sum_{j=1}^{m} \Gamma_{ij} = r, \ \forall i \in \{1, ..., n\}$.

Lema 3.1. ([16]) *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ blokovni dizajn, $G \leq Aut(\mathcal{D})$, te ω_i, Ω_j, γ_{ij}, Γ_{ij} definirani kao ranije. Vrijede sljedeće jednakosti:*

a) $\Omega_j \gamma_{ij} = \omega_i \Gamma_{ij}$;

b) $\sum_{j=1}^{m} \Gamma_{ij}\gamma_{sj} = \lambda\omega_s + \delta_{is}\cdot(r-\lambda)$, *gdje je* δ_{is} *Kroneckerov delta simbol,* $i, s \in \{1, ..., n\}$.

Dokaz. a) Ovaj dio slijedi prebrojavanjem na dva načina elemenata skupa:

$$\{(Q, x) \in \mathcal{I} \mid Q \in P_i, x \in B_j\}.$$

b) Neka je Q_i predstavnik točkovne orbite P_i i x_j predstavnik blokovne orbite B_j, za $j = 1, ..., m$. Tada:

$$\begin{aligned}
\sum_{j=1}^{m} \Gamma_{ij}\gamma_{sj} &= \sum_{j=1}^{m} |\langle Q_i\rangle \cap B_j||\langle x_j\rangle \cap P_s| = \sum_{j=1}^{m} |\langle Q_i\rangle \cap B_j| \sum_{R\in P_s} |\langle x_j\rangle \cap R| \\
&= \sum_{j=1}^{m} \sum_{x\in\langle Q_i\rangle\cap B_j} \sum_{R\in P_s} |x \cap \langle R\rangle| = \sum_{j=1}^{m} \sum_{R\in P_s} \sum_{x\in\langle Q_i\rangle\cap B_j} |x \cap \langle R\rangle| \\
&= \sum_{j=1}^{m} \sum_{R\in P_s} |\langle Q_i\rangle \cap B_j \cap \langle R\rangle| = \sum_{R\in P_s} \sum_{j=1}^{m} |\langle Q_i\rangle \cap B_j \cap \langle R\rangle| \\
&= \sum_{R\in P_s} |\langle Q_i\rangle \cap \langle R\rangle|.
\end{aligned} \tag{3.1}$$

Za $i \neq s$ dobivamo:

$$\sum_{R\in P_s} |\langle Q_i\rangle \cap \langle R\rangle| = \sum_{R\in P_s} \lambda = \lambda\omega_s.$$

Za $i = s$ imamo:

$$\sum_{R\in P_s} |\langle Q_i\rangle \cap \langle R\rangle| = (\omega_s - 1)\lambda + r = \lambda\omega_s + (r - \lambda).$$

□

Pomoću ove leme dobivamo sljedeću propoziciju.

Propozicija 3.2. ([16]) *Neka je* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *blokovni dizajn,* $G \leq Aut(\mathcal{D})$, *te* ω_i, Ω_j, γ_{ij}, Γ_{ij} *definirani kao ranije. Vrijede sljedeće jednakosti:*

1. $\sum_{i=1}^{n} \gamma_{ij} = k$;

2. $\sum_{j=1}^{m} \frac{\Omega_j}{\omega_i}\gamma_{ij}\gamma_{sj} = \lambda\omega_s + \delta_{is}\cdot(r-\lambda)$.

Dokaz. 1. Neka je $x \in B_j$. Tada je $\sum_{i=1}^{n} \gamma_{ij} = |\langle x \rangle| = k$.

2. Rezultat iz leme 3.1 pod a) povlači da je $\Gamma_{ij} = \frac{\Omega_j}{\omega_i}\gamma_{ij}$. Sada dio pod b) iz leme 3.1 dovršava dokaz.

□

Sada ćemo definirati točkovnu i blokovnu orbitnu matricu kao što su definirane u [18].

Definicija 3.1. Točkovna orbitna matrica za parametre (v, k, λ) i distribuciju duljina orbita točaka $\omega = (\omega_1, ..., \omega_n)$, odnosno blokova $\Omega = (\Omega_1, ..., \Omega_m)$ je svaka $n \times m$ matrica $S = [\Gamma_{ij}]$ s elementima iz $\mathbb{N}_0$ za koju vrijedi sljedeće:

1. $0 \leq \Gamma_{ij} \leq \Omega_j$, $1 \leq i \leq n$, $1 \leq j \leq m$;
2. $\sum_{j=1}^{m} \Gamma_{ij} = r$, $1 \leq i \leq n$;
3. $\sum_{i=1}^{n} \frac{\omega_i}{\Omega_j}\Gamma_{ij} = k$, $1 \leq j \leq m$;
4. $\sum_{j=1}^{m} \frac{\omega_t}{\Omega_j}\Gamma_{sj}\Gamma_{tj} = \begin{cases} \lambda\omega_t, & s \neq t, \\ \lambda(\omega_t - 1) + r, & s = t. \end{cases}$;

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

Definicija 3.2. Blokovna orbitna matrica za parametre (v, k, λ) i distribuciju duljina orbita točaka $\omega = (\omega_1, ..., \omega_n)$, odnosno blokova $\Omega = (\Omega_1, ..., \Omega_m)$ je svaka $n \times m$ matrica $R = [\gamma_{ij}]$ s elementima iz $\mathbb{N}_0$ za koju vrijedi sljedeće:

1. $0 \leq \gamma_{ij} \leq \omega_i$, $1 \leq i \leq n$, $1 \leq j \leq m$;
2. $\sum_{i=1}^{n} \gamma_{ij} = k$, $1 \leq j \leq m$;
3. $\sum_{j=1}^{m} \frac{\Omega_j}{\omega_i}\gamma_{ij} = r$, $1 \leq i \leq n$;
4. $\sum_{j=1}^{m} \frac{\Omega_j}{\omega_s}\gamma_{sj}\gamma_{tj} = \begin{cases} \lambda\omega_t, & s \neq t, \\ \lambda(\omega_t - 1) + r, & s = t. \end{cases}$;

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

Napomena 3.3. Orbitne matrice jednoznačno su određene do na poredak redaka i stupaca.

Napomena 3.4. Budući da djelovanje grupe automorfizama G na $2-(v,k,\lambda)$ dizajn $\mathcal{D}$ inducira taktičku dekompoziciju dizajna, dobro su definirane matrice $S=[\Gamma_{ij}]$ i $R=[\gamma_{ij}]$, gdje su Γ_{ij} i γ_{ij} definirani kao ranije. Te matrice zadovoljavaju uvjete iz definicija točkovne, odnosno blokovne orbitne matrice zbog leme 3.1 i propozicije 3.2 te ih nazivamo **točkovna i blokovna orbitna matrica dizajna** $\mathcal{D}$ inducirana djelovanjem grupe G.

U simetričnom $2-(v,k,\lambda)$ dizajnu svaka dva različita bloka sijeku se u točno λ točaka. Za proizvoljan blokovni dizajn to općenito ne mora vrijediti. Zato uvodimo pojam presječnog broja blokova.

Definicija 3.3. Presječni broj blokova B_1 i B_2 $2-(v,k,\lambda)$ dizajna $\mathcal{D}$ je broj:

$$|B_1 \cap B_2|.$$

Sljedeća će nam lema koristiti kasnije kod konstrukcije samodualnih kodova pomoću orbitnih matrica blokovnih dizajna.

Lema 3.2. *Pretpostavimo da su u $2-(v,k,\lambda)$ dizajnu $\mathcal{D}$ svi presječni brojevi blokova (uključujući i k) kongruentni modulo p, gdje je p prost broj, tj. $|B_1 \cap B_2| \equiv k (mod\ p)$ za svaka dva bloka B_1 i B_2 dizajna. Neka su $S=[\Gamma_{ij}]$ i $R=[\gamma_{ij}]$ točkovna, odnosno blokovna orbitna matrica redom, inducirane djelovanjem grupe automorfizama dizajna $\mathcal{D}$. Tada vrijedi:*

$$S^T R \equiv k \cdot \begin{bmatrix} \Omega_1 & \cdots & \Omega_1 \\ \Omega_2 & \cdots & \Omega_2 \\ \vdots & & \vdots \\ \Omega_m & \cdots & \Omega_m \end{bmatrix} (mod\ p).$$

Posebno, ako su sve orbite točaka i blokova iste duljine q (q prost broj), tada vrijedi $S=R$ i

$$R^T R \equiv kq \cdot J (mod\ p)$$

gdje je J $m \times m$ matrica sa svim elementima jednakim 1.

Dokaz. Neka je $S^T R=[x_{js}]$, gdje je $1 \leq j \leq m$, $1 \leq s \leq m$. Elemente matrice $S^T R$

možemo raspisati slično kao u dokazu leme 3.1 pod b), odnosno na sljedeći način:

$$\begin{aligned} x_{js} &= \sum_{i=1}^{n} \Gamma_{ij}\gamma_{is} = \sum_{i=1}^{n} |\langle Q_i\rangle \cap B_j| \cdot |\langle x_s\rangle \cap P_i| = \sum_{i=1}^{n} |\langle x_s\rangle \cap P_i| \sum_{x\in B_j} |\langle Q_i\rangle \cap x| = \\ &= \sum_{i=1}^{n} \sum_{R\in\langle x_s\rangle\cap P_i} \sum_{x\in B_j} |R \cap \langle x\rangle| = \sum_{i=1}^{n} \sum_{x\in B_j} \sum_{R\in\langle x_s\rangle\cap P_i} |R \cap \langle x\rangle| = \\ &= \sum_{i=1}^{n} \sum_{x\in B_j} |\langle x_s\rangle \cap P_i \cap \langle x\rangle| = \sum_{x\in B_j} \sum_{i=1}^{n} |\langle x_s\rangle \cap P_i \cap \langle x\rangle| = \sum_{x\in B_j} |\langle x_s\rangle \cap \langle x\rangle| \equiv \\ &\equiv \sum_{x\in B_j} k (\text{mod } p) \equiv k \cdot \Omega_j (\text{mod } p). \end{aligned} \tag{3.2}$$

Ako je:

$$\Omega_1 = ... = \Omega_m = \omega_1 = ... = \omega_n = q, \quad \text{za } q \text{ prost broj},$$

tada iz leme 3.1 pod a) slijedi $\Gamma_{ij} = \gamma_{ij}$, odnosno $S = R$. Također $x_{js} \equiv k \cdot q (\text{mod } p)$, pa je:

$$R^T R \equiv kq \cdot J (\text{mod } p).$$

□

3.2 Samodualni kodovi iz blokovnih dizajna

U sljedećem ćemo dijelu konstruirati primjere samoortogonalnih i samodualnih kodova korištenjem proširenih orbitnih matrica blokovnih dizajna (koji ne moraju nužno biti simetrični).

Wilson u [52] opisuje rezultat Blokhuisa i Calderbanka [6] koji pokazuje kako se korištenjem matrica incidencije blokovnih dizajna, koji zadovoljavaju određene uvjete, može dobiti samodualne kodove. O tome govori sljedeći teorem.

Teorem 3.1. ([*52, Theorem* 25]) *Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn i p neparan prost broj koji točno dijeli $r-\lambda$ (tj. $p|(r-\lambda)$, ali $p^2 \nmid (r-\lambda)$). Pretpostavimo da je $|S\cap T| \equiv k (mod\ p)$ za svaka dva bloka S i T dizajna. Pretpostavimo i da je v neparan. Ako je:*

1. *$k \not\equiv 0 (mod\ p)$ tada je $(-1)^{(v-1)/2}k$ kvadrat modulo p;*
2. *$k \equiv 0 (mod\ p)$ tada je $(-1)^{(v-1)/2}v$ (nenul) kvadrat modulo p.*

Skica dokaza. Neka je N $v \times b$ matrica incidencije za dizajn $\mathcal{D}$. Definiramo matrice:

$$M = \left[\begin{array}{c|c} & 1 \\ N^T & \vdots \\ & 1 \end{array}\right] \quad \text{i} \quad M' = \left[\begin{array}{c|c} & 0 \\ N^T & \vdots \\ & 0 \\ \hline 1 \quad \cdots \quad 1 & 1 \end{array}\right].$$

1. Ako $p \nmid k$ pokaže se da je kod razapet retcima od M samodualan p-naran kod duljine $v+1$ u odnosu na $U = diag(1, ..., 1, -k)$.

2. Ako $p \mid k$ pokaže se da je kod razapet retcima od M' samodualan p-naran kod duljine $v+1$ u odnosu na $U' = diag(1, ..., 1, -v)$.

□

U dokazu prethodnog teorema koriste se transponirane matrice incidencije dizajna proširene na odgovarajući način, koje onda generiraju samodualne kodove u odnosu na određeni skalarni produkt. Wittov teorem 2.8 zatim daje rezultate o kvadratima u $\mathbb{F}_p$.

U nastavku ćemo konstruirati samoortogonalne i samodualne kodove na sličan način kao u teoremu 3.1, ali korištenjem orbitnih matrica blokovnih dizajna umjesto njihovih matrica incidencije.

Teorem 3.2. *Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn, $G \leq Aut(\mathcal{D})$, te ω_i, Ω_j, γ_{ij}, Γ_{ij} definirani kao ranije. Nadalje, neka je p prost broj takav da $p|(r-\lambda)$, te $p \nmid \Omega_1, ..., \Omega_m, \omega_1, ..., \omega_n$. Tada vrijedi:*

1. *ako $p \nmid \lambda$ tada postoji samoortogonalan p-naran kod duljine $m+1$ u odnosu na $U = diag(\Omega_1, ..., \Omega_m, -\lambda)$;*

2. *ako $p|\lambda$ i $p \nmid b$ tada postoji samoortogonalan p-naran kod duljine $m+1$ u odnosu na $V = diag(\Omega_1, ..., \Omega_m, -b)$.*

Dokaz. Neka je R blokovna orbitna matrica dizajna $\mathcal{D}$ inducirana djelovanjem grupe G, tj. $R = [\gamma_{ij}]$. Definiramo matrice:

$$M = \left[\begin{array}{c|c} & \omega_1 \\ R & \omega_2 \\ & \vdots \\ & \omega_n \end{array}\right] \quad \text{i} \quad M' = \left[\begin{array}{c|c} & 0 \\ R & \vdots \\ & 0 \\ \hline 1 \quad \cdots \quad 1 & 1 \end{array}\right].$$

1. Ako $p \nmid \lambda$ lako se provjeri da je kod razapet retcima matrice M samoortogonalan p-naran kod duljine $m+1$ u odnosu na $U = \text{diag}(\Omega_1, ..., \Omega_m, -\lambda)$. To slijedi iz činjenice

da je MUM^T nul-matrica modulo p, budući da su elementi te matrice oblika:

$$\sum_{j=1}^{m} \gamma_{ij}\gamma_{sj} \cdot \Omega_j - \lambda\omega_i\omega_s = \lambda\omega_i\omega_s + \delta_{is}(r-\lambda)\omega_i - \lambda\omega_i\omega_s = \delta_{is}(r-\lambda)\omega_i \equiv 0 (\text{mod } p).$$

2. Ako $p|\lambda$ i $p \nmid b$, tada retci matrice M' razapinju samoortogonalan p-naran kod duljine $m+1$ u odnosu na $V = \text{diag}(\Omega_1, ..., \Omega_m, -b)$. To vidimo zbog $M'VM'^T \equiv 0 \pmod{p}$. Naime, elementi te matrice su iz skupa:

$$\left\{ \sum_{j=1}^{m} \gamma_{ij}\gamma_{sj}\Omega_j, \sum_{j=1}^{m} \gamma_{ij}\Omega_j, b-b \right\} = \{\lambda\omega_i\omega_s + \delta_{is}(r-\lambda)\omega_i, r\omega_i, 0\}.$$

Zbog $p|\lambda$ i $p|(r-\lambda)$ vrijedi da $p|r$, pa su svi elementi matrice $M'VM'^T$ jednaki 0 u $\mathbb{F}_p$.

□

Prethodni teorem daje samoortogonalne kodove. Da bi dobili samodualne dodatno ćemo pretpostaviti djelovanje određene grupe automorfizama na dizajn $\mathcal{D}$. Konkretno, pretpostavit ćemo da na dizajn djeluje grupa automorfizama generirana automorfizmom bez fiksnih točaka i blokova, prostog reda q. Slično su pretpostavili Harada i Tonchev u [29], gdje su dobili samoortogonalne kodove pomoću orbitnih matrica.

Teorem 3.3. ([*29, Proposition* 1]) *Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn koji dopušta automorfizam Φ bez fiksnih točaka i bez fiksnih blokova, reda q, gdje je q prost broj. Neka je nadalje M orbitna matrica inducirana djelovanjem grupe $G = \langle\Phi\rangle$ na dizajn $\mathcal{D}$. Ako je p prost broj koji dijeli r i λ, tada orbitna matrica M generira samoortogonalan kod duljine b/q nad $\mathbb{F}_p$, gdje je b broj blokova od $\mathcal{D}$.*

Sljedećom konstrukcijom također dobivamo samoortogonalne kodove.

Teorem 3.4. *Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn koji dopušta automorfizam Φ prostog reda q bez fiksnih točaka i blokova, te R orbitna matrica inducirana djelovanjem grupe $G = \langle\Phi\rangle$ na dizajn $\mathcal{D}$. Ako su svi presječni brojevi blokova dizajna (uključujući i k) djeljivi sa p, gdje je p prost broj, tada matrica R^T generira samoortogonalan kod duljine $\frac{v}{q}$ nad $\mathbb{F}_p$.*

Dokaz. Budući da je grupa G prostog reda q, te nema fiksnih točaka ni blokova, slijedi da sve orbite točaka i blokova dizajna imaju duljinu jednaku q. Iz leme 3.1 pod a) dobivamo da je $\Gamma_{ij} = \gamma_{ij}$, odnosno $S = R$. Sada lema 3.2 daje:

$$R^T R \equiv kq \cdot J (\text{mod } p),$$

što je nul-matrica modulo p budući da $p|k$. Dakle, kod razapet s R^T je samoortogonalan nad $\mathbb{F}_p$ i duljine je $n = \frac{v}{q}$ (jer se skup točaka particionira u n orbita duljine q). □

Potrebne su nam i dvije leme i jedna propozicija koje govore o invarijantnim faktorima matrica, a čiji se dokazi mogu naći u [52].

Lema 3.3. *Neka je L $r \times k$ matrica i M $k \times r$ matrica, gdje je $r \geq k$. Ako je*

$$ML = dI$$

za neki cijeli broj d, tada svaki nenul invarijantni faktor od LM dijeli d.

Lema 3.4. *Neka je L $r \times k$ matrica i M $k \times r$ matrica, gdje je $r \geq k$. Neka su $s_1, ..., s_k$ i $s'_1, ..., s'_k$ invarijantni faktori od L i M redom i neka su $t_1, ..., t_r$ invarijantni faktori od LM (zadnjih $r - k$ od njih moraju biti nula, jer LM ima rang najviše k). Tada je:*

$$(s_1 s_2 \cdots s_k)(s'_1 s'_2 \cdots s'_k) = t_1 t_2 \cdots t_k.$$

Propozicija 3.3. *Pretpostavimo da $n \times k$ cjelobrojna matrica A ima rang n, tako A ima desni inverz nad Q. Tada postoji $k \times n$ cjelobrojna matrica B za koju je $AB = tI$ ako i samo ako je t višekratnik najvećeg invarijantnog faktora s_n od A. Slično, ako je B $k \times n$ cjelobrojna matrica ranga n, tada postoji cjelobrojna matrica A takva da je $AB = tI$ ako i samo ako je t višekratnik najvećeg invarijantnog faktora s'_n od B.*

Slijedi konstrukcija samodualnih kodova pomoću proširenih orbitnih matrica blokovnih dizajna, koje su inducirane djelovanjem grupe automorfizama prostog reda bez fiksnih točaka i blokova.

Teorem 3.5. *Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn koji dopušta automorfizam Φ prostog reda q bez fiksnih točaka i blokova, te R orbitna matrica inducirana djelovanjem grupe $G = \langle \Phi \rangle$ na dizajn $\mathcal{D}$. Neka je p prost broj takav da $p|(r-\lambda)$ ali $p^2 \nmid (r-\lambda)$, te $p \nmid q$. Ako je broj orbita točaka n neparan, te ako su svi presječni brojevi blokova dizajna (uključujući i k) kongruentni modulo p, tada:*

1. *ako $p \nmid k$ tada postoji samodualan p-naran kod duljine $n+1$ u odnosu na $U = diag(q, ..., q, -k)$;*
2. *ako $p|k$ tada postoji samodualan p-naran kod duljine $n+1$ u odnosu na $V = diag(1, ..., 1, -n)$.*

Dokaz. Opet, zbog uvjeta teorema, slijedi da sve orbite točaka i blokova dizajna imaju jednaku duljinu q. Iz leme 3.1 pod a) sada dobivamo da je $\Gamma_{ij} = \gamma_{ij}$, odnosno $S = R$.

Definiramo matrice:

$$M = \left[\begin{array}{c|c} R^T & \begin{matrix} q \\ \vdots \\ q \end{matrix} \end{array}\right] \quad \text{i} \quad M' = \left[\begin{array}{c|c} R^T & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 1 \quad \cdots \quad 1 & 1 \end{array}\right].$$

Zbog leme 3.2 imamo:

$$R^T R \equiv kq \cdot J (\text{mod } p).$$

1. Ako $p \nmid k$ matrica MUM^T ima elemente kongruentne sa $q \cdot kq - kq^2 = 0$ modulo p. Slijedi da retci matrice M razapinju samoortogonalan kod duljine $n+1$ u odnosu na $U = \text{diag}(q, ..., q, -\lambda)$, nad $\mathbb{F}_p$.

2. Ako $p \mid k$ tada matrica $M'VM'^T$ ima elemente kongruentne modulo p s elementima iz skupa

$$\{kq, \sum_{i=1}^{n} \gamma_{ij}, n-n\} = \{kq, k, 0\}.$$

Znači da su svi elementi te matrice kongruentni s nula modulo p jer $p \mid k$. Dobivamo da retci matrice M' razapinju samoortogonalan kod duljine $n+1$ u odnosu na $V = \text{diag}(1, ..., 1, -n)$, nad $\mathbb{F}_p$.

Zbog toga je $r_p(M) \leq \dfrac{n+1}{2}$, te $r_p(M') \leq \dfrac{n+1}{2}$.

Da dokažemo samodualnost kodova koje razapinju matrice M i M' nad $\mathbb{F}_p$ u odnosu na određene skalarne produkte, potrebno je još dokazati da je:

$$r_p(M) \geq \frac{n+1}{2} \quad \text{i} \quad r_p(M') \geq \frac{n+1}{2}.$$

Definiramo matrice A i B kao:

$$A = \left[\begin{array}{c|c} & q \\ R & \vdots \\ & q \end{array}\right] \quad \text{i} \quad B = \left[\begin{array}{c} R^T \\ \hline -\lambda \quad \cdots \quad -\lambda \end{array}\right].$$

Za te matrice očito je da vrijedi:

$$0 \leq r_p(A) - r_p(B) \leq 1. \tag{3.3}$$

Također, njihov umnožak jednak je:

$$AB = RR^T - \lambda qJ = (r - \lambda) \cdot I,$$

budući da su elementi matrice AB oblika:

$$\sum_{j=1}^{m} \gamma_{ij}\gamma_{sj} - \lambda q = \lambda q + \delta_{is}(r - \lambda) - \lambda q = \delta_{is}(r - \lambda).$$

Neka su $s_1, s_2, ..., s_n$ invarijantni faktori od A, te $s'_1, s'_2, ..., s'_n$ invarijantni faktori od B. Zbog leme 3.3, svi invarijantni faktori s_i i s'_i dijele $r - \lambda$, pa je svaki od njih djeljiv s najviše prvom potencijom od p.

Može se dobiti da je matrica BA oblika:

$$BA = \left[\begin{array}{ccc|c} & R^TR & & \begin{matrix} qk \\ \vdots \\ qk \end{matrix} \\ \hline -\lambda k & \cdots & -\lambda k & -\lambda v \end{array}\right] \equiv \left[\begin{array}{ccc|c} & qk \cdot J & & \begin{matrix} qk \\ \vdots \\ qk \end{matrix} \\ \hline -\lambda k & \cdots & -\lambda k & -\lambda v \end{array}\right] \pmod p,$$

pri čemu ova kongruencija vrijedi zbog leme 3.2.

Zbog

$$r(BA) \leq \min\{r(B), r(A)\},$$

vrijedi da je $\mathbb{Q}$-rang od BA manji ili jednak od broja redaka n od A. S druge strane,

$$r(BA) \geq r(R^TR) = r(RR^T) = n.$$

Ovdje posljednju jednakost, $r(RR^T) = n$, dobivamo jer je:

$$RR^T = \lambda q \cdot J + (r - \lambda) \cdot I.$$

Slijedi da je $r(BA) = n$, odnosno svi invarijantni faktori $t_1, ..., t_n$ od BA različiti su od nula. Lema 3.3 sada povlači da svi invarijantni faktori $t_1, ..., t_n$ dijele $r - \lambda$, tj. djeljivi su s najviše prvom potencijom od p. Lema 3.4 pak daje:

$$(s_1 \cdots s_n) \cdot (s'_1 \cdots s'_n) = t_1 \cdots t_n. \tag{3.4}$$

1. Ako $p \nmid k$, tada zbog $\lambda(v-1) = r(k-1)$ i $r \equiv \lambda \pmod p$ dobivamo $\lambda k \equiv \lambda v \pmod p$. Znači da su retci od BA konstantni retci modulo p, odnosno vrijedi:

   $$r_p(BA) = 1.$$

   Slijedi da samo jedan invarijantni faktor t_i nije djeljiv s p, tj. $(n-1)$ invarijantnih faktora t_i su djeljivi s točno prvom potencijom od p. Sada iz formula (3.4) i (3.3) dobivamo da je samo najvećih $\frac{n-1}{2}$ vrijednosti iz $\{s_1, ..., s_n\}$ i najvećih $\frac{n-1}{2}$ vrijednosti iz $\{s'_1, ..., s'_n\}$ djeljivo s p, dok ostale nisu. Zbog toga je:

   $$r_p(A) = r_p(B) = n - \frac{n-1}{2} = \frac{n+1}{2}.$$

(a) Ako $p|\lambda$ tada je:

$$r_p(M) \geq r_p(R) = r_p(B) = \frac{n+1}{2}.$$

(b) Ako $p \nmid \lambda$, tada je $r_p(R) = r_p(A)$, budući da je suma stupaca od R jednaka $k \cdot \mathbf{1}$, pa je $\mathbf{1} \in \mathrm{col}_p(R)$. Ponovno slijedi da je:

$$r_p(M) \geq r_p(R) = \frac{n+1}{2}.$$

2. Ako $p|k$ tada je

$$BA \equiv 0 (\mathrm{mod}\ p),$$

što znači da su svi invarijantni faktori $t_1, ..., t_n$ djeljivi s p. Iz formula (3.4) i (3.3) sada dobivamo da je:

$$r_p(A) = \frac{n+1}{2},\ r_p(B) = \frac{n-1}{2}.$$

Također, vrijedi da je $r_p(M') > r_p(R)$, te dobivamo:

$$r_p(M') \geq r_p(R) + 1 \geq r_p(A) = \frac{n+1}{2}.$$

Primijetimo da $p \nmid n$, jer bi inače $col_p(A)$ bio samoortogonalan p-naran kod duljine n i dimenzije strogo veće od $\frac{n}{2}$, što je nemoguće.

□

Zbog Wittovog teorema dobivamo i sljedeću posljedicu koja govori o kvadratima u $\mathbb{F}_p$.

Teorem 3.6. *Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn koji dopušta automorfizam Φ prostog reda q bez fiksnih točaka i bez fiksnih blokova, te neka je R orbitna matrica inducirana djelovanjem grupe $G = \langle \Phi \rangle$ na dizajn $\mathcal{D}$. Neka je p neparan prost broj takav da $p|(r-\lambda)$ ali $p^2 \nmid (r-\lambda)$, te $p \nmid q$. Ako je broj orbita točaka n neparan, te ako su svi presječni brojevi blokova dizajna (uključujući i k) kongruentni modulo p, tada vrijedi:*

1. *ako $p \nmid k$ tada je $(-1)^{\frac{n-1}{2}} kq^n$ kvadrat u $\mathbb{F}_p$;*

2. *ako $p|k$ i $p \nmid n$ tada je $(-1)^{\frac{n-1}{2}} n$ kvadrat u $\mathbb{F}_p$.*

Dokaz. Rezultat slijedi iz Wittovog teorema 2.8 i prethodnog teorema 3.5, budući da je:

$$\begin{aligned} \det(U) &= (-1)^{\frac{n+1}{2}} \cdot q^n \cdot (-k) = (-1)^{\frac{n-1}{2}} \cdot kq^n, \\ \det(V) &= (-1)^{\frac{n+1}{2}} \cdot (-n) = (-1)^{\frac{n-1}{2}} \cdot n. \end{aligned}$$

□

3.2.1 Primjeri samodualnih kodova iz simetričnih $2-(27,13,6)$ dizajna

K. Mackenzie-Fleming i K. W. Smith su u [37] konstruirali sve simetrične $(27,13,6)$ dizajne s automorfizmom prostog reda $q=3$ bez fiksnih točaka (i bez fiksnih blokova). Pokazali su da postoje točno 22 neizomorfna simetrična $2-(27,13,6)$ dizajna s automorfizmom bez fiksnih točaka σ reda 3. Automorfizam σ ima 9 orbita veličine 3 na skupu točaka i na skupu blokova, te je identificiran s permutacijom

$$(1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15)(16,17,18)(19,20,21)(22,23,24)(25,26,27)$$

na skupu točaka i na skupu blokova. U članku [37] prvo su konstruirane moguće orbitne matrice za dizajne s tim parametrima na koje djeluje automorfizam σ. Zatim su pomoću tih orbitnih matrica konstruirani i sami simetrični $2-(27,13,6)$ dizajni s automorfizmom σ, te je provjereno koji su od njih neizomorfni. Četiri orbitne matrice koje su dale simetrične dizajne traženog oblika su:

$$R_1=\begin{bmatrix}
1&0&0&2&2&2&2&2&2\\
0&1&3&1&1&1&2&2&2\\
0&3&1&2&2&2&1&1&1\\
2&1&2&0&2&3&1&1&1\\
2&1&2&2&3&0&1&1&1\\
2&1&2&3&0&2&1&1&1\\
2&2&1&1&1&1&0&2&3\\
2&2&1&1&1&1&2&3&0\\
2&2&1&1&1&1&3&0&2
\end{bmatrix},\quad
R_2=\begin{bmatrix}
1&0&0&2&2&2&2&2&2\\
0&1&3&1&1&1&2&2&2\\
0&3&1&2&2&2&1&1&1\\
2&1&2&3&1&1&0&1&2\\
2&1&2&1&3&1&2&0&1\\
2&1&2&1&1&3&1&2&0\\
2&2&1&2&0&1&3&1&1\\
2&2&1&1&2&0&1&3&1\\
2&2&1&0&1&2&1&1&3
\end{bmatrix},$$

$$R_3=\begin{bmatrix}
0&1&2&1&1&2&3&2&1\\
1&2&0&1&2&1&2&1&3\\
2&0&1&2&1&1&1&3&2\\
1&1&2&3&1&2&1&0&2\\
1&2&1&1&2&3&0&2&1\\
2&1&1&2&3&1&2&1&0\\
3&2&1&1&0&2&2&1&1\\
2&1&3&0&2&1&1&1&2\\
1&3&2&2&1&0&1&2&1
\end{bmatrix},\quad
R_4=\begin{bmatrix}
0&3&1&1&1&1&2&2&2\\
3&1&0&1&1&1&2&2&2\\
1&0&3&1&1&1&2&2&2\\
1&1&1&2&2&2&0&3&1\\
1&1&1&2&2&2&3&1&0\\
1&1&1&2&2&2&1&0&3\\
2&2&2&0&3&1&1&1&1\\
2&2&2&3&1&0&1&1&1\\
2&2&2&1&0&3&1&1&1
\end{bmatrix}.$$

Dizajni ovog tipa zadovoljavaju sve uvjete teorema 3.5 pod 1., za prost broj $p=7$. Zato primjenom teorema 3.5 na simetrične $(27,13,6)$-dizajne s automorfizmom σ reda 3,

dobivamo pomoću orbitnih matrica R_1, R_2, R_3, R_4 četiri samodualna $[10, 5]$ koda nad $\mathbb{F}_7$ u odnosu na $U = \text{diag}(3, 3, ..., 3, -13)$. To je iskazano u sljedećem teoremu.

Teorem 3.7. *Definiramo matrice*

$$M_i = \left[\begin{array}{c|c} & 3 \\ R_i^T & \vdots \\ & 3 \end{array}\right], \quad za \;\; i = 1, 2, 3, 4.$$

Tada retci matrica M_i generiraju samodualne $[10, 5]$ kodove nad $\mathbb{F}_7$ u odnosu na $U = diag(3, 3, ..., 3, -13)$.

Dokaz. Matrice R_i su orbitne matrice simetričnih $(27, 13, 6)$-dizajna s automorfizmom σ reda 3 bez fiksnih točaka i blokova definiranim ranije. Za prost broj $p = 7$ vrijedi da $p \nmid k = 13$, $p \nmid q = 3$, $p|(k - \lambda) = 7$, te $p^2 \nmid (k - \lambda) = 7$. Također, broj orbita točaka $n = 9$ je neparan. Presječni brojevi blokova za simetričan dizajn su samo $k = 13$ i $\lambda = 6$, a vrijedi $13 \equiv 6 (\text{mod } 7)$. Dakle, ispunjeni su svi uvjeti teorema 3.5 pod 1. Slijedi da su kodovi $row_7(M_i)$, za $i = 1, 2, 3, 4$, samodualni kodovi duljine $n + 1 = 10$ nad $\mathbb{F}_7$ u odnosu na $U = \text{diag}(3, 3, ..., 3, -13)$. □

3.3 Kodovi iz simetričnih blokovnih dizajna

U ovom ćemo dijelu opisati konstrukcije samodualnih kodova uz pomoć orbitnih matrica simetričnih dizajna. Nakon toga ćemo na sličan način kao za simetrične dizajne, konstruirati i samodualne kodove pomoću kvocijentnih matrica simetričnih grupovno djeljivih dizajna s dualnim svojstvom. Ideje za konstrukcije proizlaze iz teorema Assmusa, Mezzarobe i Salwacha u [2], koji će biti prezentiran u nastavku.

3.3.1 Konstrukcije samodualnih kodova iz simetričnih dizajna

Matrice incidencije simetričnih blokovnih dizajna pokazale su se korisne za konstrukciju samodualnih kodova. O tome govori sljedeći teorem Assmusa, Mezzarobe i Salwacha čiji se dokaz može naći u [2].

Prije samog iskaza teorema Assmusa i drugih, potrebna nam je sljedeća definicija kvadratnog ostatka modulo p.

Definicija 3.4. Neka je p prost broj i $q \in \mathbb{Z}$. Kažemo da je q **kvadratni ostatak** modulo p ako postoji cijeli broj x takav da je:

$$x^2 \equiv q (\text{mod } p).$$

Teorem 3.8. ([2]) *Neka je p prost broj i $\mathcal{D}$ simetričan (v, k, λ)-dizajn s matricom incidencije M.*

1. *Ako $p|k$ i $p|\lambda$, tada retci od M razapinju samoortogonalan kod nad $\mathbb{F}_p$.*

2. *Neka $p|(k-\lambda)$ i $p \nmid k$, te neka je $v \times (v+1)$ matrica G jednaka:*

$$G = \begin{bmatrix} \sqrt{-k} & \\ \sqrt{-k} & \\ \vdots & M \\ \sqrt{-k} & \end{bmatrix}.$$

   Ako je $-k$ kvadratni ostatak modulo p, uzmimo da je $\mathbb{F} = \mathbb{F}_p$, a inače $\mathbb{F} = \mathbb{F}_{p^2}$. Tada retci od G razapinju samoortogonalan kod nad $\mathbb{F}$. Nadalje, ako $p^2 \nmid (k-\lambda)$, tada je taj kod samodualan.

3. *Ako $p|\lambda$ i $p|(k+1)$, tada retci $v \times 2v$ matrice G razapinju samodualan $[2v, v]$ kod nad $\mathbb{F}_p$, gdje je G definirana kao:*

$$G = \begin{bmatrix} I & M \end{bmatrix}.$$

4. *Ako je $p = 2$, λ neparan, te k paran, tada retci $(v+1) \times (2v+2)$ matrice G razapinju samodualan $[2v+2, v+1]$ kod nad $\mathbb{F}_2$, gdje je G definirana kao:*

$$G = \begin{bmatrix} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I & \vdots & & M & \\ & 1 & & & \end{bmatrix}.$$

U dokazu prethodnog teorema 3.8 pod 2. potrebna je sljedeća lema.

Lema 3.5. *Neka je q potencija prostog broja. Svi elementi konačnog polja $\mathbb{F}_q$ su kvadrati u polju $\mathbb{F}_{q^2}$.*

Dokaz. Neka je $s \in \mathbb{F}_q$. Ako je polinom $x^2 - s$ reducibilan nad $\mathbb{F}_q$, tada s ima kvadratni korijen već u $\mathbb{F}_q$.

Ako je pak polinom $x^2 - s$ ireducibilan nad $\mathbb{F}_q$, tada je polje cijepanja tog polinoma kvadratno proširenje od $\mathbb{F}_q$, koje je jedinstveno do na izomorfizam, te mora biti izomorfno $\mathbb{F}_{q^2}$. [1] □

[1] O polinomima, polju cijepanja polinoma, te proširenjima polja može se više pročitati u [36].

Ako umjesto matrica incidencije simetričnih blokovnih dizajna uzmemo njihove orbitne matrice, inducirane djelovanjem određene grupe automorfizama, pomoću njih također možemo na sličan način kao u teoremu 3.8 dobiti samodualne kodove.

U nastavku ćemo promatrati simetrične (v, k, λ)-dizajne koji dopuštaju grupu automorfizama G koja djeluje na skupu točaka i na skupu blokova sa svim orbitama iste duljine.

Lander je u [35] dokazao sljedeći teorem.

Teorem 3.9. ([*35, Theorem* 3.3]) *Grupa automorfizama G simetričnog (v, k, λ)-dizajna ima isti broj točkovnih i blokovnih orbita.*

Neka je sada $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ simetričan (v, k, λ) dizajn i $G \leq Aut(\mathcal{D})$. Označimo kao ranije sa $P_1, ..., P_t$ G-orbite točaka, sa $B_1, ..., B_t$ G-orbite blokova te neka je:

$$|P_i| = \omega_i, \quad |B_j| = \Omega_j, \quad \text{gdje je } 1 \leq i \leq t,\ 1 \leq j \leq t.$$

Vidimo da je zbog prethodnog teorema broj orbita točaka t jednak broju orbita blokova. Neka su i brojevi γ_{ij}, Γ_{ij} definirani kao ranije na početku poglavlja.

Pretpostavimo da G djeluje na $\mathcal{D}$ s t orbita jednake duljine Ω na skupu točaka i na skupu blokova, tj. $\omega_i = \Omega_j = \Omega$, za sve $i, j \in \{1, ..., t\}$. Tada je:

$$t = \frac{v}{\Omega}. \tag{3.5}$$

Napomena 3.5. Za orbitne matrice dizajna $\mathcal{D}$ vrijede sljedeće tvrdnje.

a) Zbog leme 3.1 pod a) slijedi da je

$$\gamma_{ij} = \Gamma_{ij},$$

odnosno točkovna i blokovna orbitna matrica dizajna inducirane ovim djelovanjem su međusobno jednake. Označit ćemo tu orbitnu matricu sa R.

b) Lema 3.1 pod b) sada daje:

$$RR^T = (k - \lambda)I_t + \lambda\Omega J_t. \tag{3.6}$$

U [17] je dokazana tvrdnja sljedeće propozicije.

Propozicija 3.4. *Neka grupa G djeluje na simetričan (v, k, λ)-dizajn $\mathcal{D}$ sa t orbita duljine Ω na skupu točaka i na skupu blokova, te neka je R orbitna matrica dizajna inducirana tim djelovanjem. Tada vrijedi:*

$$|\det(R)| = k(k - \lambda)^{\frac{t-1}{2}}. \tag{3.7}$$

Dokaz. Matrica RR^T ima za vlastite vektore vektor sa svim jedinicama s vlastitom vrijednosti k^2, te $t-1$ vlastitih vektora

$$(1,-1,0,...,0),\ (0,1,-1,0,...,0),\ ...$$

s vlastitom vrijednosti $n = k - \lambda$. Slijedi da je

$$\det(RR^T) = k^2(k-\lambda)^{t-1}.$$

Zbog

$$\det(RR^T) = \det(R)\det(R^T) = [\det(R)]^2,$$

sada dobivamo da je:

$$|\det(R)| = k(k-\lambda)^{\frac{t-1}{2}}.$$

□

Konstrukcije samodualnih kodova pomoću orbitnih matrica simetričnih blokovnih dizajna opisat ćemo u sljedećem teoremu. Prva konstrukcija već je dokazana u [17], dok su ostale nove i dokazat ćemo ih u nastavku.

Teorem 3.10. *Neka je $\mathcal{D}$ simetričan (v,k,λ)-dizajn koji dopušta grupu automorfizama G koja djeluje na skupu točaka i na skupu blokova sa $t = \frac{v}{\Omega}$ orbita duljine Ω. Nadalje, neka je R orbitna matrica dizajna $\mathcal{D}$ inducirana djelovanjem grupe G, te p prost broj.*

1. *([17, Theorem 2.3]) Ako $p|k$ i $p|\lambda$, tada retci od R razapinju samoortogonalan kod duljine t nad $\mathbb{F}_p$.*

2. *Neka $p|(k-\lambda)$ i $p \nmid k\Omega$, te neka je $t \times (t+1)$ matrica G jednaka:*

$$G = \begin{bmatrix} \sqrt{-k\Omega} & \\ \sqrt{-k\Omega} & \\ \vdots & R \\ \sqrt{-k\Omega} & \end{bmatrix}.$$

   Ako je $-k\Omega$ kvadratni ostatak modulo p, uzmimo da je $\mathbb{F} = \mathbb{F}_p$, a inače $\mathbb{F} = \mathbb{F}_{p^2}$. Tada retci od G razapinju samoortogonalan kod nad $\mathbb{F}$. Nadalje, ako $p^2 \nmid (k-\lambda)$, tada je taj kod samodualan $[t+1, \frac{t+1}{2}]$ kod.

3. *Ako $p|\lambda$ i $p|(k+1)$, tada retci $t \times 2t$ matrice G razapinju samodualan $[2t,t]$ kod nad $\mathbb{F}_p$, gdje je G definirana kao:*

$$G = \begin{bmatrix} I & R \end{bmatrix}.$$

4. *Ako je $p = 2$, λ neparan, k paran, te Ω neparan, tada retci $(t+1) \times (2t+2)$ matrice G razapinju samodualan $[2t+2, t+1]$ kod nad $\mathbb{F}_2$, gdje je G definirana kao:*

$$G = \begin{bmatrix} & & 0 & 1 & \cdots & 1 \\ & & 1 & & & \\ & I & \vdots & & R & \\ & & 1 & & & \end{bmatrix}.$$

Dokaz. 1. Ovdje tvrdnja slijedi zbog $RR^T = (k-\lambda)I_t + \lambda\Omega J_t$.

2. Svi elementi matrice GG^T nalaze se u skupu

$$\{-k\Omega + k - \lambda + \lambda\Omega, -k\Omega + \lambda\Omega\} = \{(k-\lambda)(1-\Omega), -\Omega(k-\lambda)\},$$

odnosno svi su jednaki 0 modulo p. Znači da retci od G razapinju samoortogonalan kod duljine $t+1$ nad $\mathbb{F}$ (elementi koji su jednaki 0 u $\mathbb{F}_p$ jednaki su nula i u proširenju stupnja dva od $\mathbb{F}_p$ tj. $\mathbb{F}_{p^2}$, jer su elementi tog proširenja polinomi stupnja najviše jedan s koeficijentima iz $\mathbb{F}_p$). Zato je $r_p(G) \leq \frac{t+1}{2}$.

Ako $p^2 \nmid (k-\lambda)$, trebamo još pokazati da je $r_p(G) \geq \frac{t+1}{2}$. Znamo da za matricu R postoje cjelobrojne unimodularne matrice P i Q takve da je:

$$PRQ = \operatorname{diag}(d_1, ..., d_t), \quad \text{gdje } d_i | d_{i+1}, \text{ za } i = 1, ..., t-1.$$

Budući da su P i Q unimodularne, znamo da je:

$$|\det(PRQ)| = |\det(R)| = k(k-\lambda)^{\frac{t-1}{2}}.$$

Zbog $p|(k-\lambda)$ i $p^2 \nmid (k-\lambda)$, te $p \nmid k$, dobivamo da su najviše $\frac{t-1}{2}$ faktora d_i višekratnici od p. Slijedi da je

$$r_p(G) = r_p(R) = r_p(PRQ) \geq t - \frac{t-1}{2} = \frac{t+1}{2}.$$

Znači da retci od G razapinju samodualan $[t+1, \frac{t+1}{2}]$ kod nad $\mathbb{F}$.

3. Zbog činjenice da je:

$$RR^T = (k-\lambda)I_t + \lambda\Omega J_t,$$

dobivamo da su elementi matrice GG^T iz skupa

$$\{k - \lambda + \lambda\Omega + 1, \lambda\Omega\}.$$

Slijedi da je GG^T nul-matrica modulo p, odnosno retci od G razapinju samoortogonalan kod duljine $2t$ nad $\mathbb{F}_p$. Zbog $r_p(G) = t$ imamo da je dimenzija koda jednaka t, što znači da je taj kod samodualan $[2t, t]$ kod nad $\mathbb{F}_p$.

4. U ovom slučaju, zbog $k(k-1) = \lambda(v-1)$, slijedi da je v neparan. Sada zbog $t = \frac{v}{\Omega}$ dobivamo da je t također neparan. Znači da elementi matrice GG^T moraju biti iz skupa:

$$\{t+1, k, 2+k+\lambda(\Omega-1), 1+\lambda\Omega\},$$

odnosno svi su jednaki 0 modulo 2. Slijedi da retci od G razapinju samoortogonalan kod duljine $2t+2$ nad $\mathbb{F}_2$. Zbog $r_p(G) = t+1$ dobivamo da je taj kod samodualan $[2t+2, t+1]$ kod nad $\mathbb{F}_2$.

□

3.3.2 Analogne konstrukcije za simetrične grupovno djeljive dizajne s dualnim svojstvom

Slične konstrukcije samodualnih kodova kao u teoremima 3.8 i 3.10 možemo napraviti i koristeći kvocijentne matrice simetričnih grupovno djeljivih dizajna s dualnim svojstvom, umjesto matrica incidencije ili orbitnih matrica simetričnih dizajna.

Napomena 3.6. Neka je $D = (v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom, te R njegova kvocijentna matrica. Podsjetimo se da je

$$RR^T = (k^2 - v\lambda_2)I_m + n\lambda_2 J_m,$$

te da zbog formule (2.1) vrijedi i sljedeće:

$$k^2 - v\lambda_2 = (k - \lambda_1) + n(\lambda_1 - \lambda_2). \tag{3.8}$$

Teorem 3.11. *Neka je $D = (v, k, \lambda_1, \lambda_2, m, n)$ SGDD s dualnim svojstvom, R njegova kvocijentna matrica, te p prost broj.*

1. *(Već dokazano kao teorem 2.4) Ako $p \mid (k^2 - v\lambda_2)$ i $p \mid n\lambda_2$, tada retci od R razapinju samoortogonalan kod duljine m nad $\mathbb{F}_p$.*

2. *Neka $p|(k^2 - v\lambda_2)$, te $p \nmid n\lambda_2$, te neka je $m \times (m+1)$ matrica G jednaka:*

$$G = \begin{bmatrix} \sqrt{-n\lambda_2} & \\ \sqrt{-n\lambda_2} & \\ \vdots & R \\ \sqrt{-n\lambda_2} & \end{bmatrix}.$$

Ako je $-n\lambda_2$ kvadratni ostatak modulo p, uzmimo da je $\mathbb{F} = \mathbb{F}_p$, a inače $\mathbb{F} = \mathbb{F}_{p^2}$. Tada retci od G razapinju samoortogonalan kod nad $\mathbb{F}$. Nadalje, ako $p^2 \nmid (k^2 - v\lambda_2)$, te $p \nmid k$, tada je taj kod samodualan $[m+1, \frac{m+1}{2}]$ kod.

3. *Ako $p|n\lambda_2$ i $p|(k^2+1)$, tada retci $m \times 2m$ matrice G razapinju samodualan $[2m, m]$ kod nad $\mathbb{F}_p$, gdje je G definirana kao:*

$$G = \begin{bmatrix} I & R \end{bmatrix}.$$

4. *Ako je $p = 2$, k paran, te m, n i λ_2 neparni, tada retci $(m+1) \times (2m+2)$ matrice G razapinju samodualan $[2m+2, m+1]$ kod nad $\mathbb{F}_2$, gdje je G definirana kao:*

$$G = \begin{bmatrix} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I & \vdots & & R & \\ & 1 & & & \end{bmatrix}.$$

Dokaz. 1. Slijedi zbog $RR^T = (k^2 - v\lambda_2)I_m + n\lambda_2 J_m$.

2. Svi elementi matrice GG^T nalaze se u skupu:

$$\{-n\lambda_2 + k^2 - v\lambda_2 + n\lambda_2, -n\lambda_2 + n\lambda_2\} = \{k^2 - v\lambda_2, 0\},$$

odnosno svi su jednaki 0 modulo p. Znači da retci od G razapinju samoortogonalan kod duljine $m+1$ nad $\mathbb{F}$. Zato je $r_p(G) \leq \frac{m+1}{2}$.

Ako $p^2 \nmid (k^2 - v\lambda_2)$, trebamo još pokazati da je $r_p(G) \geq \frac{m+1}{2}$. Za matricu R postoje cjelobrojne unimodularne matrice P i Q takve da je:

$$PRQ = \operatorname{diag}(d_1, ..., d_m), \quad \text{gdje } d_i | d_{i+1}, \text{ za } i = 1, ..., m-1.$$

P i Q su unimodularne, pa vrijedi:

$$|\det(PRQ)| = |\det(R)| = k(k^2 - v\lambda_2)^{\frac{m-1}{2}}.$$

Zbog $p|(k^2 - v\lambda_2)$, $p^2 \nmid (k^2 - v\lambda_2)$, te $p \nmid k$, dobivamo da su najviše $\frac{m-1}{2}$ faktora d_i višekratnici od p. Slijedi da je

$$r_p(G) = r_p(R) = r_p(PRQ) \geq m - \frac{m-1}{2} = \frac{m+1}{2}.$$

Znači da retci od G razapinju samodualan $[m+1, \frac{m+1}{2}]$ kod nad $\mathbb{F}$.

3. Zbog činjenice da je:
$$RR^T = (k^2 - v\lambda_2)I_m + n\lambda_2 J_m,$$
dobivamo da su elementi matrice GG^T iz skupa
$$\{1 + k^2 - v\lambda_2 + n\lambda_2, n\lambda_2\}.$$
Slijedi da je GG^T nul-matrica modulo p, odnosno retci od G razapinju samoortogonalan kod duljine $2m$ nad $\mathbb{F}_p$. Zbog $r_p(G) = m$ imamo da je dimenzija koda jednaka m, što znači da je taj kod samodualan $[2m, m]$ kod nad $\mathbb{F}_p$.

4. Elementi matrice GG^T u ovom su slučaju iz skupa:
$$\{m + 1, k, 2 + k^2 - n\lambda_2(m - 1), 1 + n\lambda_2\},$$
odnosno svi su jednaki 0 modulo 2. Slijedi da retci od G razapinju samoortogonalan kod duljine $2m+2$ nad $\mathbb{F}_2$. Zbog $r_p(G) = m+1$ dobivamo da je taj kod samodualan $[2m + 2, m + 1]$ kod nad $\mathbb{F}_2$.

□

3.3.3 Samodualni kodovi iz Hadamardovih dizajna

U nastavku ćemo promotriti konstrukcije samodualnih kodova uz pomoć Hadamardovih matrica, odnosno Hadamardovih dizajna.

Definicija 3.5. Svaka Hadamardova matrica ekvivalentna je matrici oblika:
$$\begin{bmatrix} -1 & 1 & 1 & \cdots & 1 \\ 1 & & & & \\ 1 & & & & \\ \vdots & & & * & \\ 1 & & & & \end{bmatrix}.$$

Hadamardova matrica u ovom obliku naziva se **standardizirana Hadamardova matrica**.

Sljedeći teorem dokazao je Ozeki u [43].

Teorem 3.12. *Neka je H_n standardizirana Hadamardova matrica reda n, te neka je:*
$$K_n = \frac{1}{2}(H_n + J_n), \quad i \quad C_n = [I_n \mid K_n].$$
Ako je $n \equiv 4 (mod\ 8)$, tada retci matrice C_n generiraju dvostruko paran samodualan kod duljine $2n$ nad $\mathbb{F}_2$. Štoviše, ekvivalentne Hadamardove matrice daju ekvivalentne kodove.

Napomena 3.7. Ako u standardiziranoj Hadamardovoj matrici H reda $n = 4a$ izbacimo prvi redak i prvi stupac, te zatim zamijenimo sve -1 sa nulama, lako se provjeri da se dobije matrica incidencije Hadamardovog $2-(4a-1, 2a, a)$-dizajna.

Neka je standardizirana Hadamardova matrica H reda $n = 4a$ dana kao:

$$H = \begin{bmatrix} -1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & M' & \\ 1 & & & \end{bmatrix}.$$

Tada je matrica incidencije pripadnog $(4a-1, 2a, a)$ Hadamardovog dizajna jednaka:

$$M = \frac{1}{2}(M' + J).$$

Teorem 3.12 sada možemo izreći u sljedećem obliku.

Teorem 3.13. *Neka je H standardizirana Hadamardova matrica reda $n = 4a$, gdje je $n \equiv 4 (mod\ 8)$, te neka je $\mathcal{D}$ pripadni simetrični $(4a-1, 2a, a)$ Hadamardov dizajn s matricom incidencije M. Tada retci matrice G razapinju dvostruko paran samodualan kod duljine $2n$ nad $\mathbb{F}_2$, gdje je G definirana kao:*

$$G = \begin{bmatrix} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I & \vdots & & M & \\ & 1 & & & \end{bmatrix}.$$

Napomena 3.8. Tvrdnju prethodnog teorema ranije je dokazao i Tonchev u [51], s dodatnom tvrdnjom da svaki takav kod ima minimalnu težinu barem 8 za $a > 0$.

Napomena 3.9. Vidimo da je prethodni teorem posebni slučaj Assmusovog teorema 3.8 pod 4., budući da je $p = 2$, $\lambda = a$ neparan (zbog $n \equiv 4 (\text{mod } 8)$), te $k = 2a$ paran. Stoga je dobiveni kod samodalan kod duljine $2n$ nad $\mathbb{F}_2$. Budući da su u ovom slučaju težine svih redaka generirajuće matrice G djeljive sa 4, kod je također i dvostruko paran.

Ako umjesto matrice incidencije Hadamardovog dizajna uzmemo njegovu orbitnu matricu induciranu djelovanjem grupe automorfizama dizajna sa svim orbitama iste duljine, tada dobivamo poseban slučaj teorema 3.10 pod 4.

Teorem 3.14. *Neka je H standardizirana Hadamardova matrica reda $n = 4a$, gdje je $n \equiv 4 (mod\ 8)$, te neka je $\mathcal{D}$ pripadni simetrični $(4a-1, 2a, a)$ Hadamardov dizajn. Neka $\mathcal{D}$ dopušta grupu automorfizama koja djeluje na skupu točaka i na skupu blokova sa $t = \frac{4a-1}{\Omega}$*

orbita duljine Ω*, te neka je* R *orbitna matrica dizajna* $\mathcal{D}$ *inducirana tim djelovanjem. Tada retci matrice* G *razapinju samodualan kod duljine* $2t+2$ *nad* $\mathbb{F}_2$*, gdje je* G *definirana kao:*

$$G = \begin{bmatrix} & & 0 & 1 & \cdots & 1 \\ & & 1 & & & \\ & I & \vdots & & R & \\ & & 1 & & & \end{bmatrix}.$$

Dokaz. Zbog $n = 4a$ i $n \equiv 4 (\text{mod } 8)$ imamo da je a neparan. Slijedi da je $p = 2$, $\lambda = a$ neparan, te $k = 2a$ paran. Sada teorem 3.10 pod 4. daje da je dobiveni kod samodalan kod duljine $2t + 2$ nad $\mathbb{F}_2$. □

3.3.4 Kroneckerov produkt

Definicija 3.6. Kroneckerov produkt dviju matrica A i B, gdje je $A = [a_{ij}]$ $n \times m$ matrica, je matrica:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ & & \cdots & \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{bmatrix}.$$

U sljedećem je teoremu pokazano kako uz pomoć Kroneckerovog produkta generirajućih matrica samodualnih kodova određenog oblika možemo konstruirati nove samodualne kodove. Dokaz teorema može se naći u [41].

Teorem 3.15. *Ako su* $[I_k \mid A_1]$ *i* $[I_l \mid A_2]$ *generirajuće matrice samodualnih kodova, tada je to i matrica* $[I_{kl} \mid A_1 \otimes A_2]$.

Napomena 3.10. Teoremi 3.8 pod 3. i 4., 3.10 pod 3. i 4., te 3.11 pod 3. i 4. daju konstrukcije samodualnih kodova s generirajućim matricama oblika $[I \mid A]$, za neku matricu A.
Znači da na generirajuće matrice dobivene tim teoremima možemo primijeniti prethodni teorem 3.15, te tako uz pomoć Kroneckerovog produkta dobiti nove samodualne kodove.

Poglavlje 4

PD-skupovi

Postupak permutacijskog dekodiranja koda, uveden od J. MacWilliams u [38], koristi određene skupove automorfizama koda koje nazivamo PD-skupovi. Ne mora se svaki kod nužno moći dekodirati ovom tehnikom, odnosno za neke kodove možda ne postoje PD-skupovi.

Ovo je poglavlje posvećeno dokazivanju postojanja, te pronalaženju PD-skupova za određene kodove povezane s flag-tranzitivnim simetričnim dizajnima. Ovdje opisani rezultati, osim teorema 4.9, dani su u [14]. U nastavku ćemo pokazati da se kod razapet retcima matrice incidencije incidencijskog grafa flag-tranzitivnog simetričnog dizajna može permutacijski dekodirati, budući da bilo koja flag-tranzitivna grupa automorfizama dizajna može poslužiti kao PD-skup za potpuno ispravljanje pogrešaka[1] za taj kod. Rezultat ćemo poopćiti i za kodove povezane s flag-tranzitivnim SGGD-ima s dualnim svojstvom.

Također ćemo proučiti konkretne primjere kodova proizašlih iz nekih flag-tranzitivnih simetričnih dizajna te za njih naći i manje PD-skupove za specifične informacijske skupove.

Pri konstrukciji primjera korišteni su programski paketi GAP [23] i Magma [9].

4.1 Kodovi iz matrica incidencije grafova

U ovom su potpoglavlju opisani rezultati o kodovima iz matrica incidencije grafova iz rada Dankelmann, Key, Rodrigues [19]. Te ćemo rezultate koristiti u nastavku.

Neka je G matrica incidencije grafa $\Gamma = (V, E)$. Sa $C_p(G)$ ćemo označiti kod razapet retcima od G nad konačnim poljem $\mathbb{F}_p$, gdje je p prost broj.

Teorem 4.1. ([*19, Result* 1]) *Neka je $\Gamma = (V, E)$ povezan graf i G njegova matrica incidencije. Tada je:*

1. $\dim(C_2(G)) = |V| - 1$*;*

[1] Pod potpuno ispravljanje pogrešaka misli se na ispravljanje pogrešaka do punoga kapaciteta za ispravljanje pogrešaka danoga koda.

2. *za neparan p,* $\dim(C_p(G)) = |V|$ *ako* Γ *nije bipartitan i* $\dim(C_p(G)) = |V| - 1$ *ako je* Γ *bipartitan.*

Teorem 4.2. ([*19, Theorem* 1]) *Neka je* $\Gamma = (V, E)$ *povezan graf, te* G $|V| \times |E|$ *matrica incidencije za* G*. Tada:*

1. $C_2(G)$ *je* $[|E|, |V| - 1, \lambda(\Gamma)]_2$ *kod,*

2. *ako je* Γ *super-*λ*, tada je* $C_2(G)$ $[|E|, |V| - 1, \delta(\Gamma)]_2$ *kod i minimalne riječi su retci od* G *težine* $\delta(\Gamma)$*.*

Slijedi da je za graf Γ za koji je $\delta(\Gamma) = \lambda(\Gamma)$, minimalna težina binarnog koda $C_2(G)$ iz matrice incidencije grafa jednaka minimalnom stupnju vrhova grafa $\delta(\Gamma)$.

Teorem 4.3. ([*19, Theorem* 2]) *Neka je* $\Gamma = (V, E)$ *povezan bipartitan graf,* G $|V| \times |E|$ *matrica incidencije za* Γ*, te* p *neparan prost broj. Tada:*

1. $C_p(G)$ *je* $[|E|, |V| - 1, \lambda(\Gamma)]_p$ *kod,*

2. *ako je* Γ *super-*λ*, tada je* $C_p(G)$ $[|E|, |V| - 1, \delta(\Gamma)]_p$ *kod i minimalne riječi su nenul skalarni višekratnici redaka od* G *težine* $\delta(\Gamma)$*.*

Teorem 4.4. ([*19, Result* 3]) *Neka je* $\Gamma = (V, E)$ *povezan bipartitan graf. Tada je* $\lambda(\Gamma) = \delta(\Gamma)$ *ako vrijedi neki od uvjeta:*

1. V *ima najviše dvije orbite pod djelovanjem* $Aut(\Gamma)$*, i posebno ako je* Γ *tranzitivan po vrhovima,*

2. *svaka dva vrha iz iste klase particije imaju zajedničkog susjeda,*

3. $diam(\Gamma) \leq 3$*,*

4. Γ *je* k*-regularan i* $k \geq \dfrac{n+1}{4}$*,*

5. Γ *ima struk* g *i* $diam(\Gamma) \leq g - 1$*.*

Ako je $\delta(\Gamma) = \lambda(\Gamma)$ *i vrijedi neki od sljedećih uvjeta, tada je* Γ *super-*λ*:*

(1a) Γ *je tranzitivan po vrhovima,*

(2a) Γ *je* k*-regularan i* $k \geq \dfrac{n+3}{4}$*.*

4.2 Flag-tranzitivne grupe automorfizama simetričnih dizajna kao PD-skupovi

U ovom potpoglavlju pokazat ćemo da kod razapet retcima matrice incidencije incidencijskog grafa flag-tranzitivnog simetričnog dizajna posjeduje PD-skup, tj. može se permutacijski dekodirati.

4.2.1 PD-skupovi i permutacijsko dekodiranje

Definicija 4.1. Neka je $C \subseteq \mathbb{F}_p^n$ linearan $[n, k, d]$ kod. Za $I \subseteq \{1, ..., n\}$ neka je $p_I : \mathbb{F}_p^n \to \mathbb{F}_p^{|I|}$, $x \mapsto x|_I$, I-projekcija od $\mathbb{F}_p^n$. Tada se I zove **informacijski skup** za C ako je $|I| = k$ i $p_I(C) = \mathbb{F}_p^{|I|}$.

Skup prvih k koordinata za riječi koda s generirajućom matricom u standardnom obliku je informacijski skup.

Definicija 4.2. Neka je $C \subseteq \mathbb{F}_p^n$ linearan $[n, k, d]$ kod koji može ispraviti najviše t pogrešaka (tj. t-error-correcting kod) te I informacijski skup za C. Podskup $S \subseteq \mathrm{Aut}(C)$ se naziva **PD-skup** za C ako za svaki podskup $B \subseteq \{1, ..., n\}$ za koji je $|B| \leq t$ postoji automorfizam $\sigma \in S$ takav da je $\sigma(B) \cap I = \emptyset$. To znači da je $S \subseteq \mathrm{Aut}(C)$ PD-skup za C ako se svaki t-podskup koordinatnih pozicija može preslikati s barem jednim elementom iz S izvan informacijskog skupa I.

Algoritam permutacijskog dekodiranja (vidi [39], [30]) koristi PD-skupove i on je to učinkovitiji što je manja veličina PD-skupa. Donja granica za veličinu PD-skupa dana je u sljedećem teoremu i za nju je zaslužan Gordon ([25]), te se naziva **Gordonova granica**.

Teorem 4.5. ([*25*]) *Ako je S PD-skup za $[n, k, d]$ kod C koji može ispraviti t grešaka, $r = n - k$, tada je:*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil .$$

4.2.2 Flag-tranzitivni simetrični dizajni

Definicija 4.3. Flag ili **zastavica** simetričnog dizajna je incidentan par točke i bloka.

Definicija 4.4. Incidencijski graf ili **Levijev graf** simetričnog dizajna (ili bilo koje incidencijske strukture) je graf kojemu su vrhovi točke i blokovi dizajna, a bridovi incidentni parovi točaka i blokova (tj. flagovi dizajna).

Lako se provjeri da je incidencijski graf Γ simetričnog (v, k, λ)-dizajna bipartitan (klase particije su skupovi točaka i blokova dizajna) i k-regularan (svaka točka je incidentna s k blokova i svaki blok je incidentan s k točaka).

Napomena 4.1. Incidencijski graf Γ simetričnog (v, k, λ)-dizajna ima dijametar $\mathrm{diam}(\Gamma)$ jednak tri.

Dokaz. Moguća su tri slučaja:

(i) $d(u, v) = 1 \Leftrightarrow (u, v)$ je flag,

(ii) $d(u, v) = 2 \Leftrightarrow (u, v)$ su dvije različite točke ili dva različita bloka,

(iii) $d(u,v) = 3 \Leftrightarrow (u,v)$ su neincidentna točka i blok (antiflag).

□

Definicija 4.5. Kažemo da je grupa automorfizama simetričnog dizajna $\mathcal{D}$ **flag-tranzitivna** ako je tranzitivna na skupu flagova od $\mathcal{D}$.

Klasifikacija flag-tranzitivnih simetričnih dizajna još je otvoren problem. H. Davies [20] dokazao je da za $\lambda > 1$ postoji konačno mnogo (v,k,λ)-dizajna (ne nužno simetričnih) koji dopuštaju flag-tranzitivnu imprimitivnu grupu automorfizama, i to dokazujući da je u tom slučaju k ograničen. Neki daljnji rezultati prema klasifikaciji flag-tranzitivnih simetričnih dizajna mogu se naći u [44] i [42].

Dankelmann, Key i Rodrigues pokazali su u [19] sljedeći rezultat.

Teorem 4.6. ([*19, Result* 7]) *Neka je $\Gamma = (V,E)$ k-regularan graf s grupom automorfizama A tranzitivnom na bridovima i neka je G matrica incidencije za Γ. Ako je $C = C_p(G)$ $[|E|, |V| - \varepsilon, k]_p$ kod, gdje je p prost broj i $\varepsilon \in \{0, 1, ...|V| - 1\}$, tada je bilo koja tranzitivna podgrupa od A PD-skup za potpuno ispravljanje pogrešaka za C.*

Teorem 4.6 primijenjen na incidencijski graf flag-tranzitivnog simetričnog dizajna vodi ka sljedećem rezultatu.

Teorem 4.7. *Neka je $\Gamma = (V,E)$ incidencijski graf simetričnog (v,k,λ)-dizajna $\mathcal{D}$ s flag-tranzitivnom grupom automorfizama A i neka je G matrica incidencije za Γ. Tada je $C = C_p(G)$ $[|E|, |V| - 1, k]_p$ kod, za bilo koji prost broj p, i bilo koja flag tranzitivna podgrupa od A može poslužiti kao PD-skup (za bilo koji informacijski skup) za potpuno ispravljanje pogrešaka za kod C.*

Dokaz. Γ je povezan i bipartitan graf pa prema teoremu 4.3 i teoremu 4.4 slijedi da je $C_p(G)$ kod s parametrima $[|E|, |V| - 1, \lambda(\Gamma)]_p$. Zbog $\mathrm{diam}(\Gamma) = 3$ te jer svaka dva vrha iz iste klase particije imaju zajedničkog susjeda, teorem 4.4 daje $\lambda(\Gamma) = \delta$. Γ je k-regularan, pa je minimalni stupanj od Γ jednak $\delta = k$. Dakle, slijedi da je $C_p(G)$ $[|E|, |V| - 1, k]_p$ kod, za bilo koji prost broj p. Grupa A je flag-tranzitivna na $\mathcal{D}$, pa je A tranzitivna na bridovima od Γ. Sada možemo primijeniti teorem 4.6 što dovršava dokaz. □

4.3 Primjeri

Za sljedeće računalne rezultate korišteni su programski paketi GAP [23] i Magma [9].

Prvo ćemo pogledati primjere flag-tranzitivnih simetričnih dizajna s $\lambda = 1$, tj. flag-tranzitivne projektivne ravnine. Tada ćemo istražiti flag-tranzitivne simetrične dizajne s $\lambda = 2$, tj. flag-tranzitivne dvoravnine. Pronaći ćemo sve flag-tranzitivne podgrupe punih grupa automorfizama dizajna. Te podgrupe su PD-skupovi za kodove dobivene iz dizajna (za bilo koji informacijski skup).

Parametri linearnog $[n, k, d]_p$ koda dobivenog iz flag-tranzitivnog simetričnog (v, k', λ)-dizajna na opisani način, mogu se prema teoremu 4.7 izračunati kako slijedi: duljina je $n = v \cdot k'$ (tj. broj flagova), dimenzija je $k = 2v - 1$ i minimalna težina $d = k'$.

4.3.1 Flag-tranzitivne projektivne ravnine

Sljedeći teorem dokazao je W. Kantor ([33]).

Teorem 4.8. *Ako je $\mathcal{D}$ projektivna ravnina reda n koja dopušta flag-tranzitivnu grupu automorfizama A, tada ili:*

(i) $\mathcal{D}$ je Desarguesova i $A \triangleright PSL(3, n)$, ili

(ii) A je strogo flag-tranzitivna Frobeniusova grupa neparnog reda $(n^2 + n + 1)(n + 1)$ i $n^2 + n + 1$ je prost broj.

Ispitat ćemo tri primjera flag-tranzitivnih projektivnih ravnina, točnije simetrične dizajne s parametrima (7,3,1), (13,4,1) i (21,5,1). Ove ravnine su $PG_2(\mathbb{F}_q)$ za $q = 2, 3, 4$. Informacije o PD-skupovima iz flag-tranzitivnih grupa automorfizama ovih projektivnih ravnina dane su u tablici 4.1.

i	Flag-tranzitivna projektivna ravnina $\mathcal{D}_i$	Kod $C_p(G_i)$	Gordonova granica g_i	Redovi svih flag-tranzitivnih podgrupa grupe automorfizama A_i
1	$(7, 3, 1)$	[21,13,3]	3	21,168
2	$(13, 4, 1)$	[52,25,4]	2	5616
3	$(21, 5, 1)$	[105,41,5]	4	20160, 40320, 60480, 120960

Tablica 4.1: Flag-tranzitivne grupe automorfizama projektivnih ravnina kao PD-skupovi

Pronađeni PD-skupovi garantiraju da se odgovarajući kod može permutacijski dekodirati. No, te flag-tranzitivne podgrupe, tj. PD-skupovi, su velikog reda, puno većeg od Gordonove granice. Ipak, našli smo i manje PD-skupove za spomenute kodove za specifične informacijske skupove, kao što je prikazano u tablici 4.2.

i	Flag-tranzitivna projektivna ravnina $\mathcal{D}_i$	Kod $C_2(G_i)$	Gordonova granica g_i	Najmanji PD-skup pronađen u A_i
1	$(7, 3, 1)$	[21,13,3]	3	4
2	$(13, 4, 1)$	[52,25,4]	2	4
3	$(21, 5, 1)$	[105,41,5]	4	64

Tablica 4.2: Najmanji PD-skupovi nađeni u kodovima dobivenim iz projektivnih ravnina $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$

Neki manji PD-skupovi za binarne kodove $C_2(G)$ za projektivne ravnine navedeni su u tablici 4.2 i dani u primjerima ispod.

U tablici 4.2, kodovi iz prva dva primjera ispravljaju samo jednu pogrešku, pa PD-skupovi nisu nužni, te bi korištenje sindroma bilo dovoljno za dekodiranje (vidi npr. [30], str.177). Zato su primjeri 4.1 i 4.2 od akademske ali ne i praktične koristi.

Koordinatne pozicije $1, 2, ..., n$ iz danih informacijskih skupova u sljedećim primjerima odgovaraju flagovima početnog simetričnog dizajna. Točnije, pridruživanje je dano sa:

$$\begin{aligned}
1 &\equiv (\text{"prva točka iz prvog bloka", "prvi blok"}) \\
2 &\equiv (\text{"druga točka iz prvog bloka", "prvi blok"}) \\
&\vdots \\
k' &\equiv (\text{"}k'\text{-ta točka iz prvog bloka", "prvi blok"}) \\
k'+1 &\equiv (\text{"prva točka iz drugog bloka", "drugi blok"}) \\
&\vdots \\
2k' &\equiv (\text{"}k'\text{-ta točka iz drugog bloka", "drugi blok"}) \\
&\vdots \\
n = v \cdot k' &\equiv (\text{"}k'\text{-ta točka iz } v\text{-tog bloka", "}v\text{-ti blok"})
\end{aligned}$$

gdje su blokovi i točke uzeti u redu u kojem su navedeni u skupu blokova.

Primjer 4.1. Neka je $\mathcal{D}_1$ simetričan $(7, 3, 1)$-dizajn sa skupom točaka

$$\mathcal{P}_1 = \{1, 2, 3, 4, 5, 6, 7\},$$

te skupom blokova

$$\mathcal{B}_1 = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 7\}, \{2, 5, 6\}, \{3, 4, 6\}, \{3, 5, 7\}\}.$$

Za odgovarajući $[21, 13, 3]_2$ kod Gordonova granica je $g_1 = 3$ i postoji točno 2752512 PD-skupova veličine četiri za informacijski skup:

$$I_1 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 16, 19\}.$$

PD-skup veličine tri nije pronađen, ali nisu svi podskupovi od A_1 veličine tri provjereni. Jedan od PD-skupove veličine četiri za I_1 je grupa S_1 generirana elementom a:

$$a = (1, 13, 20, 9)(2, 14, 21, 7)(3, 15, 19, 8)(4, 10, 6, 12)(5, 11)(16, 18).$$

Primjer 4.2. Neka je $\mathcal{D}_2$ simetričan $(13, 4, 1)$-dizajn sa skupom točaka

$$\mathcal{P}_2 = \{1, 2, 3, ..., 13\}$$

i skupom blokova

$\mathcal{B}_2 = \{\{1,2,3,4\},\{1,5,6,7\},\{1,8,9,10\},\{1,11,12,13\},\{2,5,9,11\},\{2,6,8,13\},$
$\{2,7,10,12\},\{3,5,10,13\},\{3,6,9,12\},\{3,7,8,11\},\{4,5,8,12\},\{4,6,10,11\},$
$\{4,7,9,13\}\}.$

Za odgovarajući $[52,25,4]_2$ kod Gordonova granica je $g_2 = 2$. Pronašli smo PD-skup veličine četiri za informacijski skup

$$I_2 = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,21,25,29,33,37,41,45,49\}.$$

PD-skupovi veličine dva ili tri nisu pronađeni, ali nisu provjereni svi podskupovi od A_2 tih veličina. Pronađeni PD-skup veličine četiri za I_2 je grupa S_2 generirana elementom b:

$b = (1,15,42,17)(2,13,44,18)(3,16,43,19)(4,14,41,20)(5,28,6,25)(7,27)(8,26)$
$(9,36,30,21)(10,35,29,24)(11,33,32,23)(12,34,31,22)(37,52,39,51)(38,50)(40,49)$
$(45,48)(46,47)$.

Primjer 4.3. Neka je $\mathcal{D}_3$ simetričan $(21,5,1)$-dizajn sa skupom točaka

$$\mathcal{P}_3 = \{1,2,3,...,21\}$$

i skupom blokova:

$\mathcal{B}_3 = \{\{1,2,3,4,5\},\{1,6,7,8,9\},\{1,10,11,12,13\},\{1,14,19,20,21\},\{1,15,16,17,18\},$
$\{2,6,12,14,15\},\{2,7,10,18,21\},\{2,8,11,17,20\},\{2,9,13,16,19\},\{3,6,13,17,21\},$
$\{3,7,11,14,16\},\{3,8,10,15,19\},\{3,9,12,18,20\},\{4,6,11,18,19\},\{4,7,13,15,20\},$
$\{4,8,12,16,21\},\{4,9,10,14,17\},\{5,6,10,16,20\},\{5,7,12,17,19\},\{5,8,13,14,18\},$
$\{5,9,11,15,21\}\}.$

Za odgovarajući $[105,41,5]_2$ kod Gordonova granica je $g_3 = 4$. Za informacijski skup

$I_3 = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,31,36,$
$41,46,51,56,61,66,71,76,81,86,91,96,101\},$

pronašli smo PD-skup veličine 64. To je permutacijska grupa generirana sa sljedećih šest elemenata:

$c_1 = (1,5)(2,4)(6,91)(7,94)(8,92)(9,95)(10,93)(11,101)(12,104)(13,103)(14,102)$
$(15,105)(16,96)(17,99)(18,97)(19,100)(20,98)(21,86)(22,88)(23,89)(24,87)(25,90)$
$(26,81)(27,85)(28,82)(29,84)(30,83)(31,71)(32,72)(33,74)(34,75)(35,73)(36,66)(37,70)$

$(38,68)(39,67)(40,69)(41,76)(42,78)(43,80)(44,79)(45,77)(47,49)(48,50)(57,60)(58,59)$
$(62,63)(64,65)$,

$c_2 = (1,73)(2,75)(3,72)(4,71)(5,74)(6,48)(7,47)(8,46)(9,49)(10,50)(11,15)(12,14)$
$(16,43)(17,44)(18,45)(19,41)(20,42)(21,98)(22,96)(23,99)(24,97)(25,100)(26,90)(27,87)$
$(28,88)(29,89)(30,86)(31,65)(32,61)(33,63)(34,64)(35,62)(36,40)(37,39)(51,52)(54,55)$
$(56,92)(57,94)(58,93)(59,91)(60,95)(76,81)(77,85)(78,83)(79,84)(80,82)(101,104)$
$(102,105)$,

$c_3 = (1,57)(2,58)(3,56)(4,59)(5,60)(6,9)(7,10)(11,37)(12,36)(13,38)(14,39)(15,40)$
$(16,97)(17,99)(18,96)(19,98)(20,100)(21,77)(22,76)(23,79)(24,78)(25,80)(26,83)(27,82)$
$(28,85)(29,84)(30,81)(31,33)(34,35)(41,88)(42,87)(43,90)(44,89)(45,86)(46,61)(47,62)$
$(48,65)(49,63)(50,64)(66,104)(67,102)(68,103)(69,105)(70,101)(71,74)(73,75)(91,95)$
$(93,94)$,

$c_4 = (1,48)(2,49)(3,46)(4,47)(5,50)(6,73)(7,71)(8,72)(9,75)(10,74)(11,15)(12,14)$
$(16,98)(17,99)(18,100)(19,97)(20,96)(21,43)(22,42)(23,44)(24,41)(25,45)(26,85)(27,81)$
$(28,83)(29,84)(30,82)(31,94)(32,92)(33,93)(34,95)(35,91)(36,39)(37,40)(56,61)(57,65)$
$(58,63)(59,62)(60,64)(66,67)(69,70)(76,87)(77,90)(78,88)(79,89)(80,86)(101,105)$
$(102,104)$,

$c_5 = (1,63)(2,65)(3,61)(4,64)(5,62)(6,93)(7,95)(8,92)(9,94)(10,91)(11,14)(12,15)$
$(16,28)(17,29)(18,27)(19,26)(20,30)(21,78)(22,80)(23,79)(24,77)(25,76)(31,75)(32,72)$
$(33,73)(34,71)(35,74)(36,40)(37,39)(41,90)(42,86)(43,88)(44,89)(45,87)(46,56)(47,60)$
$(48,58)(49,57)(50,59)(66,69)(67,70)(81,100)(82,96)(83,98)(84,99)(85,97)(101,102)$
$(104,105)$,

$c_6 = (1,16)(2,19)(3,17)(4,18)(5,20)(6,21)(7,25)(8,23)(9,24)(10,22)(26,65)(27,64)$
$(28,63)(29,61)(30,62)(31,90)(32,89)(33,88)(34,87)(35,86)(36,40)(37,39)(41,75)(42,74)$
$(43,73)(44,72)(45,71)(46,99)(47,100)(48,98)(49,97)(50,96)(51,54)(52,55)(56,84)(57,85)$
$(58,83)(59,82)(60,81)(66,70)(67,69)(76,95)(77,94)(78,93)(79,92)(80,91)(101,105)$
$(102,104)$.

4.3.2 Flag-tranzitivne dvoravnine

Postoji samo šest poznatih flag-tranzitivnih dvoravnina. Primijenit ćemo opisanu konstrukciju PD-skupova na njih pet, budući da šesta flag-tranzitivna dvoravnina ima parametre $(37,9,2)$ i zato daje incidencijski graf s 333 bridova što je prezahtjevno za traženi izračun. Informacije o flag-tranzitivnim dvoravninama i njihovim punim grupama auto-

morfizama i točkovnim stabilizatorima dane su u [42]. Sve flag-tranzitivne podgrupe njihovih punih grupa automorfizama su PD-skupovi za kod dobiven iz dizajna, za bilo koji informacijski skup. Informacije o PD-skupovima iz flag-tranzitivnih grupa automorfizama dvoravnina dane su u tablici 4.3.

i	Flag-tranzitivni simetrični dizajn $\mathcal{D}_i$, puna grupa automorfizama A_i, točkovni stabilizator	Kod $C_p(G_i)$	Gordonova granica g_i	redovi svih flag-tranzitivnih podgrupa od A_i
4	$(4,3,2)$, S_4, S_3	[12,7,3]	3	12, 24
5	$(7,4,2)$, $PSL_2(7)$, S_4	[28,13,4]	2	168
6	$(11,5,2)$, $PSL_2(11)$, A_5	[55,21,5]	4	55, 660
7	$(16,6,2)$, 2^4S_6, S_6	[96,31,6]	3	96, 192, 288, 384, 576, 768, 960, 1152, 1920, 5760, 11520
8	$(16,6,2)$, $(\mathbb{Z}_2 \times \mathbb{Z}_8)(S_2.4)$, $(S_2.4)$	[96,31,6]	3	384, 768

Tablica 4.3: Flag-tranzitivne grupe automorfizama dvoravnina kao PD-skupovi

Flag-tranzitivne podgrupe iz tablice 4.3 velikog su reda (kao PD-skupovi). Našli smo i manje PD-skupove za spomenute kodove, za specifične informacijske skupove, kao što je prikazano u tablici 4.4.

i	Flag-tranzitivni dizajn $\mathcal{D}_i$	Kod $C_2(G_i)$	Gordonova granica g_i	Najmanji PD-skup pronađen u A_i
4	$(4,3,2)$	[12,7,3]	3	3
5	$(7,4,2)$	[28,13,4]	2	3
6	$(11,5,2)$	[55,21,5]	4	10
7	$(16,6,2)$	[96,31,6]	3	12
8	$(16,6,2)$	[96,31,6]	3	9

Tablica 4.4: Najmanji PD-skupovi nađeni za kodove dobivene iz dvoravnina $\mathcal{D}_4, \ldots, \mathcal{D}_8$

U primjeru 4.5 samo puna grupa automorfizama dizajna $\mathcal{D}_5$ je flag-tranzitivna. U primjerima 4.4, 4.6 i 4.8 postoji još jedna flag-tranzitivna podgrupa, osim pune grupe automorfizama. U primjeru 4.7. postoji 11 flag-tranzitivnih podgrupa pune grupe automorfizama od $\mathcal{D}_7$. Neki manji PD-skupovi za binarne kodove $C_2(G)$ za dvoravnine navedene u tablici 4.3 dani su u primjerima ispod i navedeni u tablici 4.4.

Kodovi iz primjera 4.4 i 4.5 ispravljaju samo jednu pogrešku pa permutacijsko dekodiranje nije od praktične koristi.

Primjer 4.4. Neka je $\mathcal{D}_4$ simetričan $(4,3,2)$-dizajn sa skupom točaka $\mathcal{P}_4 = \{1,2,3,4\}$ i skupom blokova $\mathcal{B}_4 = \{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$. Za odgovarajući $[12,7,3]_2$ kod Gordonova granica je $g_4 = 3$ i postoji točno 128 PD-skupova veličine tri za informacijski skup $I_4 = \{1,2,3,4,6,7,10\}$. Jedan od PD-skupova za I_4 je

$S_4 = \{(1,2,5,4)(3,10,6,7)(8,11,12,9),\ (1,5,12,8)(2,6,11,7)(3,4,10,9),$
$(1,6,8,10)(2,4,9,11)(3,5,7,12)\}.$

Primjer 4.5. Neka je $\mathcal{D}_5$ simetričan $(7,4,2)$-dizajn sa skupom točaka $\mathcal{P}_5 = \{1,2,3,4,5,6,7\}$ i blokovima

$$\mathcal{B}_5 = \{\{1,2,3,4\},\{1,3,5,6\},\{1,2,5,7\},\{1,4,6,7\},\{2,3,6,7\},\{2,4,5,6\},\{3,4,5,7\}\}.$$

Ne postoje PD-skupovi veličine $g_5 = 2$ za odgovarajući $[28,13,4]_2$ kod za informacijski skup $I_5 = \{1,2,3,4,5,7,8,9,12,13,17,21,25\}$. No, postoji točno 90944 PD-skupova veličine tri za I_5. Jedan od njih je

$S_5 = \{(1,3,25,28,12,9)(2,6,26,20,11,13)\ (4,18,27,16,10,5)(7,14,17)(8,22,19,23,15,21),$
$(1,6)(2,7,4,8)(3,5)(9,25,13,18)(10,27,14,19)(11,26,15,17)(12,28,16,20)(21,23,22,24),$
$(1,7,28,17)(2,5,27,20)(3,6,25,18)(4,8,26,19)(9,11,12,10)(13,23,16,21)(14,24)(15,22)\}.$

Primjer 4.6. Neka je $\mathcal{D}_6$ simetričan $(11,5,2)$-dizajn sa skupom točaka $\mathcal{P}_6 = \{1,2,3,...,11\}$ i skupom blokova:

$\mathcal{B}_6 = \{\{1,3,4,5,9\},\{2,4,5,6,10\},\{3,5,6,7,11\},\{1,4,6,7,8\},\{2,5,7,8,9\},$
$\{3,6,8,9,10\},\{4,7,9,10,11\},\{1,5,8,10,11\},\{1,2,6,9,11\},\{1,2,3,7,10\},\{2,3,4,8,11\}\}.$

Nismo pronašli PD-skupove veličine $g_6 = 4$ za odgovarajući $[55,21,5]_2$ kod za informacijski skup

$$I_6 = \{1,2,3,4,5,6,7,9,10,11,14,15,16,20,21,26,31,36,41,46,51\},$$

ali nisu provjereni svi podskupovi veličine četiri grupe automorfizama koda A_6. Nijedna podgrupa grupe A_6 reda četiri, pet ili šest nije PD-skup za I_6. Ali, postoji točno 24 podgrupa od A_6 reda 10 koje su PD-skupovi za I_6. Jedna od njih je permutacijska grupa generirana s generatorima d i e:

$d = (2,16)(3,46)(4,36)(5,41)(6,34)(7,50)(8,39)(9,30)(11,20)(12,38)(13,28)(14,54)$
$(15,24)(17,48)(18,26)(19,52)(21,35)(22,40)(23,55)(25,45)(29,43)(31,47)(32,51)$

$(33, 42)(49, 53)$,

$e = (1, 10, 44, 37, 27)(2, 7, 42, 40, 28)(3, 6, 45, 38, 26)(4, 9, 41, 39, 29)(5, 8, 43, 36, 30)$
$(11, 17, 47, 35, 24)(12, 18, 46, 34, 25)(13, 16, 50, 33, 22)(14, 19, 49, 32, 23)(15, 20, 48, 31, 21)$
$(51, 55, 54, 52, 53)$.

Primjer 4.7. Neka je $\mathcal{D}_7$ simetričan $(16, 6, 2)$-dizajn sa skupom točaka $\mathcal{P}_7 = \{1, 2, 3, ..., 16\}$ i skupom blokova:
$\mathcal{B}_7 = \{\{1, 2, 3, 4, 5, 6\}, \{1, 2, 13, 14, 15, 16\}, \{1, 3, 9, 10, 11, 13\}, \{1, 4, 7, 8, 9, 16\},$
$\{1, 5, 8, 10, 12, 14\}, \{1, 6, 7, 11, 12, 15\}, \{2, 3, 7, 8, 12, 13\}, \{2, 4, 10, 11, 12, 16\},$
$\{2, 5, 7, 9, 11, 14\}, \{2, 6, 8, 9, 10, 15\}, \{3, 4, 9, 12, 14, 15\}, \{3, 5, 7, 10, 15, 16\},$
$\{3, 6, 8, 11, 14, 16\}, \{4, 5, 8, 11, 13, 15\}, \{4, 6, 7, 10, 13, 14\}, \{5, 6, 9, 12, 13, 16\}\}$.

Gordonova granica za odgovarajući $[96, 31, 6]_2$ kod je $g_7 = 3$. Pronašli smo 16 PD-skupova veličine 12 za informacijski skup
$I_7 = \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 15, 16, 17, 19, 21, 22, 25, 29, 31, 37, 43, 49, 55, 61, 67, 73,$
$79, 85, 91\}$.

Nisu svi podskupovi veličine 12 (ili manje) provjereni (jer izračun postaje složeniji s većom grupom automorfizama). Jedan od tih PD-skupova veličine 12 je

$S_7 =$ { (), (1,8)(3,37)(4,43)(5,49)(6,55)(9,13)(10,25)(11,31)(12,19)(14,42)(15,95)(16,89)
(17,83)(20,48)(21,72)(22,78)(23,96)(26,54)(27,77)(28,90)(29,65)(32,60)(33,71)(34,84)(35,66)
(39,67)(40,73)(41,61)(45,85)(46,79)(47,62)(51,68)(52,91)(53,80)(57,74)(58,92)(59,86)(63,94)
(70,87)(76,81), (1,14)(2,18)(3,13)(4,15)(5,16)(6,17)(7,38)(8,42)(9,37)(10,39)(11,40)
(12,41)(19,61)(20,63)(21,65)(22,66)(23,62)(24,64)(25,67)(26,70)(27,71)(28,68)(29,72)(30,69)
(31,73)(32,76)(33,77)(34,74)(35,78)(36,75)(43,95)(44,93)(45,91)(46,92)(47,96)(48,94)(49,89)
(50,88)(51,90)(52,85)(53,86)(54,87)(55,83)(56,82)(57,84)(58,79)(59,80)(60,81), (1,23,54,74)
(2,24,50,75)(3,20,51,76)(4,21,53,73)(5,22,49,78)(6,19,52,77)(7,93,30,56)(8,96,26,57)
(9,94,28,60)(10,92,25,58)(11,95,29,59)(12,91,27,55)(13,63,90,32)(14,62,87,34)(15,65,86,31)
(16,66,89,35)(17,61,85,33)(18,64,88,36)(37,48,68,81)(38,44,69,82)(39,46,67,79) (40,43,72,80)
(41,45,71,83)(42,47,70,84), (1,23,87,34)(2,93,88,82)(3,63,90,76)(4,52,86,17)(5,58,89,46)
(6,15,85,53)(7,24,69,36)(8,96,70,84)(9,48,68,60)(10,78,67,66)(11,12,72,71)(13,20,51,32)
(14,62,54,74)(16,79,49,92)(18,44,50,56)(19,21,33,31)(22,39,35,25)(26,57,42,47)(27,40,41,29)
(28,81,37,94)(30,75,38,64)(43,91,59,83)(45,80,55,95)(61,65,77,73) , (1,26)(2,30)(3,28)(4,27)
(5,25)(6,29)(7,50)(8,54)(9,51)(10,49)(11,52)(12,53)(13,68)(14,70)(15,71)(16,67)(17,72)
(18,69)(19,80)(20,81)(21,83)(22,79)(23,84)(24,82)(31,91)(32,94)(33,95)(34,96)(35,92)(36,93)
(37,90)(38,88)(39,89)(40,85)(41,86)(42,87)(43,77)(44,75)(45,73)(46,78)(47,74)(48,76)(55,65)
(56,64)(57,62)(58,66)(59,61)(60,63), (1,34,54,62)(2,36,50,64)(3,32,51,63) (4,31,53,65)
(5,35,49,66)(6,33,52,61)(7,82,30,44)(8,84,26,47)(9,81,28,48) (10,79,25,46)(11,80,29,43)
(12,83,27,45)(13,76,90,20)(14,74,87,23)(15,73,86,21) (16,78,89,22)(17,77,85,19)(18,75,88,24)
(37,60,68,94)(38,56,69,93)(39,58,67,92)(40,59,72,95)(41,55,71,91)(42,57,70,96), (1,34,87,23)

(2,82,88,93)(3,76,90,63)(4,17,86,52)(5,46,89,58)(6,53,85,15) (7,36,69,24)(8,84,70,96)
(9,60,68,48)(10,66,67,78)(11,71,72,12)(13,32,51,20)(14,74,54,62)(16,92,49,79)(18,56,50,44)
(19,31,33,21)(22,25,35,39)(26,47,42,57)(27,29,41,40)(28,94,37,81)(30,64,38,75)(43,83,59,91)
(45,95,55,80)(61,73,77,65) , (1,42)(2,18)(3,9)(4,95)(5,89)(6,83)(7,38)(8,14)(10,67)(11,73)
(12,61)(13,37)(15,43)(16,49)(17,55)(19,41)(20,94)(21,29)(22,35)(23,47)(24,64) (25,39)(26,87)
(27,33)(28,51)(30,69)(31,40)(32,81)(34,57)(36,75)(44,93)(45,52) (46,58)(48,63)(50,88)(53,59)
(54,70)(56,82)(60,76)(62,96)(65,72)(66,78)(68,90) (71,77)(74,84)(79,92)(80,86)(85,91),
(1,47,87,57)(2,44,88,56)(3,48,90,60) (4,45,86,55)(5,46,89,58)(6,43,85,59)(7,64,69,75)
(8,62,70,74)(9,63,68,76)(10,66,67,78)(11,61,72,77)(12,65,71,73)(13,94,51,81)(14,96,54,84)
(15,91,53,83)(16,92,49,79)(17,95,52,80)(18,93,50,82)(19,29,33,40)(20,28,32,37)(21,27,31,41)
(22,25,35,39)(23,26,34,42)(24,30,36,38), (1,47,54,84)(2,64,50,36)(3,94,51,60)(4,29,53,11)
(5,35,49,66)(6,41,52,71)(7,44,30,82)(8,62,26,34)(9,20,28,76)(10,79,25,46)(12,85,27,17)
(13,48,90,81)(14,96,87,57)(15,72,86,40)(16,78,89,22)(18,24,88,75)(19,45,77,83)(21,59,73,95)
(23,70,74,42)(31,43,65,80)(32,37,63,68)(33,55,61,91)(38,93,69,56)(39,58,67,92) , (1,54)(2,30)
(3,90)(4,77)(5,10)(6,65)(7,50)(8,26)(9,68)(11,91)(12,80)(13,51)(14,87)(15,33)(16,39)
(17,21)(18,69)(19,53)(20,76)(22,46)(23,34)(24,82)(25,49)(27,43)(28,37)(29,55)(31,52)(32,63)
(35,58)(36,93)(38,88)(40,45)(41,59)(42,70)(44,75)(47,57)(48,81)(56,64)(60,94)(61,86)(62,74)
(66,92)(67,89)(71,95)(72,83)(73,85)(78,79)(84,96) }.

Primjer 4.8. Neka je $\mathcal{D}_8$ simetrični $(16, 6, 2)$-dizajn sa skupom točaka $\mathcal{P}_8 = \{1, 2, 3, ..., 16\}$ i skupom blokova $\mathcal{B}_8 = \{\{1, 2, 3, 4, 5, 6\}, \{1, 2, 13, 14, 15, 16\}, \{1, 3, 9, 10, 11, 13\}, \{1, 4, 7, 8, 9, 16\}, \{1, 5, 8, 10, 12, 14\}, \{1, 6, 7, 11, 12, 15\}, \{2, 3, 7, 8, 10, 15\}, \{2, 4, 10, 11, 12, 16\}, \{2, 5, 7, 9, 11, 14\}, \{2, 6, 8, 9, 12, 13\}, \{3, 4, 9, 12, 14, 15\}, \{3, 5, 7, 12, 13, 16\}, \{3, 6, 8, 11, 14, 16\}, \{4, 5, 8, 11, 13, 15\}, \{4, 6, 7, 10, 13, 14\}, \{5, 6, 9, 10, 15, 16\}\}$.

Za odgovarajući $[96, 31, 6]_2$ kod sa grupom automorfizama A_8, Gordonova granica je $g_8 = 3$. Među svim podgrupama od A_8 reda 12, postoji točno 104 podgrupa koje su PD-skupovi za informacijski skup
$I_8 = \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 15, 16, 17, 19, 21, 22, 25, 29, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 91\}$.

Jedan od tih PD-skupova veličine 12 je permutacijska grupa generirana sa sljedećim permutacijama:

$f = (1, 82)(2, 81)(3, 83)(4, 79)(5, 80)(6, 84)(7, 76)(8, 75)(9, 73)(10, 77)(11, 74)(12, 78)$
$(13, 17)(14, 18)(15, 16)(19, 46)(20, 44)(21, 47)(22, 43)(23, 45)(24, 48)(25, 53)(26, 50)(27, 49)$
$(28, 52)(29, 51)(30, 54)(31, 34)(32, 36)(33, 35)(37, 57)(38, 60)(39, 59)(40, 55)(41, 58)(42, 56)$
$(61, 89)(62, 85)(63, 88)(64, 87)(65, 90)(66, 86)(67, 71)(69, 70)(92, 95)(93, 94)$,

$g = (1, 84, 69)(2, 81, 72)(3, 79, 71)(4, 83, 67)(5, 80, 68)(6, 82, 70)(7, 42, 21)(8, 40, 24)$
$(9, 38, 20)(10, 41, 23)(11, 39, 19)(12, 37, 22)(13, 66, 87)(14, 62, 89)(15, 65, 88)(16, 63, 90)$
$(17, 64, 86)(18, 61, 85)(25, 95, 51)(26, 91, 50)(27, 96, 49)(28, 93, 54)(29, 92, 53)(30, 94, 52)$

$(31,36,33)(32,34,35)(43,57,78)(44,60,73)(45,58,77)(46,59,74)(47,56,76)(48,55,75)$,

$h = (1,53)(2,49)(3,52)(4,54)(5,50)(6,51)(7,46)(8,43)(9,45)(10,44)(11,47)(12,48)$
$(13,17)(14,15)(16,18)(19,76)(20,77)(21,74)(22,75)(23,73)(24,78)(25,82)(26,80)(27,81)$
$(28,83)(29,84)(30,79)(31,34)(32,33)(35,36)(37,55)(38,58)(39,56)(40,57)(41,60)(42,59)$
$(61,63)(62,65)(64,66)(67,93)(68,91)(69,92)(70,95)(71,94)(72,96)(85,90)(86,87)(88,89).$

U ovom PD-skupu veličine 12 pronašli smo šest PD-skupova veličine devet. Nisu provjereni svi podskupovi veličine devet ili manje. Jedan od tih PD-skupova veličine devet za I_8 je

$S_8 =$ { (1,29,69,53,84,92)(2,27,72,49,81,96)(3,30,71,52,79,94)(4,28,67,54,83,93)
(5,26,68,50,80,91)(6,25,70,51,82,95)(7,59,21,46,42,74)(8,57,24,43,40,78)(9, 58,20,45,38,77)
(10,60,23,44,41,73)(11,56,19,47,39,76)(12,55,22,48,37,75)(13,64,87,17,66,86)(14,65,89,15,62,88)
(16,61,90,18,63,85)(31,35,33,34,36,32), (1,51)(2,49)(3,54)(4,52)(5,50)(6,53)(7,39)(8,37)(9,41)
(10,38)(11,42)(12,40)(13,87)(14,90)(15,85)(16,89)(17,86)(18,88)(19,21)(20,23)(22,24)(25,69)
(26,68)(27,72)(28,71)(29,70)(30,67)(31,33)(32,34)(43,55)(44,58)(45,60)(46,56)(47,59)(48,57)
(61,65)(62,63)(73,77)(74,76)(75,78)(79,93)(80,91)(81,96)(82,92)(83,94)(84,95),(1,53)(2,49)
(3,52)(4,54)(5,50)(6,51)(7,46)(8,43)(9,45)(10,44)(11,47)(12,48)(13,17)(14,15)(16,18)(19,76)
(20,77)(21,74)(22,75)(23,73)(24,78)(25,82)(26,80)(27,81)(28,83)(29,84)(30,79)(31,34)(32,33)
(35,36)(37,55)(38,58)(39,56)(40,57)(41,60)(42,59)(61,63)(62,65)(64,66)(67,93)(68,91)(69,92)
(70,95)(71,94)(72,96)(85,90)(86,87)(88,89), (1,69,84)(2,72,81)(3,71,79)(4,67,83)(5,68,8)(6,70,82)
(7,21,42)(8,24,40)(9,20,38)(10,23,41)(11,19,39)(12,22,37)(13,87,66)(14,89,62)(15,88,65)
(16,90,63)(17,86,64)(18,85,61)(25,51,95)(26,50,91)(27,49,96)(28,54,93)(29,53,92)(30,52,94)
(31,33,36)(32,35,34)(43,78,57)(44,73,60)(45,77,58)(46,74,59)(47,76,56)(48,75,55), (1,70)(2,72)
(3,67)(4,71)(5,68)(6,69)(7,47)(8,48)(9,44)(10,45)(11,46)(12,43)(13,64)(14,61)(15,63)(16,65)
(17,66)(18,62)(19,59)(20,60)(21,56)(22, 57)(23,58)(24,55)(25,29)(28,30)(31,35)(32,33)(34,36)
(37,78)(38,73)(39,74)(40,75)(41,77)(42,76)(49,96)(50,91)(51,92)(52,93)(53,95)(54,94)(79,83)
(82,84)(85,89)(86,87)(88,90), (1,82)(2,81)(3,83)(4,79)(5,80)(6,84)(7,76)(8,75)(9,73)(10,77)
(11,74)(12,78)(13,17)(14,18)(15,16)(19,46)(20,44)(21,47)(22,43)(23,45)(24,48)(25,53)(26,50)
(27,49)(28,52)(29,51)(30,54)(31,34)(32,36)(33,35)(37,57)(38,60)(39,59)(40,55)(41,58)(42,56)
(61,89)(62,85)(63,88)(64,87)(65,90)(66,86)(67,71)(69,70)(92,95)(93,94),(1,84,69)(2,81,72)
(3,79,71)(4,83,67)(5,80,68)(6,82,70)(7,42,21)(8,40,24)(9,38,20)(10,41,23)(11,39,19)(12,37,22)
(13,66,87)(14,62,89)(15,65,88)(16,63,90)(17,64,86)(18,61,85)(25,95,51)(26,91,50)(27,96,49)
(28,93,54)(29,92,53)(30,94,52)(31,36,33)(32,34,35)(43,57,78)(44,60,73)(45,58,77)(46,59,74)
(47,56,76)(48,55,75), (1,92,84,53,69,29)(2,96,81,49,72,27)(3,94,79,52,71,30)(4,93,83,54,67,28)
(5,91,80,50,68,26)(6,95,82,51,70,25)(7,74,42,46,21,59)(8,78,40,43,24,57)(9,77,38,45,20,58)
(10,73,41,44,23,60)(11,76,39,47,19,56)(12,75,37,48,22,55)(13,86,66,17,87,64)(14,88,62,15,89,65)
(16,85,63,18,90,61)(31,32,36,34,33,35), (1,95)(2,96)(3,93)(4,94)(5,91)(6,92)(7,11)(8,12)(9,10)

(13,66)(14,63)(15,61)(16,62)(17,64)(18,65)(19,42)(20,41)(21,39)(22,40)(23,38)(24,37)(25,84)
(26,80)(27,81)(28,79)(29,82)(30,83)(31,36)(34,35)(43,48)(44,45)(46,47)(49,72)(50,68)(51,69)
(52,67)(53,70)(54,71)(55,78)(56,74)(57,75)(58,73)(59,76)(60,77)(85,88)(89,90) }.

4.4 Flag-tranzitivne grupe automorfizama simetričnih grupovno djeljivih dizajna s dualnim svojstvom kao PD-skupovi

Budući da se simetrični grupovno djeljivi dizajni mogu promatrati kao poopćenje simetričnih dizajna, prethodni se teorem, teorem 4.7, može generalizirati i za SGDD-e s dualnim svojstvom.

Teorem 4.9. *Neka je $\Gamma = (V, E)$ incidencijski graf simetričnog grupovno djeljivog dizajna s dualnim svojstvom $D(v, k, \lambda_1, \lambda_2, m, n)$ ($\lambda_1 > 0, \lambda_2 > 0$) s flag-tranzitivnom grupom automorfizama A i neka je G matrica incidencije za Γ. Tada vrijedi da je kod $C = C_p(G)$ $[|E|, |V| - 1, k]_p$ kod, za bilo koji prost broj p, i bilo koja flag tranzitivna podgrupa od A može poslužiti kao PD-skup (za bilo koji informacijski skup) za potpuno ispravljanje pogrešaka za kod C.*

Dokaz. Slično kao i za simetričan dizajn i za SGDD s dualnim svojstvom se može lagano pokazati da je njegov incidencijski graf uz dane uvjete povezan, bipartitan, k-regularan graf s $\text{diam}(\Gamma) = 3$. Slijedi da je $C_p(G)$ $[|E|, |V| - 1, k]_p$ kod, za bilo koji prost broj p. Opet, zbog flag-tranzitivnosti od A, imamo da je A tranzitivna na bridovima od Γ. Teorem 4.6 sada daje tvrdnju teorema. □

Literatura

[1] E. F. Assmus, Jr., J. D. Key, Designs and their codes, Cambridge Tracts in Math., vol. 103, Cambridge University Press, Cambridge, 1992.

[2] E. F. Assmus, Jr., J. A. Mezzaroba, C. J. Salwach, Planes and biplanes, Proceedings of the 1976 Berlin Combinatorics Conference, Vance-Reidle (1977), 205–212.

[3] R. Balakrishnan, K. Ranganathan, A Textbook of Graph Theory, Springer, New York, 2012.

[4] H. Beker, C. Mitchell, F. Piper, Tactical decompositions of designs, Aequationes Math. 25 (1982), 123–152.

[5] T. Beth, D. Jungnickel, H. Lenz, Design Theory, 2nd Edition. Cambridge University Press, Cambridge, 1999.

[6] A. Blokhuis, A. R. Calderbank, Quasi-symmetric designs and the Smith normal form, Des. Codes Cryptogr. 2 (1992), 189–206.

[7] R. C. Bose, Symmetric group divisible designs with the dual property, J. Statist. Plann. Inference 1 (1977), 87–101.

[8] R. C. Bose, W. S. Connor, Combinatorial properties of group divisible incomplete block designs, Ann. Math. Statist. 23 (1952), 367–383.

[9] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997), 235–265.

[10] A. E. Brouwer, A. M. Cohen, A. Neumaier, Distance Regular Graphs, Springer-Verlag, New York, 1989.

[11] P. J. Cameron, J. H. van Lint, Designs, Graphs, Codes and their Links, Cambridge University Press, Cambridge, 1991.

[12] D. Crnković, W. Haemers, Walk-regular divisible design graphs, Des. Codes Cryptogr. 72 (2014), 165–175.

[13] D. Crnković, H. Kharaghani, Divisible Design Digraphs, in: C. J. Colbourn (Eds.), Algebraic Design Theory and Hadamard Matrices, Springer Proceedings in Mathematics & Statistics, vol. 133, Springer, Cham, 2015, 43–46.

[14] D. Crnković, N. Mostarac, PD-sets for codes related to flag-transitive symmetric designs, Trans. comb., prihvaćeno za objavljivanje.

[15] D. Crnković, N. Mostarac, S. Rukavina, Self-dual codes from quotient matrices of symmetric divisible designs with the dual property, Discrete Math. 339 (2016), 409–414.

[16] D. Crnković, S. Rukavina, Construction of block designs admitting an Abelian automorphism group, Metrika 62 (2005), 175–183.

[17] D. Crnković, S. Rukavina, Self-dual codes from extended orbit matrices of symmetric designs, Des. Codes Cryptogr. 79 (2016), 113–120.

[18] V. Ćepulić, On symmetric block designs (40, 13, 4) with automorphisms of order 5, Discrete Math. 128 (1994), 45–60.

[19] P. Dankelmann, J. D. Key, B. G. Rodrigues, Codes from incidence matrices of graphs, Des. Codes Cryptogr. 68 (2013), 373–393.

[20] H. Davies, Flag-transitivity and primitivity, Discrete Math. 63 (1987), 91–91.

[21] J. D. Dixon, B. Mortimer, Permutation groups, Springer, New York, 1996.

[22] L. Euler, Solutio problematis ad geometriam situs pertinentis, Commentarii Academiae Scientiarum Imperialis Petropolitanae 8 (1741) 128–140.

[23] The GAP Group, GAP - Groups, Algorithms and Programming, Version 4.4.12, available at `www.gap-system.org`

[24] M. J. E. Golay, Notes on digital coding, In Proceedings of the I. R. E., vol. 37, 657, 1949.

[25] D. M. Gordon, Minimal permutation sets for decoding the binary Golay codes, IEEE Trans. Inform. Theory, 28 (1982), 541–543.

[26] W. H. Haemers, H. Kharaghani, M. A. Meulenberg, Divisible Design Graphs, J. Combin. Theory Ser. A 118 (2011), 978–992.

[27] M. Hall, Jr., Combinatorial Theory (Reprint of the 1986 second edition), John Wiley & Sons, Inc., New York, 1998.

[28] R. W. Hamming, Error detecting and error correcting codes, Bell Syst. Tech. J. 29 (1950), 147–160.

[29] M. Harada, V. D. Tonchev, Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms, Discrete Math. 264 (1-3) (2003) 81–90.

[30] W. C. Huffman, Codes and groups, in: Handbook of Coding Theory, (V. S. Pless, W. C. Huffman, Eds.), Elsevier, Amsterdam, 1998, 1345–1440.

[31] T. W. Hungerford, Algebra, Springer, 1974.

[32] D. Jungnickel, On automorphism groups of divisible designs, Can. J. Math. 34 (1982), 257–297.

[33] W. Kantor, Automorphism Groups of Designs, Math. Z. 109 (1969), 246–252.

[34] J. D. Key, Permutation decoding for codes from designs, finite geometries and graphs, in: D. Crnković and V. Tonchev (Eds.), Information Security, Coding Theory and Related Combinatorics, NATO Science for Peace and Security Series - D: Information and Communication Security 29, IOS Press, Amsterdam, 2011, 172–201.

[35] E. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press, Cambridge, 1983.

[36] S. Lang, Algebra, Revised Third Edition, Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2005.

[37] K. Mackenzie-Fleming, K. W. Smith, $(27, 13, 6)$ designs with an automorphism of order 3, J. Combin. Math. Combin. Comput. 22 (1996), 241–253.

[38] F. J. MacWilliams, Permutation decoding of systematic codes, Bell Syst. Tech. J. 43 (1964), 485–505.

[39] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1998.

[40] R. C. Mullin, H. D. O. F. Gronau, PBDs and GDDs: the basics, in: C. J. Colbourn, J. H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, 185–213.

[41] H. Oral, Self-dual codes and graphs, Doktorski rad, Simon Fraser University, 1989.

[42] E. O'Reilly-Regueiro, Classification of flag-transitive symmetric designs, 6th Czech-Slovak International Symposium on Combinatorics, Graph Theory, Algorithms and Applications, Electron. Notes Discrete Math. 28 (2007), 535–542.

[43] M. Ozeki, Hadamard matrices and doubly even self-dual error correcting codes, J. Combin. Theory Ser. A, 44 (1987), 274–287.

[44] C. E. Praeger, S. Zhou, Imprimitive flag-transitive symmetric designs, J. Combin. Theory Ser. A 113 (2006), 1381–1395.

[45] D. Raghavarao, Constructions and Combinatorial Problems in Design of Experiments, John Wiley, New York, 1971.

[46] J. J. Rotman, An Introduction to the Theory of Groups, Graduate Texts in Mathematics 148, Springer-Verlag, New York, 1995.

[47] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. 27 (1948), 379–423, 623–656.

[48] D. R. Stinson, Combinatorial Designs: Constructions and Analysis, Springer, New York, 2004.

[49] A. P. Street, D. J. Street, Combinatorics of Experimental Design, Clarendon Press, Oxford, 1987.

[50] A. P. Street, D. J. Street, Partially balanced incomplete block designs, in: C. J. Colbourn, J. H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, 419–423.

[51] V. D. Tonchev, Block designs of Hadamard type and self-dual codes, Problemy Peredachi Informatsii 19, No. 4 (1983), 25–30. [Russian] English translation, Problems Inform. Transmission, April (1984) 270–275.

[52] R. M. Wilson, Codes and modules associated with designs and t-uniform hypergraphs, in: D. Crnković, V. D. Tonchev (Eds.), Information Security, Coding Theory and Related Combinatorics, NATO Science for Peace and Security Series-D: Information and Communication Security, vol. 29, IOS, Amsterdam, 2011, 404–436.

Sažetak

Predmet istraživanja ove doktorske disertacije su kodovi konstruirani iz nekih kombinatoričkih dizajna i njihova svojstva. Uvodno, u prvom su poglavlju izloženi pojmovi iz teorije grupa potrebni u nastavku, te osnove teorije kodiranja, grafova i dizajna.

Zatim su u drugom poglavlju disertacije promatrani kodovi razapeti retcima kvocijentne matrice simetričnog (grupovno) djeljivog dizajna (SGDD) s dualnim svojstvom. Definirana je proširena kvocijentna matrica i pokazano je da pod određenim uvjetima retci proširene kvocijentne matrice razapinju samodualan kod u odnosu na određeni skalarni produkt. Također je pokazano da se ponekad lanac kodova može koristiti da pridružimo samodualan kod kvocijentnoj matrici SGDD-a s dualnim svojstvom. Navedeni su rezultati objavljeni u članku [15] čiji su autori Crnković, Mostarac i Rukavina. Tamo su razvijane ideje koje su prezentirali Lander [35] i Wilson [52], te posebno one iz [17], gdje su Crnković i Rukavina dali konstrukciju samodualnih kodova iz proširenih orbitnih matrica simetričnih dizajna. Zatim su opisani i primjeri samodualnih kodova dobivenih opisanom konstrukcijom uz pomoć grafova i digrafova-djeljivih dizajna.

Treće poglavlje sadrži konstrukcije samoortogonalnih i samodualnih kodova iz proširenih orbitnih matrica blokovnih dizajna. U njemu su također opisane i konstrukcije samodualnih kodova uz pomoć orbitnih matrica simetričnih dizajna, te analogne konstrukcije pomoću kvocijentnih matrica SGDD-a s dualnim svojstvom, pri čemu su ideje za njih proizašle iz teorema Assmusa, Mezzarobe i Salwacha u [2]. Kao specijalan slučaj jedne od konstrukcija dana je i konstrukcija uz pomoć Hadamardovih dizajna. Opisano je i kako nam Kroneckerov produkt može pomoći u dobivanju samodualnih kodova.

Četvrto je poglavlje posvećeno pronalaženju PD-skupova iz flag-tranzitivnih simetričnih dizajna. Za prost broj p neka je $C_p(G)$ p-narni kod razapet retcima matrice incidencije G grafa Γ. Neka je Γ incidencijski graf flag-tranzitivnog simetričnog dizajna $\mathcal{D}$. Pokazano je da se bilo koja flag-tranzitivna grupa automorfizama od $\mathcal{D}$ može koristiti kao PD-skup za potpuno ispravljanje pogrešaka za linearan kod $C_p(G)$ (za bilo koji informacijski skup). Dakle, tako dobiveni kodovi mogu se permutacijski dekodirati. Rezultat je poopćen i za kodove iz flag-tranzitivnih SGGD-a s dualnim svojstvom. PD-skupovi dobiveni na opisani način obično su velike kardinalnosti, no proučavanjem primjera kodova proizašlih iz nekih flag-tranzitivnih simetričnih dizajna pokazali smo da se za njih mogu naći manji PD-skupovi za specifične informacijske skupove.

Summary

The main subject of this thesis are codes constructed from certain combinatorial designs and their properties. We have constructed some self-dual codes obtained with the use of symmetric (group) divisible designs with the dual property. Self-dual codes obtained with the use of block designs have also been constructed. Next, we have shown that codes spanned by the rows of the incidence matrix of the incidence graph of a flag-transitive symmetric design, are permutation decodable.

Some necessary concepts from group theory, and also basic concepts from coding theory, graph theory and design theory are introduced in the first chapter.

In the second chapter of the thesis we looked at codes spanned by the rows of a quotient matrix of a symmetric (group) divisible design with the dual property. We defined an extended quotient matrix and showed that under certain conditions the rows of the extended quotient matrix span a self-dual code with respect to a certain scalar product. We also showed that sometimes a chain of codes can be used to associate a self-dual code to a quotient matrix of a symmetric group divisible design with the dual property. This was published in the article [15] whose authors are Crnković, Mostarac and Rukavina. There we developed ideas presented by Lander [35] and Wilson [52], and especially from [17], where Crnković and Rukavina gave a construction of self-dual codes from extended orbit matrices of symmetric designs. Then some examples of self-dual codes are given, that were obtained on the described way, using divisible design graphs and divisible design digraphs.

The next part of the thesis containes constructions of self-orthogonal and self-dual codes from extended orbit matrices of block designs. It also containes constructions of self-dual codes obtained with the use of orbit matrices of symmetric designs, and analog constructions obtained with the use of quotient matrices of symmetric group divisible designs with the dual property, ideas for which were taken from a theorem of Assmus, Mezzaroba and Salwach in [2]. As a special case of one of the constructions we describe a construction from orbit matrices of Hadamard designs. We also remark how Kronecker product of matrices can help to obtain some new self-dual codes from the previously constructed ones.

The last, fourth chapter, is devoted to finding PD-sets from flag-transitive symmetric designs. For any prime p let $C_p(G)$ be the p-ary code spanned by the rows of the incidence

matrix G of a graph Γ. Let Γ be the incidence graph of a flag-transitive symmetric design $\mathcal{D}$. We showed that any flag-transitive automorphism group of $\mathcal{D}$ can be used as a PD-set for full error correction for the linear code $C_p(G)$ (with any information set). Therefor, such codes derived from flag-transitive symmetric designs can be decoded using permutation decoding. We noticed that PD-sets obtained in the described way are usually of large cardinality, but by studying some examples of codes arising from flag-transitive symmetric designs we showed that smaller PD-sets can be found for them for specific information sets. The result is also generalized for codes obtained from flag-transitive symmetric group divisible designs with the dual property.

Životopis

Nina Mostarac rođena je 20. veljače 1987. godine u Rijeci. Tamo je završila Prvu sušačku hrvatsku gimnaziju 2005. godine te preddiplomski studij matematike na Odjelu za matematiku Sveučilišta u Rijeci 2008. godine. Nakon toga upisala je na istom Odjelu diplomski studij matematike - nastavnički smjer te ga završila 2010. godine stekavši naziv magistre edukacije matematike. Te je godine dobila rektorovu nagradu za najboljeg studenta Odjela za matematiku Sveučilišta u Rijeci.

Poslije završenog diplomskog studija upisala je zajednički sveučilišni poslijediplomski doktorski studij matematike Sveučilišta u Osijeku, Rijeci, Splitu i Zagrebu, čiji je nositelj Matematički odsjek Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.

Od rujna 2010. godine radi kao asistent na Odjelu za matematiku Sveučilišta u Rijeci, gdje je članica Zavoda za diskretnu matematiku. Članica je Društva matematičara i fizičara iz Rijeke, Alumni kluba Odjela za Matematiku Sveučilišta u Rijeci te Seminara za konačnu matematiku u Rijeci, u sklopu kojega je održala niz seminara.

U lipnju 2015. sudjelovala je na međunarodnom znanstvenom skupu 2015 PhD Summer School in Discrete Mathematics u Rogli u Sloveniji gdje je održala izlaganje pod nazivom "Self-dual codes from quotient matrices of symmetric divisible designs with the dual property".

Koautorica je u dva znanstvena rada:

- D. Crnković, N. Mostarac, S. Rukavina, Self-dual codes from quotient matrices of symmetric divisible designs with the dual property, Discrete Mathematics 339 (2016), 409–414.
- D. Crnković, N. Mostarac, PD-sets for codes related to flag-transitive symmetric designs, Transactions on Combinatorics, prihvaćeno za objavljivanje.

Udana je i ima dvoje djece.