Samoortogonalni i LCD kodovi konstruirani iz slabo samoortogonalnih dizajna

Traunkar, Ivona

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ivona Traunkar

Samoortogonalni i LCD kodovi konstruirani iz slabo samoortogonalnih dizajna

DOKTORSKI RAD

Zagreb, 2021.

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ivona Traunkar

Samoortogonalni i LCD kodovi konstruirani iz slabo samoortogonalnih dizajna

DOKTORSKI RAD

Mentor:

dr. sc. Vedrana Mikulić Crnković

Zagreb, 2021.

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Ivona Traunkar

Self-orthogonal and LCD codes obtained from weakly self-orthogonal designs

DOCTORAL DISSERTATION

Supervisor:

dr. sc. Vedrana Mikulić Crnković

Zagreb, 2021.

ZAHVALA

Prije svega, iskreno i ogromno hvala mojoj mentorici, dr. sc. Vedrani Mikulić Crnković na vođenju, pomoći, sugestijama i uputama tijekom cijelog mog doktorskog studija, znanstvenog istraživanja i u konačnici tijekom pisanja ove doktorske disertacije. Tijekom cijelog mog studija bila je mnogo više od samo mentorice i bez njene podrške, motivacije, kritike i vođenja cijeli ovaj proces bio bi puno teži i u svakom slučaju puno manje zabavan. Nisam mogla ni zamisliti boljeg i predanijeg mentora, u svakom segmentu.

Hvala članovima Seminara za konačnu matematiku u Rijeci na strpljenju i slušanju mojih izlaganja koja su vodila ka pisanju ove disertacije. Hvala i svim članovima povjerenstva na vremenu i trudu koji su uložili u čitanje ovog rada, kao i na upućenim sugestijama kako bi ova disertacija bila što kvalitetnija.

Veliko hvala i mojoj obitelji i prijateljima koji su bili uz mene i pružali mi podršku na svakom koraku mog puta. Sanjine, hvala ti na ogromnom angažmanu i odricanju posljednjih par mjeseci, što si bio tu uz moje nervozne trenutke i što si me ohrabrivao i gurao dalje. Bez tvoj potpore i brige sve ovo bilo bi mnogo stresnije!

SAŽETAK

Predmet istraživanja doktorske disertacije su samoortogonalni i LCD kodovi konstruirani iz slabo p-samoortogonalnih 1-dizajna.

U prvom dijelu disertacije uvest će se osnovni pojmovi i tvrdnje teorije grupa, teorije dizajna, teorije grafova i teorije kodiranja. U drugom dijelu disertacije opisat će se postojeće metode dobivanja binarnih samoortogonalnih kodova iz slabo samoortogonalnih 1-dizajna proširivanjem matrice incidencije, orbitne matrice dizajna i podmatrica orbitnih matrica te će se postojeće metode proširiti i generalizirati. Uvest će se metode konstrukcije samoortogonalnih kodova iz slabo p-samoortogonalnih dizajna nad proizvoljnim konačnim poljem.

U trećem dijelu disertacije uvest će se konstrukcija LCD kodova nad proizvoljnim konačnim poljem iz slabo p-samoortogonalnih 1-dizajna, bazirana na proširenju incidencijske matrice, orbitne matrice dizajna i podmatrica orbitnih matrica dizajna. Dodatno, analizirat će se pod kojim uvjetima će proširenje matrice incidencije t-dizajna i matrice susjedstva jako regularnog grafa generirati LCD kod.

U zadnjem poglavlju razvijene metode potkrijepit će se konkretnim primjerima i djelomičnim klasifikacijama te će se opisati i analizirati svojstva dobivenih samoortogonalnih kodova. Priložit će se primjeri konkretnih samoortogonalnih i LCD kodova i djelomične klasifikacije te će se opisati i analizirati njihova svojstva. Za sve navedene konstrukcije koristit će se programski paket GAP ([28]) i njegov paket DESIGN ([41]) te programski paket Magma ([6]).

SUMMARY

The main subject of the thesis are self-orthogonal and LCD codes constructed from weakly self-orthogonal 1-designs.

First part of dissertation will be introduction to group theory, design theory, graph theory, and coding theory. In the second part, we will describe known methods of construction binary self-orthogonal codes from weakly self-orthogonal 1-designs obtained by using extended incidence matrix, orbit matrices, and submatrices of orbit matrices of a design as a generator matrix of a code. Known methods will be extended and generalized in order to obtain self-orthogonal codes over arbitrary finite field. We will describe methods of construction of self-orthogonal codes from weakly p-self-orthogonal designs.

In the third part of dissertation we will develop a method of construction of LCD codes from weakly p-self-orthogonal 1-designs, using suitable extension of incidence matrix, orbit matrix and submatrices of orbit matrices of 1-designs as generator matrix of a code. Additionally, we will analyse under which conditions the extension of incidence matrix of t-design and adjacency matrix of a strongly regular graph generates an LCD code.

In the last part, we will provide examples and partial classification of self-orthogonal and LCD codes constructed using described methods. We will analyse properties of constructed codes using the computational algebra system GAP ([28]) and it's package DESIGN ([41]) and computational algebra system Magma ([6]).

SADRŽAJ

UVOD

Teorija kodiranja je grana diskretne matematike koja se bavi problemom prijenosa informacija od pošiljatelja do primatelja putem komunikacijskog kanala sa smetnjama te detekcijom i ispravljanjem pogrešaka nastalih prilikom prijenosa. Temelje teorije kodiranja postavio je C. E. Shannon 1948. godine u [39] gdje navodi izraz za kapacitet komunikacijskog kanala, poznat i kao Shannonova granica. Intenzivnijim razvojem računalne tehnologije došlo je do razvoja teorije kodiranja te povećane potrebe za konstrukcijom kodova s dobrim svojstvima te je omogućen razvoj i implementacija algoritama za konstrukciju kodova. Posebni interes privukli su linearni kodovi. Zbog njihove algebarske strukture, lako ih je opisati te je proces kodiranja i dekodiranja lakši u odnosu na nelinearne kodove. Važna klasa linearnih kodova su samoortogonalni kodovi i njihova podklasa samodualni kodovi ([46]). Obzirom da su mnogi poznati dobri kodovi samodualni, aktivno se radi na razvoju metoda konstrukcije samodualnih kodova i na klasifikaciji samodualnih kodova za danu duljinu i dimenziju. Poznata je veza samoortogonalnih i samodualnih kodova s drugim kombinatornim strukturama, npr. s blokovnim dizajnima. Konstrukcija kodova iz blokovnih dizajna ([1], [2], [44]) i orbitnih matrica ([18], [19], [20], [22], [23], [33]) jako su proučavana tema. U [43] Tonchev je dao metodu proširenja incidencijskih matrica blokovnih dizajna kako bi se dobila generirajuća matrica samoortogonalnog koda. U [17] autori daju proširenja orbitnih matrica slabo samoortogonalnih 1-dizajna kako bi konstruirali binarne samoortogonalne kodove na koje jednostavna Heldova grupa djeluje kao grupa automorfizama. U [21] autori konstruiraju samodualne kodove nad proizvoljnim konačnim poljem proširivanjem matrica incidencije i orbitnih matrica blokovnih dizajna. U [15] su autori pokazali da je svaki G-inavrijantan binarni samoortogonalan kod sadržan u dualnom kodu koda razapetog skupom fiksnih točaka involucija od G i daju klasifikaciju svih binarnih samodualnih kodova na koje grupa M_{11} djeluje kao grupa automorfizama.

LCD kodovi (linearni kodovi s komplementarnim dualom) su relativno nova klasa linearnih kodova. Uveo ih je Massey 1992. godine u [37] i od tada su izazvali veliki interes te

imaju široku primjenu u komunikacijskim sustavima, sustavima za pohranu podataka, elektronici, kriptografiji... Massey je predstavio LCD kodove kao optimalno rješenje za kodiranje kroz BAC (binary adder channel) kanal s dva korisnika. U [13] Carlet i Guilley su proučavali primjenu LCD kodova u kriptografiji prilikom SCA (side-channel attack) napada i FIA (fault injection attack) napada. Također, razvili su nekoliko konstrukcija LCD kodova i pokazali da se svaki nebinaran LCD kod u polju karakteristike 2 može transformirati u binaran LCD kod koristeći odgovarajuće proširenje. Yang i Massey su u [45] dali nužne i dovoljne uvjete da bi ciklički kod imao komplementarni dualni kod. U [24] Ding, Li i Li konstruirali su nekoliko familija cikličkih LCD kodova nad konačnim poljima i analizirali njihove parametre. Dougherty, Kim, Ozkaya, Sok i Solé su u [26] konstruirali binarne LCD kodove koristeći samodualne kodove, ortogonalne matrice i blokovne dizajne. Također, pokazali su da se iz jednog samodualnog koda, odnosno iz jedne ortogonalne matrice, može dobiti više LCD kodova. Carlet, Mesnager, Tang i Qi su u [14] prikazali općenitu konstrukciju LCD kodova iz linearnih kodova i pokazali da je svaki linearni kod nad $\mathbb{F}_q$ $(q > 3)$ ekvivalentan nekom euklidskom LCD kodu i svaki linearni kod nad $\mathbb{F}_{q^2}$ $(q > 2)$ ekvivalentan nekom hermitskom LCD kodu. Za $q < 3$ i za neke vrijednosti n i k ne postoji optimalan linearan $[n,k]$ LCD kod. Granice za minimalnu udaljenost binarnih i ternarnih LCD kodova mogu biti više ograničavajuće nego za linearne kodove općenito, obzirom da LCD kodovi zadovoljavaju dodatna ograničenja. Nedavno je u [8] autorica proširila klasifikaciju optimalnih binarnih LCD kodova, do duljine 40. U radu [16] Crnković, Egan, Rodrigues i Švob konstruirali su LCD kodove iz težinskih matrica, uključujući Paleyeve konferencijske matrice i Hadamardove matrice, a zatim su konstrukciju proširili za dobivanje hermitskih LCD kodova nad poljem $\mathbb{F}_4$.

Cilj je generalizacija postojećih metoda konstrukcije samoortogonalnih i LCD kodova koristeći odgovarajuća proširenja matrice incidencije, orbitnih matrica i podmatrica orbitnih matrica slabo samoortogonalnih 1-dizajna. U poglavlju 2 generalizirane su metode konstrukcije binarnih samoortogonalnih kodova navedene u [17] i [43] te su dane konstrukcije samoortogonalnih kodova nad proizvoljnim konačnim poljem koristeći matrice incidencije, orbitne matrice i podmatrice orbitnih matrica slabo p-samoortogonalnih dizajna. U poglavlju 3 uvdene metode konstrukcije su modificirane kako bi se konstruirali LCD kodovi koristeći proširenja matrice incidencije, orbitnih matrica i podmatrica orbitnih matrica slabo p-samoortogonalnih dizajna. Uvedene metode modificirane su korištenjem proširenja istog tipa kao u metodama iz poglavlja 2.

Metode konstrukcije uvedene u poglavljima 2 i 3 potkrijepljene su konkretnim primjerima i djelomičnim klasifikacijama samoortogonalnih i LCD kodova, opisanim u poglavlju 4.

1. OSNOVNI POJMOVI

U ovom poglavlju uvest ćemo uvodne pojmove teorije grupa i konačnih polja, teorije dizajna, teorije grafova i teorije kodova potrebne za razumijevanje disertacije. Pritom pretpostavljamo da je čitatelj upoznat s osnovama linearne algebre, temeljnim pojmovima grupa i polja, kao i s osnovama kombinatorike.

1.1. OSNOVNI POJMOVI TEORIJE GRUPA I KONAČNIH POLJA

Grupa je osnovna algebarska struktura. Teorija grupa ima primjenu u različitim područjima matematike, kao na primjer u geometriji, diferencijalnoj geometriji, teoriji reprezentacija, algebarskoj topologiji i sl., pa tako i u teoriji dizajna i teoriji grafova. Pretpostavljamo da je čitatelj upoznat s definicijom grupe te osnovnim pojmovima i tvrdnjama teorije grupa, kao npr. red grupe G (oznaka $|G|$), podgrupa grupe, normalna podgrupa, indeks podgrupe u grupi (oznaka $[G:H]$), puna grupa automorfizama, kao i s definicijom i osnovnim svojstvima sljedećih grupa: ciklička grupa reda n (oznaka Z_n), simetrična grupa stupnja n (oznaka S_n), alternirajuća grupa stupnja n (oznaka A_n).

Definicija 1.1.1. Neka su G_1 i G_2 grupe. **Direktni produkt** grupa G_1 i G_2, u oznaci $G_1 \times G_2$, je skup $G = \{(g_1, g_2) \mid g_1, g_2 \in G\}$ uz operaciju $(g_1, g_2) \circ (g_1', g_2') = (g_1 g_1', g_2 g_2')$.

Lako se pokaže da je $(G, \circ)$ grupa reda $|G_1| \cdot |G_2|$. Pojam direktnog produkta grupa možemo poopćiti na sljedeći način.

Neka su G i H grupe i $f : H \to \mathrm{Aut}G$, gdje je $\mathrm{Aut}G$ puna grupa automorfizama grupe G, homomorfizam. Na skupu $G \times H = \{(g,h) \mid g \in G, h \in H\}$ definiramo operaciju

$$(g,h)(g',h') = (gf(h)(g')), hh').$$

Skup $G \times H$ uz tako definiranu operaciju je grupa.

Definicija 1.1.2. Kartezijev produkt grupa G i H uz gore definiranu operaciju naziva se **semidirektni produkt** grupa G i H, uz oznaku $G : H$.

Napomena. Ako je $f : H \to \mathrm{Aut}G$ trivijalni homomorfizam, semidirektni produkt grupa G i H je direktni produkt grupa G i H.

Definicija 1.1.3. Grupa G je izomorfna **proširenju grupe** H grupom K, uz oznaku $H.K$, ako postoji normalna podgrupa H' u G takva da je $H' \cong H$ i $G/H' \cong K$.

Napomena. Neka je $G \cong H.K$ i $H' \trianglelefteq G$ takva da je $H' \cong H$ te neka postoji $K' \leq G$ takva da je $K' \cong K$, $K'H' = \{kh \mid k \in K', h \in H'\} = G$ i $K' \cap H' = \{e\}$. Tada je $G \cong H : K$. Ako je K' normalna podgrupa u G, onda je $G \cong H \times K$.

Definicija 1.1.4. Abelova grupa G reda n u kojoj su svi elementi osim neutrala reda p, gdje je p prost broj, naziva se **elementarno Abelova grupa**.

Može se pokazati da je svaka elementarno Abelova grupa direktni produkt cikličkih grupa reda p, gdje je p prost broj. Elementarno Abelovu grupu koja je direktni produkt α cikličkih grupa reda p označavat ćemo E_{p^α}.

Definicija 1.1.5. Neka je G grupa i Ω neprazan skup. Grupa G djeluje na skup Ω ako postoji preslikavanje $f : G \times \Omega \to \Omega$ takvo da vrijedi

1. $f(e,x) = x, \forall x \in \Omega$,
2. $f(g_1, f(g_2,x)) = f(g_1 g_2, x), \forall x \in \Omega, \forall g_1, g_2 \in G$.

Sliku djelovanja elementa $g \in G$ na element $x \in \Omega$ označavat ćemo sa $g.x$.

Definicija 1.1.6. Skup $G_x = \{g \in G \mid g.x = x\}$ naziva se **stabilizator** elementa x za djelovanje grupe G.

Stabilizator G_x je podgrupa grupe G.

Definicija 1.1.7. Skup $G.x = \{g.x \mid g \in G\}$ naziva se **orbita** elementa x za djelovanje grupe G.

Definicija 1.1.8. G djeluje **tranzitivno** na skup Ω ako postoji element $x \in \Omega$ takav da je $G.x = \Omega$.

Drugim riječima, djelovanje je tranzitivno ako za svaka dva elementa $x, y \in \Omega$ postoji element $g \in G$ takav da je $g.x = y$, tj. postoji samo jedna orbita za djelovanje grupe G na skup Ω.

Definicija 1.1.9. Grupa G djeluje **poluregularno** na skup Ω ako su stabilizatori svih elemenata trivijalne grupe. Grupa G djeluje **regularno** na skup Ω ako G djeluje na Ω tranzitivno i poluregularno.

Dokaz sljedećeg teorema može se pronaći u [11].

Teorem 1.1.10. Neka grupa G djeluje na skup Ω. Tada je $F : G \to S(\Omega)$ preslikavanje koje svakom elementu $g \in G$ pridružuje bijekciju $f_g : \Omega \to \Omega$, $f_g(x) = g.x$, homomorfizam grupa (induciran djelovanjem grupe G na Ω). Obrnuto, ako postoji homomorfizam $F : G \to S(\Omega)$, onda grupa G djeluje na skup Ω.

Definicija 1.1.11. Homomorfizam $F : G \to S(\Omega)$ naziva se **permutacijska reprezentacija** grupe G.

Definicija 1.1.12. Grupa G djeluje **vjerno** na skup Ω, tj. $F : G \to S(\Omega)$ je vjerna permutacijska reprezentacija ako je F monomorfizam.

Teorem 1.1.13 (Cayley)**.** Svaka grupa je izomorfna permutacijskoj grupi. Specijalno, ako je G konačna grupa reda n, onda je G izomorfna nekoj podgrupi simetrične grupe S_n.

Definicija 1.1.14. Neka grupa G_1 djeluje vjerno na skup X_1 i neka grupa G_2 djeluje vjerno na skup X_2. Grupe G_1 i G_2 su **permutacijski izomorfne** ako postoje izomorfizam grupa $\phi : G_1 \to G_2$ i bijekcija skupova $\psi : X_1 \to X_2$ takvi da za svaki $g \in G_1$ sljedeći dijagram komutira.

$$\begin{array}{ccc} X_1 & \xrightarrow{\psi} & X_2 \\ \downarrow f_g & & \downarrow f_{\phi(g)} \\ X_1 & \xrightarrow{\psi} & X_2 \end{array},$$

gdje je $f_g(x) = g.x$.

Ako je u gornjoj definiciji $G_1 = G_2$, za opisana djelovanja kažemo da su **ekvivalentna**.

Ako su grupe permutacijski izomorfne, onda su one i izomorfne. No, obrat ne mora vrijediti.

Primjer 1.1.1. Neka je $X = X_1 = X_2 = \{1,2,3,4,5,6\}$ te neka su $G_1 = \langle (1,2,3,4,5,6) \rangle$ i $G_2 = \langle (1,2,3)(4,5) \rangle$. Grupe G_1 i G_2 su generirane elementima reda 6 pa su izomorfne cikličkoj grupi reda 6 i postoji izomorfizam $\phi : G_1 \to G_2$. U grupi G_1 ne postoji niti jedna netrivijalna permutacija koja fiksira element 6, dok u grupi G_2 svaka permutacija fiksira element

6. Pretpostavimo da su G_1 i G_2 permutacijski izomorfne. Tada je $f_g(\psi(6)) = \psi(f_{\phi(g)}(6))$, tj. $f_g(6) = f_{\phi(g)}(6)$. Obzirom da je $f_g(6) \neq 6$ i $f_{\phi(g)}(6) = 6, \forall g \in G_1, g \neq 1$, zaključujemo da postoji $g \in G_1$ takav da je $f_g(6) \neq f_{\phi(g)}(6)$ pa G_1 i G_2 nisu permutacijski izomorfne grupe.

Napomena 1.1.15. Neka je G konačna grupa i $H \leq G$. Promotrimo skup lijevih suskupova podgrupe H u G, tj. skup $\Gamma_H = \{aH \mid a \in G\}$. G djeluje tranzitivno na skup Γ_H lijevim množenjem: $g.(aH) = gaH$ i to djelovanje inducira permutacijsku reprezentaciju grupe G na $|\Gamma_H| = [G : H]$ točaka. Uočimo da je $G_H = H$.

Sljedeća lema omogućava da opišemo sve tranzitivne permutacijske reprezentacije grupe G, do na ekvivalenciju. Dokaz sljedeće leme može se pronaći u [25].

Lema 1.1.16. Neka grupa G djeluje tranzitivno na skupove Ω i Γ te neka je H stabilizator elementa skupa Ω za djelovanje grupe G. Dva su djelovanja ekvivalentna ako i samo ako postoji element skupa Γ čiji stabilizator je jednak H.

Djelovanje grupe na skup Ω možemo poširiti na djelovanje grupe G na skup podskupova od Ω na sljedeći način:

$$g.\Delta = \{g.s \mid s \in \Delta\},\ \Delta \subseteq \Omega, g \in G.$$

Stabilizator skupa Δ je $G_\Delta = \{g \in G \mid g.\Delta = \Delta\}$.

Definicija 1.1.17. Neka grupa G djeluje tranzitivno na skup Ω i neka je $\Delta \subseteq \Omega$. Ako za svaki $g \in G$ vrijedi $g.\Delta = \Delta$ ili $g.\Delta \cap \Delta = \emptyset$, skup Δ nazivamo **blok**.

Neka grupa G djeluje tranzitivno na skup Ω. Tada su Ω i $\{x\} \subseteq \Omega$ blokovi za svaki $x \in \Omega$. Opisani blokovi nazivaju se **trivijalni blokovi**. Svi ostali blokovi su netrivijalni. Dokaz sljedeće propozicije može se pronaći u [25].

Propozicija 1.1.18. Neka grupa G djeluje tranzitivno na skup Ω i neka je $\Delta \subseteq \Omega$ netrivijalan blok. Neka je $x \in \Delta$. Tada je $G_x \leq G_\Delta \leq G$.

Definicija 1.1.19. Ako grupa G djeluje tranzitivno na skup Ω tako da ne postoje netrivijalni blokovi, kažemo da je G djeluje **primitivno** na skup Ω i da je G primitivna grupa.

Dokaz sljedeće propoziije može se pronaći u [25].

Propozicija 1.1.20. Neka grupa G djeluje tranzitivno na skup Ω. Djelovanje grupe G na skup Ω je primitivno ako i samo ako je G_x maksimalna podgrupa grupe G, za svaki $x \in \Omega$.

1.1.1. Jednostavne grupe

Podsjetimo se, grupa G je jednostavna ako nema netrivijalnih normalnih podgrupa. Jednostavne grupe imaju važnu ulogu u proučavanju konačnih grupa (Jordan-Hölderov teorem, [35]). Jedine jednostavne komutativne grupe su cikličke grupe $\mathbb{Z}_p$, gdje je p prost broj. Klasifikacija nekomutativnih jednostavnih grupa predstavljala je veliki problem u 19. i 20. stoljeću. Prva otkrivena nekomutativna jednostavna grupa je alternirajuća grupa A_5. Da je grupa A_5 jednostavna dokazao je Gauss, a kasnije je dokazano i da je alternirajuća grupa A_n jednostavna ako i samo ako je $n \geq 5$.

Nekomutativne jednostavne grupe dijele se na klasične i sporadične. Klasične jednostavne grupe su one koje pripadaju beskonačnim familijama konačnih alternirajućih grupa i grupa Liejevog tipa. U grupe Liejevog tipa spadaju familije projektivnih linearnih, projektivnih ortogonalnih, projektivnih unitarnih i projektivnih simplektičkih grupa. Osim klasičnih jednostavnih grupa, postoji još 26 sporadičnih jednostavnih grupa koje ne pripadaju niti jednoj gore navedenoj familiji. Prvih 5 sporadičnih grupa konstruirao je E. Mathieu u 19. stoljeću. Smatralo se da su to jedine sporadične jednostavne grupe sve do 1964. godine, kada je Zvonimir Janko konstruirao prvu sljedeću sporadičnu jednostavnu grupu. Do 1975. godine pronađeno ih je još 20.

Opća i specijalna linearna grupa

Neka je V vektorski prostor dimenzije n nad konačnim poljem $\mathbb{F}_q$, $q = p^k$, gdje je p prost broj, uz oznaku $V(n,q)$. Vektorski prostor $V(n,q)$ sadrži q^n elemenata.

Skup svih automorfizama vektorskog prostora čini grupu uz operaciju kompozicije funkcija. Svakom automorfizmu prostora $V(n,q)$ jednoznačno je pridružena regularna kvadratna matrica reda n nad poljem $\mathbb{F}_q$.

Definicija 1.1.21. **Opća linearna grupa**, u oznaci $GL(n,q)$, je skup svih regularnih kvadratnih matrica reda n nad poljem $\mathbb{F}_q$ uz operaciju množenja matrica.

Red grupe $GL(n,q)$ jednak je broju uređenih n-torki linearno nezavisnih vektora prostora $V(n,q)$, tj.

$$|GL(n,q)| = (q^n - q^{n-1})(q^n - q^{n-2}) \cdot \ldots \cdot (q^n - 1) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1).$$

Skup svih matrica iz grupe $GL(n,q)$ čije determinante su jednake 1 je grupa i naziva se **specijalna linearna grupa**, u oznaci $SL(n,q)$. $SL(n,q)$ je normalna podgrupa grupe $GL(n,q)$ indeksa $q-1$ čiji red je

$$|SL(n,q)| = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1).$$

Kvocijentna grupa opće linearne grupe po svom centru $GL(n,q)/Z(GL(n,q))$ naziva se **projektivna opća linearna grupa**, u oznaci $PGL(n,q)$. Grupa $PGL(n,q)$ je reda

$$|PGL(n,q)| = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1).$$

Kvocijentna grupa specijalne linearne grupe po svom centru $SL(n,q)/Z(SL(n,q))$ naziva se **linearna grupa**, u oznaci $L(n,q)$. Grupa $L(n,q)$ je reda

$$L(n,q) = \frac{1}{M(q-1,n)} q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1).$$

Linearna grupa je jednostavna, osim u slučajevima $(p,q) = (2,2)$ i $(p,q) = (2,3)$ ([4]).

Polulinearne grupe

Neka je $V(n,q)$ vektorski prostor nad poljem $\mathbb{F}_q$. Preslikavanje $f : V(n,q) \to V(n,q)$ je **polulinearno preslikavanje** ako vrijedi:

1. $f(u+v) = f(u) + f(v),\ \forall u,v \in V(n,q)$,
2. $f(ku) = \alpha(k) f(u),\ \forall u \in V(n,q),\ \forall k \in \mathbb{F}_q$, gdje je α automorfizam polja $\mathbb{F}_q$.

Skup svih bijektivnih polulinearnih preslikavanja vektorskog prostora $V(n,q)$ čini grupu, uz operaciju kompozicije funkcija. Ta grupa se naziva **polulinearna grupa**, u oznaci $\Gamma L(n,q)$. Uočimo da ako je automorfizam iz svojstva 2. trivijalan, f je automorfizam vektorskog prostora pa zaključujemo da $\Gamma L(n,q)$ sadrži sve automorfizme vektorskog prostora $V(n,q)$, tj. grupa $GL(n,q)$ je podgrupa grupe $\Gamma L(n,q)$ indeksa $|Aut(\mathbb{F}_q)|$.

Kvocijentna grupa polulinearne grupe po centru opće linearne grupe naziva se **projektivna polulinearna grupa**, u oznaci $P\Gamma L(n,q)$.

Projektivna geometrija $PG(n-1,q)$

Neka je na $V^*(n,q) = V(n,q)\backslash\{0\}$ definirana relacija: $x \sim y$ ako i samo ako postoji $\lambda \in \mathbb{F}_q$ takav da je $y = \lambda x$. Relacija $\sim$ je relacija ekvivalencije i klase ekvivalencije te relacije su točke

projektivne geometrije $PG(V(n,q))$. Klasu ekvivalencije elementa x za navedenu relaciju označavat ćemo s $[x]$. Prostor $[U]$ projektivne geometrije $PG(V(n,q))$ je slika potprostora U vektorskog prostora $V(n,q)$ obzirom na preslikavanje $g : V(n,q) \to PG(V(n,q)),\ g(x) = [x]$. Ako je U prostor dimenzije k u vektorskom prostoru $V(n,q)$, onda kažemo da je $[U]$ potprostor dimenzije $k-1$ u projektivnoj geometriji $PG(V(n,q))$. Vidimo da je sama projektivna geometrija dimenzije $n-1$ pa koristimo oznaku $PG(n-1,q)$. Projektivna geometrija $PG(n-1,q)$ sadrži $\frac{q^n-1}{q-1}$ točaka ([4]).

Definicija 1.1.22. Preslikavanje $f : PG(n-1,q) \to PG(n-1,q)$ za koje vrijedi

$$U \subseteq U' \Leftrightarrow f(U) \subseteq f(U'),\ \forall U, U' \subseteq PG(n-1,q)$$

naziva se **kolineacija** ili **automorfizam** projektivne geometrije $PG(n-1,q)$.

Definicija 1.1.23. Preslikavanje $f : PG(n-1,q) \to PG(n-1,q)$ za koje vrijedi

$$U \subseteq U' \Leftrightarrow f(U') \subseteq f(U),\ \forall U, U' \subseteq PG(n-1,q)$$

naziva se **korelacija** projektivne geometrije $PG(n-1,q)$.

Dokaz sljedećeg teorema može se pronaći u [1].

Teorem 1.1.24 (Fundamentalni teorem projektivne geometrije)**.** Neka je V vektorski prostor dimenzije veće ili jednake 3. Tada je puna grupa automorfizama projektivne geometrije $PG(V)$ izomorfna projektivnoj polulinearnoj grupi $P\Gamma L(V)$.

Bilinearne forme i jednostavne grupe

Neka je $V(n,q)$ vektorski prostor nad poljem $\mathbb{F}_q$. Preslikavanje $f : V(n,q) \times V(n,q) \to \mathbb{F}_q$ je **bilinearna forma** ako vrijedi:

1. $f(\alpha u, v) = f(u, \alpha v) = \alpha f(u,v),\ \forall u, v \in V(n,q),\ \forall \alpha \in \mathbb{F}_q$,
2. $f(u_1 + u_2, v) = f(u_1, v) + f(u_2, v),\ \forall u_1, u_2, v \in V(n,q)$,
3. $f(u, v_1 + v_2) = f(u, v_1) + f(u, v_2),\ \forall u, v_1, v_2 \in V(n,q)$.

Bilinearna forma f je **simetrična** ako za svaka dva elementa $u, v \in V(n,q)$ vrijedi $f(u,v) = f(v,u)$. **Alternirajuća** bilinearna forma je bilinearna forma f takva da je $f(u,u) = 0,\ \forall u \in V(n,q)$.

Preslikavanje $f : V(n,q) \times V(n,q) \to \mathbb{F}_q$ je **seskvilinearna forma** ako vrijedi:

1. $f(\alpha u, v) = \alpha f(u,v),\ \forall u,v \in V(n,q),\ \forall \alpha \in \mathbb{F}_q$,
2. $f(u, \alpha v) = \overline{\alpha} f(u,v),\ \forall u,v \in V(n,q),\ \forall \alpha \in \mathbb{F}_q$, gdje je preslikavanje $\alpha \to \overline{\alpha}$ automorfizam polja $\mathbb{F}_q$ reda 2,
3. $f(u_1 + u_2, v) = f(u_1,v) + f(u_2,v),\ \forall u_1,u_2,v \in V(n,q)$,
4. $f(u, v_1 + v_2) = f(u,v_1) + f(u,v_2),\ \forall u,v_1,v_2 \in V(n,q)$.

Hermitska forma je seskvilinearna forma f za koju vrijedi $f(v,u) = \overline{f(u,v)}$, gdje je preslikavanje $\alpha \to \overline{\alpha}$ automorfizam polja $\mathbb{F}_q$ reda dva.
Forma $f : V(n,q) \times V(n,q) \to \mathbb{F}_q$ je **nedegenerirana** ako vrijedi

$$f(u,v) = 0,\ \forall v \in V(n,q) \Rightarrow u = 0.$$

Neka je f forma (bilinearna ili seskvilinearna) na vektorskom prostoru $V(n,q)$ i neka je U potprostor vektorskog prostora $V(n,q)$. Tada je skup

$$U^{\perp} = \{u \in V(n,q) \mid f(u,v) = 0,\ \forall v \in U\}$$

potprostor vektorskog prostora $V(n,q)$.

Ako je f nedegenerirana forma, onda preslikavanje $o : V(n,q) \to V(n,q),\ o(U) = U^{\perp}$ inducira permutaciju skupa potprostora vektorskog prostora $V(n,q)$ te je

$$U \subseteq U' \Rightarrow o(U') \subseteq o(U).$$

Kompozicija preslikavanja $g : V(n,q) \to PG(n-1,q),\ g(x) = [x]$, i preslikavanja o je korelacija projektivne geometrije $PG(n-1,q)$. Ako je o^2 identično preslikavanje, onda se korelacija naziva **polaritet** projektivne geometrije $PG(n-1,q)$.

Forma $f : V(n,q) \times V(n,q) \to \mathbb{F}_q$ dopušta polaritet ako i samo ako vrijedi

$$f(u,v) = 0 \Leftrightarrow f(v,u) = 0.$$

Simetrična, alternirajuća i hermitska forma zadovoljavaju navedeni uvjet. Može se pokazati da su to ujedno i jedine forme koje dopuštaju polaritet. S obzirom na to, razlikujemo ortogonalni, simplektički i unitarni polaritet.

Definicija 1.1.25. Neka je f bilinearna/seskvilinearna forma i neka je A automorfizam vektorskog prostora $V(n,q)$. A je automorfizam bilinearne/seskvilinearne forme ako je $f(Au,Av) = f(u,v),\ \forall u,v \in V(n,q)$.

Skup svih automorfizama forme čini grupu, uz operaciju kompozicije funkcija.

Neka je a simetrična forma vektorskog prostora $V(n,q)$. Kvocijentna grupa grupe automorfizama forme a po svom centru naziva se **ortogonalna grupa**, u oznaci $O(n,q)$. Za $n = 2m+1$ neparan broj, ortogonalna grupa $O(2m+1,q)$ je reda

$$|O(2m+1,q)| = \frac{1}{M(q-1,2)} q^{m^2} \prod_{i=1}^{m} (q^{2i}-1)$$

i ona je jednostavna za $m \geq 2$. Za $n = 2m$ paran broj postoje dvije ortogonalne grupe $O^+(2m,q)$ i $O^-(2m,q)$ čiji redovi su

$$|O^+(2m,q)| = \frac{1}{M(q^m-1,4)} q^{m(m-1)} (q^m-1) \prod_{i=1}^{m-1} (q^{2i}-1)$$

i

$$|O^-(2m,q)| = \frac{1}{M(q^m+1,4)} q^{m(m-1)} (q^m+1) \prod_{i=1}^{m-1} (q^{2i}-1).$$

Grupe $O^+(2m,q)$ i $O^-(2m,q)$ su jednostavne za $m \geq 4$.

Simplektička grupa, u oznaci $S(n,q)$, za $n = 2m$ paran broj, je kvocijentna grupa grupe automorfizama alternirajuće bilinearne forme po svom centru. Red grupe $S(2m,q)$ je

$$|S(2m,q)| = \frac{1}{M(q-1,2)} q^{m^2} \prod_{i=1}^{m} (q^{2i}-1).$$

Grupa $S(2m,q)$ je jednostavna za $m \geq 2$, osim grupe $S(4,2)$ koja je izomorfna grupi S_6.

Neka je $V(n,p^2)$ vektorski prostor i neka je G grupa svih automorfizama hermitske forme na $V(n,p^2)$ koji su sadržani u grupi $SL(n,p^2)$. Kvocijentna grupa grupe G po svom centru naziva se **unitarna grupa**, u oznaci $U(n,p)$. Red unitarne grupe je

$$|U(n,p)| = \frac{1}{M(p+1,n)} p^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (p^i - (-1)^i)$$

i ona je jednostavna za $n \geq 3$, osim u slučaju grupe $U(3,2)$ ([4]).

1.1.2. Konačna polja

Pretpostavljamo da je čitatelj upoznat s definicijom polja te osnovnim pojmovima i tvrdnjama teorije polja, kao npr. polje ostataka modulo p, gdje je p prost broj (oznaka $\mathbb{Z}_p$), prsten polinoma $\mathbb{Z}_p[x]$, proširenja polja. Prisjetit ćemo se osnovnih tvrdnji vezanih uz konačna polja.

Neka je p prost broj i neka je n prirodan broj. Tada postoji jedinstveno (do na izomorfizam) konačno polje reda $q = p^n$. Neka je $\mathbb{F}_p = \mathbb{Z}_p$ konačno polje reda p i $\mathbb{F}_q$ konačno polje reda

$q = p^n$. Polje $\mathbb{F}_q$ može se realizirati kao proširenje polja $\mathbb{F}_p$ ireducibilnim polinomom $f(x)$ stupnja n nad $\mathbb{F}_p$. Tada su elementi polja $\mathbb{F}_q$ polinomi stupnja manjeg ili jednakog $n-1$ s koeficijentima iz $\mathbb{Z}_p$ (takvih polinoma ima p^n), dok su operacije zbrajanje i množenje polinoma u $\mathbb{Z}_p[x]$, s time da se nakon množenja računa ostatak pri dijeljenju s polinomom $f(x)$.

Definicija 1.1.26. Neka je p prost broj, n prirodan broj i neka je $q = p^n$. Za cjelobrojnu matricu $A = [a_{ij}]$ definiramo matricu $A_p = [a'_{ij}]$, gdje je $a'_{ij} \equiv a_{ij} \pmod{p}$. Uočimo da je matrica A_p matrica s elementima iz polja $\mathbb{F}_p$.

Matricu A_p možemo promatrati kao matricu s elementima iz polja $\mathbb{F}_q$, obzirom da je svaki element polja $\mathbb{F}_p$ ujedno i element polja $\mathbb{F}_q$ (dobiven kao polinom nultog stupnja). Kraće ćemo pisati da je matrica A_p matrica s elementima iz polja $\mathbb{F}_p \hookrightarrow \mathbb{F}_q$.

Napomena 1.1.27. Elementi koji su jednaki 0 u polju $\mathbb{F}_q$ su također 0 u polju $\mathbb{F}_{q^2}$, obzirom da su elementi polja $\mathbb{F}_q$ u polju $\mathbb{F}_{q^2}$ polinomi stupnja najviše 1 s koeficijentima iz $\mathbb{F}_q$.

1.2. OSNOVNI POJMOVI TEORIJE DIZAJNA

1.2.1. Incidencijske strukture

Definicija 1.2.1. **Incidencijska struktura** $\mathscr{D}$ je uređena trojka $(\mathscr{P}, \mathscr{B}, \mathscr{I})$, gdje su $\mathscr{P}$ i $\mathscr{B}$ neprazni disjunktni skupovi i $\mathscr{I} \subseteq \mathscr{P} \times \mathscr{B}$. Elemente skupa $\mathscr{P}$ nazivamo **točkama**, elemente skupa $\mathscr{B}$ **blokovima**, a relaciju $\mathscr{I}$ **relacijom incidencije**.

Broj blokova koji su incidentni s točkom P naziva se **stupnjem točke** P i broj točaka koje su incidentne s blokom B naziva se **stupnjem bloka** B.

Prebrojavanjem uređenih parova (P,B), gdje je P točka incidencijske strukture i B blok incidentan s točkom P, dobivamo sljedeću tvrdnju.

Propozicija 1.2.2. Neka je $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ incidencijska struktura sa v točaka i b blokova za koju su stupnjevi točaka $r_1, \ldots, r_v$ i stupnjevi blokova $k_1, \ldots, k_b$. Tada je

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

Korolar 1.2.3. Za incidencijsku strukturu s v točaka i b blokova u kojoj svaka točka ima stupaj r i u kojoj svaki blok ima stupanj k vrijedi $vr = bk$.

Definicija 1.2.4. Neka je $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ incidencijska struktura. Struktura $\mathscr{D}^* = (\mathscr{P}^*, \mathscr{B}^*, \mathscr{I}^*)$, gdje je $\mathscr{P}^* = \mathscr{B}$, $\mathscr{B}^* = \mathscr{P}$, $\mathscr{I}^* = \{(x,P) \mid (P,x) \in \mathscr{I}\}$ naziva se **dualnom strukturom** strukture $\mathscr{D}$.

Svakoj incidencijskoj strukturi možemo pridružiti matricu incidencije na sljedeći način.

Definicija 1.2.5. Neka je $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ incidencijska struktura takva da je $\mathscr{P} = \{P_1, \ldots, P_v\}$ i $\mathscr{B} = \{B_1, \ldots, B_b\}$. **Matrica incidencije** incidencijske strukture $\mathscr{D}$ je $b \times v$ matrica $M = [m_{ij}]$, pri čemu je

$$m_{ij} = \begin{cases} 1, & P_j \in B_i, \\ 0, & \text{inače} \end{cases}.$$

Napomena. Neka je M matrica incidencije incidencijske strukture $\mathscr{D}$. Matrica incidencije dualne strukture $\mathscr{D}^*$ je M^T.

Definicija 1.2.6. Neka su $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ i $\mathscr{D}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ incidencijske strukture. Bijektivno preslikavanje $f : \mathscr{P} \cup \mathscr{B} \to \mathscr{P}' \cup \mathscr{B}'$ je **izomorfizam** iz $\mathscr{D}$ na $\mathscr{D}'$ ako

1. f preslikava $\mathscr{P}$ na $\mathscr{P}'$ i $\mathscr{B}$ na $\mathscr{B}'$,

2. $(P,B) \in \mathscr{I} \Leftrightarrow \big(f(P), f(B)\big) \in \mathscr{I}'$, $\forall P \in \mathscr{P}$ i $\forall B \in \mathscr{B}$.

Ako je $\mathscr{D} = \mathscr{D}'$, preslikavanje f naziva se **automorfizam**.

Skup svih automorfizama incidencijske strukture $\mathscr{D}$ je grupa s obzirom na kompoziciju funkcija i naziva se **puna grupa automorfizama** incidencijske strukture $\mathscr{D}$, u oznaci Aut$\mathscr{D}$.

Neka je M matrica incidencije incidencijske strukture $\mathscr{D}$ i M' matrica incidencije incidencijske strukture $\mathscr{D}'$. Strukture $\mathscr{D}$ i $\mathscr{D}'$ su izomorfne ako i samo ako postoje permutacijske matrice P i Q takve da je $P \cdot M \cdot Q = M'$. Matrica P opisuje djelovanje izomorfizma na skup točaka, a matrica Q opisuje djelovanje izomorfizma na skup blokova.

Napomena 1.2.7. Grupa automorfizama incidencijske strukture djeluje na skup točaka i blokova te strukture.

1.2.2. Dizajni

Definicija 1.2.8. Konačna incidencijska struktura $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ je t-(v,k,λ) dizajn ako vrijedi sljedeće.

1. $|\mathscr{P}| = v$,

2. svaki element skupa $\mathscr{B}$ je incidentan s točno k elemenata skupa $\mathscr{P}$,

3. svakih t elemenata skupa $\mathscr{P}$ je incidentno s točno λ elemenata skupa $\mathscr{B}$.

Kako bi izbjegli trivijalne slučajeve, zahtijevamo da su svi parametri t-(v,k,λ) dizajna prirodni brojevi za koje je $v > k \geq t$. Za k-$(v,k,1)$ dizajn kažemo da je **potpun**. Ako za broj blokova b t-(v,k,λ) dizajna $\mathscr{D}$ vrijedi da je $b < \binom{v}{k}$, kažemo da je dizajn $\mathscr{D}$ **nepotpun**.

Propozicija 1.2.9. Neka je $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ t-(v,k,λ) dizajn. Tada je $\mathscr{D}$ ujedno i s-(v,k,λ_s) dizajn za svaki $s \in \{1,2,\ldots,t-1\}$, gdje je

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

Dokaz. Neka je $S \subseteq \mathscr{P}$ proizvoljni s-člani podskup skupa točaka. Tvrdnju dokazujemo dvostrukim prebrojavanjem parova skupa $\{(T,B) \mid S \subseteq T \subseteq \mathscr{B}, |T| = t, B \in \mathscr{B}\}$.

■

Napomena 1.2.10. Posebno, iz prethodne propozicije slijedi da je svaki t-dizajn ujedno i 1-dizajn.

Kako je λ_s iz propozicije 1.2.9 prirodan broj, slijedi tvrdnja sljedećeg korolara.

Korolar 1.2.11. Ako postoji t-(v,k,λ) dizajn, onda $\binom{k-s}{t-s}$ dijeli $\lambda\binom{v-s}{t-s}$, za svaki $s \in \{1,2,\ldots,t-1\}$.

Korolar 1.2.11 daje nužan uvjet postojanja t-dizajna. U slučaju da je $t = 1$, ovaj uvjet je i dovoljan, što je dokazano u [42].

Teorem 1.2.12. 1-(v,k,λ) dizajn postoji ako i samo ako je $v\lambda \equiv 0 \pmod{k}$.

Neka je M matrica incidencije t-(v,k,λ) dizajna. Tada vrijedi:

1. $M \cdot \mathbf{J} = k \cdot \mathbf{J}$,
2. $\mathbf{J} \cdot M = r \cdot \mathbf{J}$,
3. ako je $t = 2$, onda je $M^T \cdot M = (r-\lambda) \cdot I + \lambda \cdot \mathbf{J}$,

gdje je I jedinična matrica odgovarajućeg reda, a $\mathbf{J}$ matrica odgovarajućeg reda čiji svi elementi su jedinice.

Definicija 1.2.13. 2-(v,k,λ) dizajn naziva se **blokovni dizajn**.

Nužan uvjet za postojanje 2-dizajna daje Fisherova nejednakost, čiji dokaz se može pronaći u [42].

Teorem 1.2.14 (Fisherova nejednakost)**.** Neka je $\mathscr{D}$ 2-(v,k,λ) dizajn s b blokova. Tada je $b \geq v$.

Napomena 1.2.15. U 1-dizajnu moguće je da je $b \leq v$.

Prema propoziciji 1.2.9 svaki blokovni dizajn je ujedno i 1-dizajn te vrijedi sljedeća propozicija.

Propozicija 1.2.16. Neka je $\mathscr{D}$ 2-(v,k,λ) dizajn. Tada sve točke dizajna $\mathscr{D}$ imaju isti stupanj

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

Iz prethodne propozicije slijedi nužan uvjet postojanja blokovnog dizajna:

$$(k-1) \mid \lambda(v-1).$$

Definicija 1.2.17. Nepotpun t-(v,k,λ) dizajn je **simetričan** ako je $b = v$.

Uvjet iz definicje 1.2.17 ekvivalentan je uvjetu $r = k$.

Propozicija 1.2.18. Ako je t-(v,k,λ) dizajn simetričan, onda je $t \leq 2$.

Iz propozicije 1.2.16 slijedi da je nužan uvjet za postojanje simetričnog blokovnog dizajna $k(k-1) = \lambda(v-1)$. Slijede još dva nužna uvjeta egzistencije simetričnog dizajna, Schützenbergerov uvjet i Bruck-Ryser-Chowla uvjet čiji dokaz se može pronaći u [42].

Teorem 1.2.19 (Schützenberger)**.** Neka je $\mathscr{D}$ simetričan 2-(v,k,λ) dizajn. Ako je v paran broj, onda je $k-\lambda$ kvadrat nekog prirodnog broja.

Teorem 1.2.20 (Bruck-Ryser-Chowla)**.** Neka je $\mathscr{D}$ simetričan 2-(v,k,λ) dizajn. Ako je v neparan broj, onda jednadžba

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

ima rješenje $(x,y,z) \in \mathbb{Z}^3$ takvo da je $(x,y,z) \neq (0,0,0)$.

Navedeni uvjeti su nužni, ali ne i dovoljni uvjeti postojanja simetričnog blokovnog dizajna. Na primjer, simetričan dizajn s parametrima 2-$(111,11,1)$ ne postoji iako zadovoljava nužne uvjete egzistencije simetričnog dizajna ([12]).

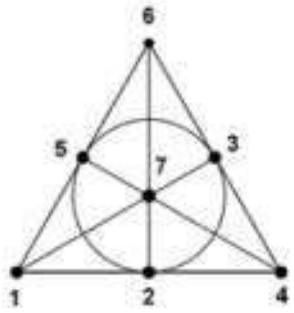
Primjer 1.2.1. Neka je

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

i

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

Tada je $\mathscr{D} = (\mathscr{P},\mathscr{B})$ simetrični 2-$(7,3,1)$ dizajn, prikazan slikom 1.1.



Slika 1.1: Simetrični 2-$(7,3,1)$ dizajn.

Dizajn $\mathscr{D}$ je najmanja projektivna ravnina reda 2, poznat i pod imenom Fanova ravnina. Matrica incidencije navedenog dizajna je

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

a puna grupa automorfizama je $\mathrm{Aut}\mathscr{D} = P\Gamma L(3,2)$.

Napomena 1.2.21. Dualni dizajn 2-(v,k,λ) dizajna s b blokova i stupnjem točke r je 1-(b,r,k) dizajn. Dualni dizajn dizajna $\mathscr{D}$ je 2-dizajn ako i samo ako je $\mathscr{D}$ simetričan dizajn.

Dokaz sljedećeg teorema može se pronaći u [42].

Teorem 1.2.22. U simetričnom 2-(v,k,λ) dizajnu su svaka dva bloka incidentna s točno λ zajedničkih točaka.

Definicija 1.2.23. **Presječni broj blokova** B_1 i B_2 t-(v,k,λ) dizajna je broj $|B_1 \cap B_2|$.

Definicija 1.2.24. Neka su x i y nenegativni cijeli brojevi. Blokovni dizajn je **kvazisimetričan** ako su svi presječni blokovi dva različita bloka x ili y.

Uočimo da je svaki simetričan dizajn i kvazisimetričan za $x = \lambda$ i y proizvoljan.

Simetrični dizajni postoje samo za $t \leq 2$ (propozicija 1.2.18). Cameron je u [10] dokazao sličnu tvrdnju i za egzistenciju kvazisimetričnih t-dizajna.

Teorem 1.2.25. Ako postoji netrivijalni kvazisimetričan t-dizajn, onda je $t \leq 4$.

Kvazisimetrični 4-dizajni su klasificirani i poznato je da su jedini netrivijalni kvazisimetrični 4-dizajni derivirani veliki Wittov dizajn 4-$(23,7,1)$ i njegov komplement 4-$(23,16,52)$. Klasifikaciju kvazisimetričnih 3-dizajna s presječnim brojem $x = 0$ riješio je P. J. Cameron u [9], dok je za $x > 0$ poznato jako malo primjera te je u [40] postavljena hipoteza da su to jedini poznati primjeri kvazisimetričnih 3-dizajna s presječnim brojem $x > 0$. Egzistencija kvazisimetričnih 2-dizajna je težak otvoreni problem te postoje mnogi parametri (v,k,λ) za koje egzistencija kvazisimetričnih 2-dizajna nije poznata.

Definicija 1.2.26. Neka je p prost broj i neka je $\mathscr{D}$ 1-(v,k,λ) dizajn takav da je $k \equiv a \pmod{p}$ i $|B_i \cap B_j| \equiv d \pmod{p}$, gdje su B_i i B_j različiti blokovi dizajna $\mathscr{D}$, $i \in \{1,\ldots,b\}$. Dizajn $\mathscr{D}$ zovemo **slabo p-samoortogonalan dizajn**.
Posebno, slabo p-samoortogonalan dizajn za koji je $a = d = 0$ zovemo **p-samoorotogonalan dizajn**.

Napomena 1.2.27. Ako je $p = 2$, dizajn $\mathscr{D}$ iz prethodne definicije zovemo slabo samoortogonalan dizajn / samoortogonalan dizajn.

Napomena 1.2.28. Uočimo da je kvazisimetričan dizajn $\mathscr{D}$ s veličinama presjeka x i y za koji vrijedi da x i y daju isti ostatak pri dijeljenju s prostim brojem p slabo p-samoortogonalan dizajn.

Orbitne matrice

Definicija 1.2.29. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn i neka je G grupa automorfizama dizajna $\mathscr{D}$. Neka su $\mathscr{V}_1,\ldots,\mathscr{V}_n$ orbite za djelovanje grupe G na skupu točaka veličina $v_1,\ldots,v_n$ te neka su $\mathscr{B}_1,\ldots,\mathscr{B}_m$ orbite za djelovanje grupe G na skupu blokova veličina $b_1,\ldots,b_m$.
Orbitna matrica za djelovanje grupe G je $m \times n$ matrica

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{bmatrix},$$

gdje je $a_{i,j}$ broj točaka iz orbite $\mathscr{V}_j$ incidentnih s blokom iz orbite $\mathscr{B}_i$.

Napomena 1.2.30. Lako se vidi da je orbitna matrica dobro definirana i da je $k = \sum_{j=1}^{n} a_{i,j}$. Za $x \in \mathscr{B}_s$, prebrojavanjem parova (P,x') za koje je $x' \in \mathscr{B}_t$ i P točka incidentna s blokom x, dobivamo da vrijedi $\sum_{x' \in \mathscr{B}_t} |x \cap x'| = \sum_{j=1}^{n} \frac{b_t}{v_j} a_{s,j} a_{t,j}$ ([27]).

Definicija 1.2.31. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn i neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka sa f_1 fiksnih točaka i n orbita duljine $w > 1$ te koja djeluje na skup blokova sa f_2 fiksnih blokova i m orbita duljine w. Definiramo matrice $OM1$ i $OM2$ redom kao matrice

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,f_1} \\ a_{2,1} & a_{2,2} & \dots & a_{2,f_1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{f_2,1} & a_{f_2,2} & \dots & a_{f_2,f_1} \end{bmatrix}$$

i

$$\begin{bmatrix} a_{f_2+1,f_1+1} & a_{f_2+1,f_1+2} & \dots & a_{f_2+1,f_1+n} \\ a_{f_2+2,f_1+1} & a_{f_2+2,f_1+2} & \dots & a_{f_2+2,f_1+n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{f_2+m,f_1+1} & a_{f_2+m,f_1+2} & \dots & a_{f_2+m,f_1+n} \end{bmatrix},$$

gdje stupci $1,2,\dots,f_1$ odgovaraju fiksnim točkama i retci $1,2,\dots,f_2$ odgovaraju fiksnim blokovima.

Napomena 1.2.32.

a) Ako su B_1 i B_2 fiksni blokovi djelovanja grupe G na dizajn, tada su B_1, B_2 i $B_1 \cap B_2$ unije nekih G-orbita skupa točaka dizajna.

b) Neka su $\mathscr{B}_t$ i $\mathscr{B}_s$ blokovi iz orbite duljine w. Iz napomene 1.2.30 slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| = \sum_{j=1}^{f_1} \frac{b_t}{v_j} a_{s,j} a_{t,j} + \sum_{j=f_1+1}^{f_1+n} \frac{b_t}{v_j} a_{s,j} a_{t,j} = w \sum_{j=1}^{f_1} a_{s,j} a_{t,j} + \sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{t,j}.$$

1.2.3. Konstrukcija dizajna iz grupe

Sljedeća dva teorema opisuju metodu konstrukcije dizajna iz grupe, a ekvivalenta su teoremu iz [18].

Teorem 1.2.33. Neka je G konačna permutacijska grupa koja djeluje tranzitivno na $n-$člani skup Ω. Neka su $\alpha \in \Omega$ i $\Delta = \bigcup_{i=1}^{s} G_\alpha.\delta_i$, gdje su $\delta_i,\dots,\delta_s \in \Omega$ predstavnici različitih G_α-orbita. Ako je $\Delta \neq \Omega$ i

$$\mathscr{B} = \{g.\Delta \mid g \in G\},$$

tada je $\mathscr{D} = (\Omega, \mathscr{B})$ 1-$(n, |\Delta|, \frac{|G_\alpha|}{|G_\Delta|} \sum_{i=1}^{s} |G_{\delta_i}.\alpha|)$ dizajn s $b = \frac{n \cdot |G_\alpha|}{|G_\Delta|}$ blokova na kojeg grupa G djeluje tranzitivno.

Uočimo da je $G_\alpha \leq G_\Delta$ pa je $b \leq n$.

Napomena 1.2.34. Posebno, ako je djelovanje iz prethodnog teorema primitivno, tada je $G_\alpha = G_\Delta$ pa je $b = n$, odnosno 1-dizajn je simetričan.

Teorem 1.2.35. Neka je G konačna permutacijska grupa koja djeluje tranzitivno na $n-$člani skup Ω i neka je P podgrupa grupe G. Neka je $\Delta = \cup_{i=1}^{s} P.\delta_i$ gdje su $\delta_1, \ldots, \delta_s \in \Omega$ predstavnici različitih P-orbita. Tada je

$$\mathscr{B} = \{g.\Delta \mid g \in G\}$$

skup blokova 1-dizajna s parametrima $1 - \left(n, |\Delta|, \frac{|P|}{|G_\Delta|} \sum_{i=1}^{s} \frac{|G_{\delta_i}|}{|P \cap G_{\delta_i}|}\right)$ i $b = \frac{|G|}{|G_\Delta|}$ blokova. Grupa G djeluje tranzitivno na skup točaka i blokova dizajna.

Napomena 1.2.36. Teorem 1.2.35 je poopćenje teorema 1.2.33, obzirom da je G_α podgrupa grupe G. Posebno, za $P = G_\alpha$ je

$$b = |G.\Delta| = \frac{|G|}{|G_\Delta|} = \frac{|G| \cdot |G_\alpha|}{|G_\Delta| \cdot |G_\alpha|} = \frac{|\Omega| \cdot |G_\alpha|}{|G_\Delta|} = \frac{n \cdot |G_\alpha|}{|G_\Delta|},$$

$$r = \frac{|G_\alpha|}{|G_\Delta|} \sum_{i=1}^{s} \frac{|G_{\delta_i}|}{|G_\alpha \cap G_{\delta_i}|} = \frac{|G_\alpha|}{|G_\Delta|} \sum_{i=1}^{s} \frac{|G_{\delta_i}|}{|(G_{\delta_i})_\alpha|} = \frac{|G_\alpha|}{|G_\Delta|} \sum_{i=1}^{s} |G_{\delta_i}.\alpha|.$$

Teorem 1.2.35 omogućuje konstrukciju i nesimetričnih t-dizajna za $t \geq 2$.

1.3. OSNOVNI POJMOVI TEORIJE GRAFOVA

Definicija 1.3.1. **Graf** $\mathscr{G}$ je incidencijska struktura $\mathscr{G} = (\mathscr{V}, \mathscr{E}, \mathscr{I})$, gdje je $\mathscr{V}$ neprazan skup vrhova, $\mathscr{E}$ skup bridova i $\mathscr{I}$ funkcija incidencije koja svakom bridu pridružuje par ne nužno različitih vrhova.

Kažemo da su vrhovi u i v **susjedni** ako su incidentni s istim bridom. Ako je vrh v incidentan sa samim sobom, brid (v,v) zovemo **petljom.** Broj bridova incidentnih s vrhom v naziva se **stupnjem** vrha v, pri čemu petlje računamo dvaput.

Definicija 1.3.2. Graf je **jednostavan** ako je bez petlji i ako su svaka dva vrha incidentna s najviše jednim bridom.

Definicija 1.3.3. **Matrica susjedstva** grafa $\mathscr{G}$ s vrhovima $v_1, \ldots, v_n$ je $n \times n$ matrica $A = [a_{ij}]$ gdje je a_{ij} broj bridova incidentnih sa v_i i v_j.

Matrica susjedstva jednostavnog grafa je matrica čiji elementi su 0 ili 1 i čiji svi elementi na dijagonali su 0.

Definicija 1.3.4. Graf $\mathscr{G}$ je **k-regularan** ako je svaki vrh grafa $\mathscr{G}$ stupnja k.

Napomena 1.3.5. Matrica susjedstva jednostavnog k-regularnog grafa je matrica incidencije simetričnog 1-dizajna.

Definicija 1.3.6. Jednostavan graf $\mathscr{G} = (\mathscr{V}, \mathscr{E}, \mathscr{I})$ je **jako regularan** s parametrima (n,k,λ,μ) ako vrijedi sljedeće.

1. $|\mathscr{V}| = n$,
2. $\mathscr{G}$ je k-regularan graf,
3. svaka dva susjedna vrha imaju točno λ zajedničkih susjednih vrhova,
4. svaka dva nesusjedna vrha imaju točno μ zajedničkih susjednih vrhova.

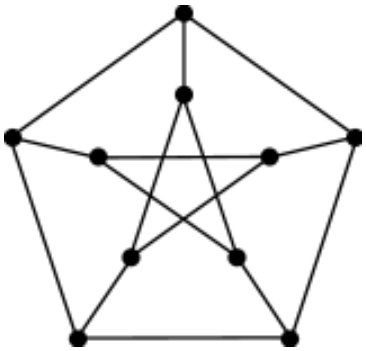
Jako regularan graf s parametrima (n,k,λ,μ) označavamo sa $SRG(n,k,\lambda,\mu)$ (*strongly regular graph*).

Sljedećim teoremom, čiji dokaz se može pronaći u [3], dan je nužan uvjet za egzistenciju $SRG(n,k,\lambda,\mu)$.

Teorem 1.3.7. Neka je $\mathscr{G}$ jako regularan graf s parametrima (n,k,λ,μ). Tada je

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

Primjer jako regularnog grafa je Petersenov graf, prikazan na slici 1.2. Petersenov graf je jako regularan graf s parametrima $(10,3,0,1)$.



Slika 1.2: Petersenov graf, $SRG(10,3,0,1)$

Definicija 1.3.8. Neka je $\mathscr{D}$ 2-(v,k,λ) kvazisimetričan dizajn s b blokova i presječnim brojevima x i y, $x<y$. **Blokovni graf** dizajna $\mathscr{D}$ je graf čiji vrhovi su blokovi dizajna $\mathscr{D}$, a dva vrha su susjedna ako se pripadni blokovi sijeku u y točaka.

Napomena 1.3.9. U prethodnoj definiciji možemo promatrati i da su dva vrha susjedna ako se pripadni blokovi sijeku u x točaka.

R. C. Bose [5] je dokazao da je blokovni graf u slučaju $\lambda = 1$ jako regularan s parametrima $SRG(b,k(r-1),r-2+(k-1)^2,k^2)$. Sljedeći teorem pokazuje da je blokovni graf kvazisimetričnog dizajna jako regularan, a dokaz se može pronaći [29].

Teorem 1.3.10. Neka je $\mathscr{D}$ kvazisimetričan 2-(v,k,λ) dizajn s presječnim brojevima x i y te neka je $\mathscr{G}$ njemu pridružen blokovni graf. Pretpostavimo da je graf $\mathscr{G}$ povezan. Tada je $\mathscr{G}$ jako regularan graf s parametrima $SRG(b,a,c,d)$ za

$$a = \frac{k(r-1)-x(b-1)}{y-x},\ \ c = a+\Theta_1+\Theta_2+\Theta_1\Theta_2 \ \text{ i } \ d = a+\Theta_1\Theta_2,$$

pri čemu je $\Theta_1 = \dfrac{r-\lambda-k+x}{y-x}$ i $\Theta_2 = -\dfrac{k-x}{y-x}$.

1.4. OSNOVNI POJMOVI TEORIJE KODIRANJA

Teorija kodiranja bavi se prijenosom informacija od pošiljatelja do primatelja kroz komunikacijski kanal sa smetnjama te dekodiranjem, odnosno određivanjem originalne poruke iz primljene poruke. Prilikom dekodiranja potrebno je detektirati i ispraviti pogreške nastale prilikom prijenosa poruke. Začetnik teorije kodiranja je C. E. Shannon, a temelje teorije kodiranja postavio je u radu [39] 1948. godine, a osim njegovog rada, najraniji radovi vezani za teoriju kodiranja su radovi Golaya ([30]) i Hamminga ([32]). Neki od najboljih poznatih kodova su upravo prošireni Golayev kod i prošireni Hammingov kod.

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 LCD kodovi.

Definicija 1.4.1. **Kod** $\mathscr{C}$ duljine n nad alfabetom F je podskup $\mathscr{C} \subseteq F^n$. Skup F^n zovemo **prostorom koda**, a $|\mathscr{C}|$ je veličina koda. Elemente skupa $\mathscr{C}$ zovemo **riječima koda**.

Kod nad alfabetom $\mathbb{F}_2$ zovemo **binarnim kodom**.

Definicija 1.4.2. Neka su $\mathbf{x} = (x_1, \ldots, x_n)$ i $\mathbf{y} = (y_1, \ldots, y_n)$ riječi koda $\mathscr{C} \subseteq F^n$. Broj

$$d_H(\mathbf{x}, \mathbf{y}) = \left| \{ i \mid x_i \neq y_i,\ i \in \{1, \ldots, n\} \} \right|$$

zovemo **Hammingovom udaljenost** riječi $\mathbf{x}$ i $\mathbf{y}$.

Definicija 1.4.3. **Najmanja udaljenost koda** $\mathscr{C}$ u oznaci $d_{min}(\mathscr{C})$ je broj

$$d_{min}(\mathscr{C}) = \min\{d_H(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathscr{C}, \mathbf{x} \neq \mathbf{y}\}.$$

Definicija 1.4.4. Neka je $\mathbf{x}$ riječ koda $\mathscr{C} \subseteq F^n$. **Težina riječi** $\mathbf{x}$ je broj

$$w(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0}),$$

gdje je $\mathbf{0} = (0, \ldots, 0) \in F^n$.

Definicija 1.4.5. Dva koda $\mathscr{C}_1$ i $\mathscr{C}_2$ duljine n nad istim alfabetom su **izomorfna** ako postoji permutacija f skupa $\{1,2,\ldots,n\}$ takva da za svaku riječ $\mathbf{x} = (x_1,\ldots,x_n) \in \mathscr{C}_1$ postoji riječ $\mathbf{y} = (y_1,\ldots,y_n) \in \mathscr{C}_2$ takva da je $\mathbf{y} = (x_{f(1)},\ldots,x_{f(n)})$ i obratno.

Definicija 1.4.6. Neka je q potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathbb{F}_q^n$ vektorski prostor dimenzije n nad poljem $\mathbb{F}_q$. **Linearan kod** $\mathscr{C}$ duljine n i dimenzije k nad poljem $\mathbb{F}_q$ je k-dimenzionalan vektorski potprostor prostora $\mathbb{F}_q^n$. Parametre linearnog koda $\mathscr{C}$ označavamo s $[n,k]_q$.
Ako je najmanja udaljenost koda $\mathscr{C}$ jednaka d, parametre linearnog koda $\mathscr{C}$ označavamo sa $[n,k,d]_q$.

Napomena 1.4.7. Ukoliko je $q = 2$, parametre linearnog $[n,k,d]_2$ koda $\mathscr{C}$ označavamo sa $[n,k,d]$.

Sljedeće propozicije govore o minimalnoj udaljenosti koda, a dokaz se može pronaći u [36].

Propozicija 1.4.8. Minimalna udaljenost linearnog koda $\mathscr{C}$ jednaka je

$$d = \min\{w_H(\mathbf{x}) \mid \mathbf{x} \in \mathscr{C}, \mathbf{x} \neq \mathbf{0}\}.$$

Propozicija 1.4.9. Kod $\mathscr{C}$ s minimalnom udaljenosti d može detektirati najviše $d-1$ pogrešaka u jednoj riječi koda.

Propozicija 1.4.10. Linearan $[n,k,d]$ kod $\mathscr{C}$ može ispraviti najviše

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

pogrešaka u jednoj riječi koda.

Linearan $[n,k,d]$ kod je **optimalan** ako je za dane n,k njegova minimalna udaljenost d dostiže teorijsku granicu. Linearan $[n,k,d]$ kod je **skoro optimalan** ako je njegova minimalna udaljenost za 1 manja od minimalne udaljenosti optimalnog koda s istim n i k.

Definicija 1.4.11. Dva linearna koda nad istim poljem su **ekvivalentna** ako se jedan može dobiti iz drugog permutacijom koordinata u svim riječima koda i množenjem pojedine koordinate u svim riječima koda nekim nenul elementom polja.

Definicija 1.4.12. **Automorfizam** koda $\mathscr{C}$ je izomorfizam sa $\mathscr{C}$ u $\mathscr{C}$, tj. permutacija koordinatnih pozicija koja preslikava riječ koda u riječ koda. Skup svih automorfizama linearnog koda $\mathscr{C}$ čini grupu koju nazivamo **puna grupa automorfizama** koda $\mathscr{C}$ i označavamo $\mathrm{Aut}\mathscr{C}$.

Linearan kod često zadajemo njegovom generirajućom matricom.

Definicija 1.4.13. **Generirajuća matrica** linearnog $[n,k]_q$ koda $\mathscr{C}$ je $k \times n$ matrica čiji retci su vektori baze koda $\mathscr{C}$.

Kažemo da je generirajuća matrica linearnog $[n,k]_q$ koda u standardnom obliku ako je ona oblika $[I_k, A]$, gdje je I_k jedinična matrica reda k.

Definicija 1.4.14. Neka je $\mathscr{C}$ linearan kod nad konačnim poljem $\mathbb{F}_q$. **Dualni kod** koda $\mathscr{C}$, u oznaci $\mathscr{C}^\perp$, je kod

$$\mathscr{C}^\perp = \{x \in \mathbb{F}_q \mid x \cdot c = 0, \forall c \in C\},$$

gdje je sa $x \cdot c$ označen standardni skalarni produkt vektora x i c.

Definicija 1.4.15. Linearan kod $\mathscr{C}$ je

- **samoortogonalan** ako je $\mathscr{C} \subseteq \mathscr{C}^\perp$,
- **samodualan** ako je $\mathscr{C} = \mathscr{C}^\perp$.
- **LCD** (*linear code with complementary dual*) ako je $\mathscr{C} \cap \mathscr{C}^\perp = \{\mathbf{0}\}$.

Napomena 1.4.16. Ako je $\mathscr{C}$ samoortogonalan kod, tada je $\dim(C) \leq \frac{n}{2}$. Ako je $\mathscr{C}$ samodualan kod duljine n nad konačnim poljem $\mathbb{F}_q$, tada je n paran i

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

Iz prethodne napomene slijedi sljedeća propozicija.

Propozicija 1.4.17. Neka je $\mathscr{C}$ linearan $[n,k,d]_q$ kod čija generirajuća matrica je G.

1. $\mathscr{C}$ je samoortogonalan kod ako i samo ako je $G \cdot G^T = \mathbf{0}$.
2. $\mathscr{C}$ je samoodualan kod ako i samo ako je $G \cdot G^T = \mathbf{0}$ i $\dim(C) = \frac{n}{2}$.

Neka je A matrica dimenzije $m \times n$. S $A[i]$ označavat ćemo i-ti redak matrice A, $i \in \{1, \ldots, m\}$. S $A[i] \cdot A[j]$ označavamo skalarni produkt i-tog i j-tog retka matrice A. Uočimo da je uvjet $A \cdot A^T = \mathbf{0}$ ekvivalentan uvjetu $A[i] \cdot A[j] = 0,\ \forall i, j \in \{1, \ldots, m\}$.

Sljedećom propozicijom opisana je karakterizacija LCD kodova, a dokaz se može pronaći u [37].

Propozicija 1.4.18. Neka je $\mathscr{C}$ linearan $[n,k,d]_q$ kod čija generirajuća matrica je G. $\mathscr{C}$ je LCD kod ako i samo ako je $\det(G \cdot G^T) \neq 0$.

2. SAMOORTOGONALNI KODOVI IZ SLABO p-SAMOORTOGONALNIH DIZAJNA

U ovom poglavlju opisat ćemo metodu konstrukcije samoortogonalnih kodova koristeći odgovarajuće proširenje matrice incidencije, orbitne matrice i podmatrice orbitnih matrica slabo p-samoortogonalnih dizajna. Rezultati opisani u ovom poglavlju objavljeni su u [38].

Metodu konstrukcije binarnih samoortogonalnih kodova koristeći matricu incidencije slabo-samoortogonalnih dizajna dao je Tonchev 1989. godine u [43].

Teorem 2.0.1. Neka je $\mathscr{D}$ slabo samoortogonalan dizajn i neka je M njegova $b \times v$ matrica incidencije.

- Ako je $\mathscr{D}$ samoortogonalan dizajn, tada M generira binarni samoortogonalan kod.
- Ako je $\mathscr{D}$ dizajn s parnim k i neparnim presječnim brojevima dva različita bloka, tada matrica $[I_b, M, \mathbf{1}]$ generira binaran samoortogonalan kod, gdje je s $\mathbf{1}$ označena stupčana matrica čiji svi elementi su jednaki 1.
- Ako je $\mathscr{D}$ dizajn s neparnim k i parnim presječnim brojevima dva različita bloka, tada matrica $[I_b, M]$ generira binaran samoortogonalan kod.
- Ako je $\mathscr{D}$ dizajn s neparnim k i neparnim presječnim brojevima dva različita bloka, tada matrica $[M, \mathbf{1}]$ generira binaran samoortogonalan kod, gdje je s $\mathbf{1}$ označena stupčana matrica čiji svi elementi su jednaki 1.

Napomena 2.0.2. Uočimo da se permutacijom redaka u matrici M pri proširenju matrice M mogu dobiti neekvivalentni kodovi.

Napomena 2.0.3. U daljnjem tekstu, stupčanu matricu čiji svi elementi su jednaki 1 označavat ćemo s $\mathbf{1}$.

Teorem 2.0.1 primijenili smo na slabo samoortogonalne dizajne konstruirane iz Mathieuove grupe M_{11}. Dobiveni samoortogonalni kodovi prikazani su u poglavlju 4.1.1 u tablicama 4.2, 4.3, 4.4, 4.5, 4.6 i 4.7.

Prethodni teorem generalizirali smo kako bismo konstruirali samoortogonalne kodove nad konačnim poljem $\mathbb{F}_q$, gdje je q potencija prostog broja.

Teorem 2.0.4. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ slabo p-samoortogonalan dizajn za koji je $k \equiv a \pmod{p}$ i $|B_i \cap B_j| \equiv d \pmod{p}$, za sve $i, j \in \{1, \ldots, b\},\ i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$. Neka je M $b \times v$ matrica incidencije dizajna $\mathscr{D}$.

1. Ako je $\mathscr{D}$ p-samoortogonalan dizajn, tada matrica M_p generira samoortogonalan kod nad poljem $\mathbb{F}_q$.

2. Ako je $a = 0$ i $d \neq 0$, tada matrica $[\sqrt{d} \cdot I_b, M_p, \sqrt{-d} \cdot \mathbf{1}]$ generira b-dimenzionalan samoortogonalan kod nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su d i $-d$ kvadrati u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

3. Ako je $a \neq 0$ i $d = 0$, tada matrica $[M_p, \sqrt{-a} \cdot I_b]$ generira b-dimenzionalan samoortogonalan kod nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

4. Ako je $a \neq 0$ i $d \neq 0$, razlikujemo dva slučaja.

   4.1 Ako je $a = d$, tada matrica $[M_p, \sqrt{-a} \cdot \mathbf{1}]$ generira samoortogonalan kod nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

   4.2 Ako je $a \neq d$, tada matrica $[\sqrt{d-a} \cdot I_b, M_p, \sqrt{-d} \cdot \mathbf{1}]$ generira b-dimenzionalan samoortogonalan kod nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $d - a$ i $-d$ kvadrati u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

Dokaz.

1. Kako je $a = 0$ i $M[s] \cdot M[s] = k$, tada je

$$M_p[s] \cdot M_p[s] = 0.$$

   Kako je $d = 0$ i $M[s] \cdot M[t] = |B_i \cap B_j|$, tada je

$$M_p[s] \cdot M_p[t] = 0$$

za sve $s,t \in \{1,\ldots,b\},\ s \neq t$. Zaključujemo da je kod nad poljem $\mathbb{F}_q$ generiran matricom M_p samoortogonalan.

2. Neka je $A = [\sqrt{d} \cdot I_b, M_p, \sqrt{-d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su d i $-d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Tada je

$$A[s] \cdot A[s] = d + 0 - d = 0$$

i

$$A[s] \cdot A[t] = d - d = 0,$$

za sve $s,t \in \{1,\ldots,b\},\ s \neq t$. Zaključujemo da je kod nad poljem $\mathbb{F}$ generiran matricom A b-dimenzionalan samoortogonalan kod.

3. Neka je $A = [\sqrt{-a} \cdot I_b, M_p]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Tada je

$$A[s] \cdot A[s] = -a + a = 0$$

i

$$A[s] \cdot A[t] = 0,$$

za sve $s,t \in \{1,\ldots,b\},\ s \neq t$. Zaključujemo da je kod nad poljem $\mathbb{F}$ generiran matricom A b-dimenzionalan samoortogonalan kod. Ako je $b = v$, dimenzija koda je polovica njegove duljine pa je dobiveni kod samodualan.

4. (a) Neka je $A = [M_p, \sqrt{-a} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Tada je

$$A[s] \cdot A[s] = a - a = 0$$

i

$$A[s] \cdot A[t] = d - a = a - a = 0,$$

za sve $s,t \in \{1,\ldots,b\},\ s \neq t$. Zaključujemo da je kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan.

(b) Neka je $A = [\sqrt{d-a} \cdot I_b, M_p, \sqrt{-d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $d-a$ i $-d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Tada je

$$A[s] \cdot A[s] = d - a + a - d = 0$$

i

$$A[s]\cdot A[t] = d - d = 0,$$

za sve $s,t \in \{1,\ldots,b\},\ s \neq t$. Zaključujemo da je kod nad poljem $\mathbb{F}$ generiran matricom A b-dimenzionalan samoortogonalan kod.

■

Samoortogonalni kodovi dobiveni primjenom prethodnog teorema prikazani su u poglavlju 4 u tablicama 4.15, 4.16, 4.17, 4.18 i 4.19.

2.1. KODOVI IZ ORBITNIH MATRICA

Opisat ćemo konstrukciju samoorotogonalnih kodova koristeći orbitne matrice i podmatrice orbitnih matrica slabo p-samoortogonalnih dizajna.

Napomena 2.1.1. Neka je $\mathscr{D}$ slabo p-samoortogonalan 1-(v,k,r) dizajn za koji je $k \equiv a \pmod p$ i $|B_i \cap B_j| \equiv d \pmod p$, za sve $i,j \in \{1,\ldots,b\},\ i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na $\mathscr{D}$ sa n točkovnih orbita duljine w i koja djeluje na skup blokova dizajna $\mathscr{D}$ u orbitama duljina $b_1, b_2, \ldots, b_m$, te neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G. Iz napomene 1.2.30 slijedi da za $x \in \mathscr{B}_s$ i $s \neq t$ vrijedi

$$\begin{aligned}\frac{b_t}{w}O[s]\cdot O[t] &= \sum_{j=1}^{n}\frac{b_t}{w}a_{s,j}a_{t,j}\\ &= \sum_{x'\in\mathscr{B}_t}|x\cap x'|.\end{aligned}$$

Slijedi da je

$$\frac{b_t}{w}O[s]\cdot O[t] \equiv b_t\cdot d \pmod p.$$

Slično, za $x \in \mathscr{B}_s$ vrijedi

$$\begin{aligned}\frac{b_t}{w}O[s]\cdot O[s] &= \sum_{x'\in\mathscr{B}_s}|x\cap x'|\\ &= |x\cap x| + \sum_{x'\in\mathscr{B}_s,\ x\neq x'}|x\cap x'|.\end{aligned}$$

Slijedi da je

$$\frac{b_s}{w}O[s]\cdot O[s] \equiv a + (b_s - 1)\cdot d \pmod p.$$

Neka je p prost broj i $q = p^n$, za $n \in \mathbb{N}$. Uočimo da su a i d iz prethodne napomene elementi polja $\mathbb{F}_p \hookrightarrow \mathbb{F}_q$ te da je $b_t \cdot d = \underbrace{d + d + \ldots + d}_{b_t \text{ puta}} \in \mathbb{F}_p \hookrightarrow \mathbb{F}_q$. Posebno, $p \cdot d = 0$.

2.1.1. Kodovi iz orbitnih matrica samoortogonalnih 1-dizajna

Konstrukcija binarnih kodova koristeći orbitne matrice samoortogonalnih 1-dizajna opisana je u [17], a prikazana je sljedećim teoremom.

Teorem 2.1.2. Neka je $\mathscr{D}$ samoortogonalan 1-dizajn i neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na $\mathscr{D}$ sa n točkovnih orbita duljine w i koja djeluje na skup blokova u orbitama duljina $b_1, b_2, \ldots, b_m$ tako da je $b_i = 2^o \cdot b_i',\ w = 2^u \cdot w',\ o \leq u, 2 \nmid b_i'$ i $2 \nmid w'$, za $i \in \{1, \ldots, m\}$. Neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G. Tada je binaran kod razapet retcima matrice O samoortogonalan kod duljine $\frac{v}{w}$.

Teorem 2.1.2 primijenili smo na orbitne matrice slabo samoortogonalnih dizajna konstruiranih iz Mathieuove grupe M_{11}. Orbitne matrice dobivene su obzirom na djelovanje svih cikličkih podgrupa grupe M_{11} prostog reda koje djeluju na skup točaka dizajna bez fiksnih točaka. Dobiveni samoortogonalni kodovi prikazani su u poglavlju 4.1.1 u tablici 4.8.

Prethodni teorem može se generalizirati kako bi se konstruirali samoortogonalni kodovi nad konačnim poljem $\mathbb{F}_q$, gdje je q potencija prostog broja.

Teorem 2.1.3. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv 0 \pmod{p}$ i $|B_i \cap B_j| \equiv 0 \pmod{p}$, za sve $i, j \in \{1, \ldots, b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na $\mathscr{D}$ sa n točkovnih orbita duljine w i m blokovnih orbita duljine w. Neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G. Kod nad poljem $\mathbb{F}_q$ generiran matricom O_p je samoortogonalan kod duljine $\frac{v}{w}$.

Dokaz. Iz napomene 2.1.1 slijedi da je $O_p[s] \cdot O_p[t] = 0$ i $O_p[s] \cdot O_p[s] = 0$. Zaključujemo da je kod nad poljem $\mathbb{F}_q$ generiran matricom O_p samoortogonalan kod.

■

Teorem 2.1.3 primijenili smo na 3-samoortogonalne dizajne dobivene iz grupe A_5 na 30 točaka na koje ciklička grupa reda 3 djeluje bez fiksnih točaka. Dobiveni kodovi prikazani su u tablici 4.20.

Dokaz sljedećeg teorema može se pronaći u [17].

Teorem 2.1.4. Neka je $\mathscr{D}$ samoortogonalan 1-(v,k,r) dizajn i neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka dizajna $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine 2 i koja djeluje na skup blokova dizajna $\mathscr{D}$ u orbitama duljine 1 i 2. Tada vrijedi sljedeće.

1. Binarni linearni kod razapet retcima matrice $OM1$ je samoortogonalan kod duljine f_1.
2. Binarni linearan kod razapet retcima matrice $OM2$ je samoortogonalan kod duljine n.

Teorem 2.1.4 primijenili smo na orbitne matrice slabo samoortogonalnih dizajna konstruirane iz grupe M_{11} na koje ciklička grupa reda 2 djeluje s fiksnim točkama. Dobiveni samoortogonalni kodovi prikazani su u poglavlju 4.1.1 u tablici 4.13.

Sljedećim teoremom opisana je generalizacija prethodnog teorema kako bi se konstruirali samoortogonalni kodovi nad proizvoljnim konačnim poljem.

Teorem 2.1.5. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv 0 \pmod{p}$ i $|B_i \cap B_j| \equiv 0 \pmod{p}$, za sve $i,j \in \{1,\ldots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka od $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$, i koja djeluje na skup blokova dizajna $\mathscr{D}$ u orbitama duljine 1 i p^α. Tada vrijedi sljedeće.

1. Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM1_p$ je samoortogonalan kod duljine f_1.
2. Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM2_p$ je samoortogonalan kod duljine n.

Dokaz.

1. Obzirom da je $k \equiv 0 \pmod{p}$, svaki blok sadrži $p \cdot \beta$, $\beta \in \mathbb{N}$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv 0 \pmod{p}$, za sve $i,j \in \{1,\ldots,b\}$, $i \neq j$, presjek svaka dva bloka sadrži $p \cdot \gamma$, $\gamma \in \mathbb{N}$ fiksnih točaka. Slijedi da je

$$OM1_p[s] \cdot OM1_p[s] = 0$$

i da je

$$OM1_p[s] \cdot OM1_p[t] = 0.$$

Zaključujemo da je kod nad poljem $\mathbb{F}_q$ generiran matricom $OM1_p$ samoortogonalan kod duljine f_1.

2. Iz napomena 2.1.1 i 1.2.32, za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita veličine p^α slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv 0 \pmod{p}.$$

Za $s = t$ slijedi da je

$$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s, x \neq x'} |x \cap x'| \equiv 0 + (p^\alpha - 1) \cdot 0 \pmod{p}.$$

Tada je $OM2_p[s] \cdot OM2_p[t] = 0$, $\forall s,t \in \{1,\ldots,m\}$. Zaključujemo da je kod nad poljem $\mathbb{F}_q$ generiran matricom $OM2_p$ samoortogonalan kod duljine n.

■

Teorem 2.1.5 primijenili smo na 3-samoortogonalne dizajne dobivene iz grupe $O(7,3)$ na 364 točaka na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni kodovi prikazani su u tablici 4.26.

2.1.2. Kodovi iz orbitnih matrica proširenih slabo samoortogonalnih 1-dizajna s parnim k i neparnim presječnim brojevima

Opisat ćemo metode konstrukcije binarnih samoortogonalnih kodova koristeći orbitne matrice i podmatrice orbitnih matrica slabo samoortogonalnih 1-dizajna s parnim k i neparnim presječnim brojevima te generalizacije konstrukcija za samoortogonalne kodove nad poljem $\mathbb{F}_q$.

Teorem 2.1.6. Neka je $\mathscr{D}$ slabo samoortogonalan 1-dizajn s parnim k i neparnim presječnim brojevima te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na $\mathscr{D}$ sa n točkovnih orbita duljine w i koja djeluje na skup blokova dizajna $\mathscr{D}$ u orbitama duljina $b_1, b_2, \ldots, b_m$ tako da je $b_i = 2^o \cdot b_i'$, $w = 2^u \cdot w'$, $o \leq u, 2 \nmid b_i'$ i $2 \nmid w'$ za $i \in \{1,\ldots,m\}$. Neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G.

a) Ako je $o = u = 0$, binarni linearan kod razapet retcima matrice $[I_m, O, \mathbf{1}]$ je samoortogonalan kod duljine $m + \frac{v}{w} + 1$ i dimenzije m.

b) Ako je $o \geq 1$ i $o = u$, binarni linearan kod razapet retcima matrice $[I_m, O]$ je samoortogonalan kod duljine $m + \frac{v}{w}$ i dimenzije m. Ako je $m = n$, dobiveni kod je samodualan.

c) Ako je $o < u$, binarni linearan kod razapet retcima matrice O je samoortogonalan kod duljine $\frac{v}{w}$.

Dokaz.

a) Kako su $w, b_1, \ldots, b_m$ neparni brojevi, iz napomene 2.1.1 slijedi da je

$$O[s] \cdot O[t] \equiv 1 \pmod 2, \quad O[s] \cdot O[s] \equiv 0 \pmod 2,$$

za sve $s,t \in \{1,\ldots,m\},\ s \neq t$.
Tada za matricu $A = [I_m, O, \mathbf{1}]$ vrijedi da je

$$A[s] \cdot A[t] \equiv 1+1 \pmod 2 \equiv 0 \pmod 2,$$
$$A[s] \cdot A[s] \equiv 1+0+1 \pmod 2 \equiv 0 \pmod 2,$$

za sve $s,t \in \{1,\ldots,m\},\ s \neq t$. Vidimo da matrica A generira samoortogonalan kod duljine $m + \frac{v}{w} + 1$ i dimenzije m.

b) Kako su $w, b_1, \ldots, b_m$ parni i kako je $\frac{b_t}{w} = \frac{2^o \cdot b'_t}{2^o \cdot w'} = \frac{b'_t}{w'}$, za svaki $t \in \{1,\ldots,m\}$, iz napomene 2.1.1 slijedi da je

$$O[s] \cdot O[t] \equiv 0 \pmod 2, \quad O[s] \cdot O[s] \equiv 1 \pmod 2,$$

za sve $s,t \in \{1,\ldots,m\}$. Tada za matricu $A = [I_m, O]$ vrijedi da je

$$A[s] \cdot A[t] \equiv 1+1 \pmod 2 \equiv 0 \pmod 2,$$
$$A[s] \cdot A[s] \equiv 0 \pmod 2,$$

za sve $s,t \in \{1,\ldots,m\},\ s \neq t$. Vidimo da matrica A generira samoortogonalan kod duljine $m + \frac{v}{w}$ i dimenzije m. Ako je $m = n$, dimenzija dobivenog koda je upola manja od njegove duljine pa je dobiveni kod samodualan.

c) Kako je $o < u$ i kako je $\dfrac{b_t}{w} O[s] \cdot O[t] = \dfrac{b'_t}{2^{u-o} w'} O[s] \cdot O[t]$ prirodan broj, iz napomene 2.1.1 slijedi da $2 \mid O[s] \cdot O[t]$, za sve $s,t \in \{1,\ldots,m\}$. Direktno slijedi da retci matrice O razapinju binarni samoortogonalni kod duljine $\frac{v}{w}$.

■

Teorem 2.1.6 primijenili smo na orbitne matrice slabo samoortogonalnih dizajna konstruiranih iz Mathieuove grupe M_{11}. Orbitne matrice dobivene su obzirom na djelovanje svih cikličkih podgrupa grupe M_{11} prostog reda koje djeluju na skup točaka dizajna bez fiksnih točaka. Dobiveni samoortogonalni kodovi prikazani su u poglavlju 4.1.1 u tablici 4.9.

Prethodni teorem može se generalizirati kako bi se opisala konstrukcija samoortogonalnih kodova nad proizvoljnim konačnim poljem. Sljedeći teorem opisuje navedenu generalizaciju.

Teorem 2.1.7. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv 0 \pmod{p}$ i $|B_i \cap B_j| \equiv d \pmod{p}$, za sve $i, j \in \{1,\ldots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na dizajn $\mathscr{D}$ sa n točkovnih orbita duljine w i m blokovnih orbita duljine w. Neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G.

a) Ako $p \mid w$, linearan kod nad poljem $\mathbb{F}$ generiran matricom $A = [\sqrt{d} \cdot I_m, O_p]$ je samoortogonalan $[m+n, m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je d kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Ako je $m = n$, dobiveni kod je samodualan.

b) Ako $p \mid w-1$, linearan kod nad poljem $\mathbb{F}$ generiran matricom $A = [\sqrt{w \cdot d} \cdot I_m, O_p, \sqrt{-w \cdot d} \cdot \mathbf{1}]$ je samoortogonalan $[m+n+1, m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $w \cdot d$ i $-w \cdot d$ kvadrati u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

c) Ako $p \nmid w$ i $p \nmid w-1$, linearan kod nad poljem $\mathbb{F}$ generiran matricom $A = [\sqrt{d} \cdot I_m, O_p, \sqrt{-w \cdot d} \cdot \mathbf{1}]$ je samoortogonalan $[m+n+1, m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $-w \cdot d$ i d kvadrati u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

Dokaz.

Iz napomene 2.1.1 slijedi da je

$$O_p[s] \cdot O_p[t] = w \cdot d,$$

za $s \neq t$ i

$$O_p[s] \cdot O_p[s] = (w-1) \cdot d = w \cdot d - d.$$

a) Neka je $A = [\sqrt{d} \cdot I_m, O_p]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je d kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
Ako $p \mid w$, tada je

$$A[s] \cdot A[t] = 0$$

i

$$A[s] \cdot A[s] = d - d = 0.$$

Zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan kod duljine $m+n$ i dimenzije m. Ako je $m = n$, dimenzija koda je polovica njegove duljine pa je dobiveni kod samodualan.

b) Neka je $A = [\sqrt{w \cdot d} \cdot I_m, O, \sqrt{-w \cdot d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $w \cdot d$ i $-w \cdot d$ kvadrati u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
Ako $p \mid w-1$, tada je

$$A[s] \cdot A[t] = w \cdot d - w \cdot d = 0$$

i

$$A[s] \cdot A[s] = w \cdot d + 0 - w \cdot d = 0.$$

Zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan kod duljine $m+n+1$ i dimenzije m.

c) Neka je $A = [\sqrt{d} \cdot I_m, O, \sqrt{-w \cdot d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $-w \cdot d$ i d kvadrati u $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
Ako $p \nmid w$ i $p \nmid w-1$, tada je

$$A[s] \cdot A[t] = w \cdot d - w \cdot d = 0$$

i

$$A[s] \cdot A[s] = d + w \cdot d - d - w \cdot d = 0.$$

Zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan kod duljine $m+n+1$ i dimenzije m.

■

Teorem 2.1.9 primijenili smo na 3-samoortogonalne dizajne dobivene iz grupe A_5 na 30 točaka na koje ciklička grupa reda 5 djeluje bez fiksnih točaka. Dobiveni kodovi prikazani su u tablici 4.21.

Teorem 2.1.8. Neka je $\mathscr{D}$ slabo samoortogonalan 1-(v,k,r) dizajn s parnim k i neparnim presječnim brojevima dva različita bloka. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja na skup točaka dizajna $\mathscr{D}$ djeluje s f_1 fiksnih točaka i n orbita duljine 2 i koja na skup blokova djeluje sa f_2 fiksnih blokova i m orbita duljine 2. Tada vrijedi sljedeće.

1. Binaran linearan kod razapet retcima matrice $[I_{f_2}, OM1, \mathbf{1}]$ je samoortogonalan kod duljine $f_2 + f_1 + 1$ i dimenzije f_2.

2. Binaran linearan kod razapet retcima matrice $[I_m, OM2]$ je samoortogonalan kod duljine $m+n$ i dimenzije m. Ako je $m = n$, dobiveni kod je samodualan.

Dokaz.

1. Obzirom da je k paran, svaki blok sadrži paran broj fiksnih točaka i obzirom da su presječni brojevi svaka dva bloka neparni, presjek svaka dva bloka sadrži neparan broj fiksnih točaka. Slijedi da retci matrice $[I_{f_2}, OM1, \mathbf{1}]$ razapinju binaran samoortogonalan kod.

2. Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine 2, iz napomene 1.2.32 slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv 2 \cdot 1 \pmod 2 \equiv 0 \pmod 2$$

i za $s = t$ slijedi da je

$$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s,\ x \neq x'} |x \cap x'| \equiv 0 + 1 \pmod 2.$$

Zaključujemo da je $\sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{t,j} \equiv 0 \pmod 2$, za $s \neq t$ i $\sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{s,j} \equiv 1 \pmod 2$ te da je binarni kod razapet retcima matrice $[I_m, OM2]$ samoortogonalan. Ako je $m = n$, dimenzija koda je upola manja od njegove duljine pa je dobiveni kod samodualan.

■

Prethodni teorem može se generalizirati kako bi se konstruirali samoortogonalni kodovi nad poljem $\mathbb{F}_q$, gdje je q potencija prostog broja.

Teorem 2.1.9. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv 0 \pmod p$ i $|B_i \cap B_j| \equiv d \pmod p$, za sve $i, j \in \{1, \ldots, b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja na skup točaka dizajna $\mathscr{D}$ djeluje sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$, i na skup blokova djeluje sa f_2 fiksnih blokova i m orbita duljine p^α. Tada vrijedi sljedeće.

1. Linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{d} \cdot I_{f_2}, OM1_p, \sqrt{-d} \cdot \mathbf{1}]$ je samoortogonalan $[f_2 + f_1 + 1, f_2]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su d i $-d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

2. Linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{d} \cdot I_m, OM2_p]$ je samoortogonalan $[m+n, m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je d kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Ako je $m = n$, dobivani kod je samodualan.

Dokaz.

1. Obzirom da je $k \equiv 0 \pmod{p}$, svaki blok sadrži $p \cdot \beta,\ \beta \in \mathbb{N}$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv d \pmod{p}$, za sve $i, j \in \{1, \ldots, b\},\ i \neq j$, presjek svaka dva bloka sadrži $p \cdot \gamma + d, \gamma \in \mathbb{N}$ fiksnih točaka.
   Neka je $A = [\sqrt{d} \cdot I_{f_2}, OM1_p, \sqrt{-d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su d i $-d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
   Slijedi da je
   $$A[s] \cdot A[t] = d - d = 0$$
   i
   $$A[s] \cdot A[s] = d + 0 - d = 0,$$
   za $s,t \in \{1, \ldots, f_2\},\ s \neq t$. Zaključujemo da je linearan kod razapet retcima matrice A samoortogonalan kod duljine $f_2 + f_1 + 1$ i dimenzije f_2,

2. Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je
   $$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv p^\alpha \cdot d \pmod{p} \equiv 0 \pmod{p}$$
   i da je za $s = t$
   $$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s,\ x \neq x'} |x \cap x'| \equiv 0 + (p^\alpha - 1) \cdot d \pmod{p} \equiv -d \pmod{p}.$$
   Zaključujemo da je
   $$OM2_p[s] \cdot OM2_p[t] = 0$$
   i
   $$OM2_p[s] \cdot OM2_p[s] = -d$$
   za sve $s,t \in \{1, \ldots, m\},\ s \neq t$.
   Zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{d} \cdot I_m, OM2_p]$ samoortogonalan kod duljine $m + n$ i dimenzije m, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je d kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Ako je $m = n$, duljina dobivenog koda je dvostruko veća od njegove dimenzije pa je dobiveni kod samodualan.

■

Teorem 2.1.9 primijenili smo na orbitne matrice slabo 3-samoortogonalnih dizajna konstruiranih iz grupe $S(4,9)$ na 1640 točke na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni samoortogonalni kodovi prikazani su u tablici 4.27.

2.1.3. Kodovi iz orbitnih matrica proširenih slabo samoortogonalnih 1-dizajna s parnim k i parnim presječnim brojevima dva različita bloka

Opisat ćemo metode konstrukcije binarnih samoortogonalnih kodova koristeći orbitne matrice i podmatrice orbitnih matrica slabo samoortogonalnih 1-dizajna s parnim k i parnim presječnim brojevima te generalizacije konstrukcija za samoortogonalne kodove nad poljem $\mathbb{F}_q$.

Metoda konstrukcije binarnih samoortogonalnih kodova koristeći orbitne matrice slabo samoortogonalnih 1-dizajna s parnim k i parnim presječnim brojevima iskazana je sljedećim teoremom čiji dokaz se može pronaći u [17].

Teorem 2.1.10. Neka je $\mathscr{D}$ slabo samoortogonalan 1-dizajn s neparnim k i parnim presječnim brojevima dva različita bloka i neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka dizajna $\mathscr{D}$ u n orbita duljine w i koja djeluje na skup blokova dizajna u orbitama duljina $b_1, b_2, \ldots, b_m$ tako da je $b_i = 2^o \cdot b_i',\ w = 2^u \cdot w',\ o \leq u, 2 \nmid b_i', w'$, za $i \in \{1, \ldots, m\}$. Neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G.

a) Ako je $o = u$, binarni linearni kod razapet retcima matrice $[I_m, O]$ je samoortogonalan kod duljine $m + \frac{v}{w}$ i dimenzije m. Ako je $m = n$, dobiveni kod je samodualan.

b) Ako je $o < u$, binarni linearni kod razapet retcima matrice O je samoortogonalan kod duljine $\frac{v}{w}$.

Teorem 2.1.10 primijenili smo na orbitne matrice slabo samoortogonalnih dizajna konstruiranih iz Mathieuove grupe M_{11}. Orbitne matrice dobivene su obzirom na djelovanje svih cikličkih podgrupa grupe M_{11} prostog reda koje djeluju na skup točaka dizajna bez fiksnih točaka. Dobiveni samoortogonalni kodovi prikazani su u poglavlju 4.1.1 u tablicama 4.10 i 4.11.

Prethodni teorem može se generalizirati kako bi konstruirali samoortogonalne kodove nad poljem $\mathbb{F}_q$, gdje je q potencija prostog broja.

Teorem 2.1.11. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ slabo p-samoortogonalan dizajn za koji je $k \equiv a \pmod{p}$ i $|B_i \cap B_j| \equiv 0 \pmod{p}$, za sve $i, j \in \{1, \ldots, b\},\ i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka dizajna u n orbita duljine w i koja na skup blokova dizajna djeluje u m orbita duljine w. Tada je linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{-a} \cdot I_m, O_p]$, gdje je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G, samoortogonalan

$[m+n,m]$ kod, gdje je $\mathbb{F}=\mathbb{F}_q$ ako je $-a$ kvadrat u $\mathbb{F}_q$ i $\mathbb{F}=\mathbb{F}_{q^2}$ inače. Ako je $m=n$, dobiveni kod je samodualan.

Dokaz. Iz napomene 2.1.1 slijedi da je

$$O_p[s]\cdot O_p[t]=0$$

i

$$O_p[s]\cdot O_p[s]=a$$

za $s,t\in\{1,\ldots,m\},\ s\neq t$.
Neka je $A=[\sqrt{-a}\cdot I_m,O_p]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F}=\mathbb{F}_q$ ako je $-a$ kvadrat u $\mathbb{F}_q$ i $\mathbb{F}=\mathbb{F}_{q^2}$ inače. Zaključujemo da je

$$A[s]\cdot A[t]=0,\ \forall s,t\in\{1,\ldots,m\},$$

pa je linearan kod generiran matricom A samoortogonalan $[m+n,m]$ kod. Ako je $m=n$, dimenzija koda je upola manja od njegove duljine pa je dobiveni kod samodualan.

■

Teorem 2.1.11 primijenili smo na orbitne matrice slabo 3-samoortogonalnih dizajna na 30 točaka konstruiranih iz grupe A_5 na koje ciklička grupa reda 3 djeluje bez fiksnih točaka. Dobiveni samoortogonalni kodovi prikazani su u tablici 4.22.

Metoda konstrukcije binarnih samoortogonalnih kodova koristeći podmatrice orbitne matrice slabo samoortogonalnih 1-dizajna s parnim k i parnim presječnim brojevima iskazana je sljedećim teoremom čiji dokaz se može pronaći u [17].

Teorem 2.1.12. Neka je $\mathscr{D}$ slabo samoortogonalan 1-(v,k,r) dizajn s neparnim k i parnim presječnim brojevima dva različita bloka. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka dizajna sa f_1 fiksnih točaka i n orbita duljine 2 i koja djeluje na skup blokova dizajna sa f_2 fiksnih blokova i m orbita duljine 2. Tada vrijedi sljedeće.

1. Binaran linearan kod razapet retcima matrice $[I_{f_2},OM1]$ je samoortogonalan kod duljine f_2+f_1 i dimenzije f_2.

2. Binaran linearan kod razapet retcima matrice $[I_m,OM2]$ je samoortogonalan kod duljine $m+n$ i dimenzije m. Ako je $m=m$, dobiveni kod je samodualan.

Teorem 2.1.12 primijenili smo na orbitne matrice slabo samoortogonalnih dizajna konstruirane iz grupe M_{11} na koje ciklička grupa reda 2 djeluje s fiksnim točkama. Dobiveni samoortogonalni kodovi prikazani su u poglavlju 4.1.1 u tablici 4.14.

Prethodni teorem može se generalizirati kako bi konstruirali samoortogonalne kodove nad poljem $\mathbb{F}_q$, gdje je q potencija prostog broja.

Teorem 2.1.13. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv a \pmod p$ i $|B_i \cap B_j| \equiv 0 \pmod p$, za sve $i, j \in \{1,\ldots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka od $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$ i koja djeluje na skup blokova sa f_2 fiksnih blokova i m orbita duljine p^α. Tada vrijedi sljedeće.

1. Linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{-a} \cdot I_{f_2}, OM1_p]$ je samoortogonalan $[f_2 + f_1, f_2]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

2. Linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{-a} \cdot I_m, OM2_p]$ je samoortogonalan $[m+n, m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Ako je $m = n$, dobiveni kod je samodualan.

Dokaz.

1. Obzirom da je $k \equiv a \pmod p$, svaki blok sadrži $p \cdot \beta + a$, $\beta \in \mathbb{N}$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv 0 \pmod p$, za sve $i, j \in \{1,\ldots,b\}$, $i \neq j$, presjek svaka dva bloka sadrži $p \cdot \gamma$, $\gamma \in \mathbb{N}$ fiksnih točaka.
   Slijedi da je
   $$OM1_p[s] \cdot OM1_p[s] = a$$
   i
   $$OM1_p[s] \cdot OM1_p[t] = 0$$
   za $s,t \in \{1,\ldots,f_2\}$, $s \neq t$. Neka je $A = [\sqrt{-a} \cdot I_m, OM1_p]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Slijedi da je
   $$A[s] \cdot A[t] = 0, \ \forall s,t \in \{1,\ldots,f_2\},$$
   pa zaključujemo je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan kod duljine $f_2 + f_1$ i dimenzije f_2.

2. Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv p^\alpha \cdot 0 \pmod{p} \equiv 0 \pmod{p}$$

i za $s = t$ slijedi da je

$$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s,\ x \neq x'} |x \cap x'| \equiv a + (p^\alpha - 1) \cdot 0 \pmod{p} \equiv a \pmod{p}.$$

Iz napomene 2.1.1 zaključujemo da je

$$OM2_p[s] \cdot OM2_p[t] = 0$$

i

$$OM2_p[s] \cdot OM2_p[s] = a$$

za $s,t \in \{1,\ldots,m\},\ s \neq t$.

Neka je $A = [\sqrt{-a} \cdot I_m, OM2]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Slijedi da je

$$A[s] \cdot A[t] = 0,\ \forall s,t \in \{1,\ldots,m\},$$

pa zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan kod duljine $m+n$ i dimenzije m. Ako je $m = n$, dimenzija koda je upola manja od njegove duljine pa je dobiveni kod samodualan.

■

Teorem 2.1.13 primijenili smo na orbitne matrice 3−slabo samoortogonalnih dizajna na 1640 točaka konstruiranih iz grupe $S(4,9)$ na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni samoortogonalni kodovi prikazani su u tablici 4.28.

Objasnimo detaljnije primjer iz tablice 4.28.

Primjer 2.1.1. $\mathscr{D}$ je 1-$(1640,2,1)$ dizajn s 820 blokova za koji je $k \equiv 2 \pmod 3$ i za koji su presječni brojevi svaka dva bloka višekratnici broja 3, tj. $|B_i \cap B_j| \equiv 0 \pmod 3$, za sve $i,j \in \{1,\ldots,820\}$, $i \neq j$. Ciklička grupa reda 3 djeluje na skup točaka dizajna $\mathscr{D}$ s 38 fiksnih točaka i 534 orbite duljine 3 te na skup blokova dizajna s 19 fiksnih blokova i 267 orbita duljine 3. Matrice $OM1_3$ i $OM2_3$ su dimenzija redom 19×38 i 267×534. Primjenom teorema 2.1.13, matrice $[I_{19}, OM1_3]$ i $[I_{267}, OM2_3]$ (obzirom da je $\sqrt{-a} = \sqrt{-2} = \sqrt{1} = 1 \in \mathbb{F}_3$) generiraju $[57,19]$ i $[801,267]$ kodove nad poljem $\mathbb{F}_3$ koji su samoortogonalni.

2.1.4. Kodovi iz orbitnih matrica proširenih slabo samoortogonalnih dizajna s neparnim k i neparnim presječnim brojevima dva različita bloka

Opisat ćemo metode konstrukcije binarnih samoortogonalnih kodova koristeći orbitne matrice i podmatrice orbitnih matrica slabo samoortogonalnih 1-dizajna s neparnim k i neparnim presječnim brojevima te generalizacije konstrukcija za samoortogonalne kodove nad poljem $\mathbb{F}_q$ iz slabo p-samoortogonalnih 1-dizajna.

Teorem 2.1.14. Neka je $\mathscr{D}$ slabo samoortogonalan 1-dizajn s neparnim k i neparnim presječnim brojevima dva različita bloka i neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka dizajna $\mathscr{D}$ u n orbita duljine w i koja djeluje na skup blokova dizajna u orbitama duljina $b_1, b_2, \ldots, b_m$ tako da je $b_i = 2^o \cdot b_i',\ w = 2^u \cdot w',\ o \leq u, 2 \nmid b_i', w'$, za $i \in \{1, \ldots, m\}$. Neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G.

a) Ako je $o = u = 0$, binarni linearni kod razapet retcima matrice $[O, \mathbf{1}]$ je samoortogonalan kod duljine $\frac{v}{w} + 1$.

b) Inače, binarni linearni kod razapet retcima matrice O je samoortogonalan kod duljine $\frac{v}{w}$.

Dokaz.

a) Ako je $o = u = 0$, iz napomene 2.1.1 slijedi da je

$$\frac{b_t}{w} O[s] \cdot O[t] \equiv 1 \pmod 2$$

i

$$\frac{b_s}{w} O[s] \cdot O[s] \equiv 1 \pmod 2$$

za sve $s, t \in \{1, \ldots, m\}$. Kako su $w, b_1, \ldots, b_s$ neparni brojevi, slijedi da je $O[s] \cdot O[t] \equiv 1 \pmod 2$ i $O[s] \cdot O[s] \equiv 1 \pmod 2$.

b) Ako je $o = u > 1$, iz napomene 2.1.1 slijedi da je

$$\frac{b_t'}{w'} O[s] \cdot O[t] \equiv 0 \pmod 2$$

za sve $s, t \in \{1, \ldots, m\}$. Kako su $w', b_1', \ldots, b_s'$ neparni brojevi, slijedi da je $O[s] \cdot O[t] \equiv 0 \pmod 2$ i $O[s] \cdot O[s] \equiv 0 \pmod 2$.

Ako je $1 < o < u$, iz napomene 2.1.1 slijedi da je

$$\frac{b_s'}{2^{u-o} \cdot w'} O[s] \cdot O[t] \equiv 0 \pmod 2$$

za sve $s,t \in \{1,\ldots,m\}$ i kako $\frac{b'_s}{2^{u-o}\cdot w'} O[s]\cdot O[t]$ mora biti cijeli broj, slijedi da je $O[s]\cdot O[t] \equiv 0 \pmod 2$ i $O[s]\cdot O[s] \equiv 0 \pmod 2$.

■

Teorem 2.1.14 primijenili smo na orbitne matrice slabo samoortogonalnih dizajna konstruiranih iz Mathieuove grupe M_{11}. Orbitne matrice dobivene su obzirom na djelovanje svih cikličkih podgrupa grupe M_{11} prostog reda koje djeluju na skup točaka dizajna bez fiksnih točaka. Dobiveni samoortogonalni kodovi prikazani su u poglavlju 4.1.1 u tablici 4.12.

Prethodni teorem može se generalizirati kako bi konstruirali samoortogonalne kodove nad poljem $\mathbb{F}_q$, gdje je q potencija prostog broja.

Teorem 2.1.15. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv a \pmod p$ i $|B_i \cap B_j| \equiv d \pmod p$, za sve $i,j \in \{1,\ldots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja na skup točaka dizajna $\mathscr{D}$ djeluje u n orbita duljine w i koja na skup blokova djeluje u m orbita duljine w. Neka je O orbitna matrica dizajna $\mathscr{D}$ za djelovanje grupe G.

- Ako je $a = d$ razlikujemo dva slučaja.

  a) Ako $p \mid w$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom O_p je samoortogonalan kod duljine m.

  b) Ako $p \nmid w$, linearan kod nad poljem $\mathbb{F}$ generiran matricom $[O_p, \sqrt{-w\cdot d}\cdot \mathbf{1}]$ je samoortogonalan kod duljine $m+1$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-w\cdot d$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

- Ako $a \neq d$, razlikujemo dva slučaja.

  a) Ako $p \mid w$, linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{d-a}\cdot I_m, O_p]$ je samoortogonalan $[m+n,m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $d-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Ako je $m = n$, dobiveni kod je samodualan.

  b) Ako $p \mid w-1$, linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{w\cdot d-a}\cdot I_m, O_p, \sqrt{-w\cdot d}\cdot \mathbf{1}]$ je samoortogonalan $[m+n,m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $w\cdot d-a$ i $-w\cdot d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Ako je $m = n$, dobiveni kod je samodualan.

c) Ako $p \nmid w$ i $p \nmid w-1$, linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{d-a}\cdot I_m, O_p, \sqrt{-w\cdot d}\cdot \mathbf{1}]$ je samoortogonalan $[m+n+1, m]$ kod, gdje je $\mathbb{F}=\mathbb{F}_q$ ako su $d-a$ i $-w\cdot d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F}=\mathbb{F}_{q^2}$ inače.

Dokaz.

- Ako je $a=d$, iz napomene 2.1.1 slijedi da je

$$O_p[s]\cdot O_p[t] = w\cdot d,\ \forall s,t\in\{1,\ldots,m\}.$$

Ako $p \mid w$, vidimo da je

$$O_p[s]\cdot O_p[t] = 0,\ \forall s,t\in\{1,\ldots,m\},$$

pa je linearan kod nad poljem $\mathbb{F}_q$ generiran matricom O_p je samoortogonalan kod duljine m.

Neka $p \nmid w$ i neka je $A=[O_p, \sqrt{-w\cdot d}\cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F}=\mathbb{F}_q$ ako je $-w\cdot d$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F}=\mathbb{F}_{q^2}$ inače.

Slijedi da je

$$A[s]\cdot A[t] = 0,\ \forall s,t\in\{1,\ldots,m\},$$

pa zaključujemo je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan kod duljine $m+1$.

- Ako je $a\neq d$, iz napomene 2.1.1, za $s,t\in\{1,\ldots,m\},\ s\neq t$, slijedi da je

$$O_p[s]\cdot O_p[t] = w\cdot d$$

i

$$O_p[s]\cdot O_p[s] = a+(w-1)\cdot d = a+w\cdot d-d.$$

a) Ako $p \mid w$, tada je

$$O_p[s]\cdot O_p[t] = 0$$

i

$$O_p[s]\cdot O_p[s] = a-d.$$

Neka je $A=[\sqrt{d-a}\cdot I_m, O_p]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F}=\mathbb{F}_q$ ako je $d-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F}=\mathbb{F}_{q^2}$ inače. Vidimo da je

$$A[s]\cdot A[t] = 0,\ \forall s,t\in\{1,\ldots,m\},$$

pa zaključujemo je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan $[m+n,m]$ kod. Ako je $m=n$, dimenzija koda je upola manja od njegove duljine pa je dobiveni kod samodualan.

b) Ako $p \mid w-1$, tada je za $s,t \in \{1,\ldots,m\},\ s \neq t$

$$O_p[s] \cdot O_p[t] = w \cdot d$$

i

$$O_p[s] \cdot O_p[s] = a.$$

Neka je $A = [\sqrt{w \cdot d - a} \cdot I_m, O_p, \sqrt{-w \cdot d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $w \cdot d - a$ i $-w \cdot d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Vidimo da je

$$A[s] \cdot A[t] = 0,\ \forall s,t \in \{1,\ldots,m\},$$

pa zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan $[m+n+1,m]$ kod.

c) Neka $p \nmid w$ i $p \nmid w-1$ i neka je $A = [\sqrt{d-a} \cdot I_m, O_p, \sqrt{-w \cdot d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $d-a$ i $-w \cdot d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
Tada je za $s,t \in \{1,\ldots,m\},\ s \neq t$

$$A[s] \cdot A[t] = w \cdot d - w \cdot d = 0$$

i

$$A[s] \cdot A[s] = d - a + a + w \cdot d - d - w \cdot d = 0$$

pa zaključujemo je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan $[m+n+1,m]$ kod.

■

Teorem 2.1.15 primijenili smo na orbitne matrice slabo 3-samoortogonalnih dizajna na 416 točaka konstruiranih iz grupe $U(3,4)$ na koje ciklička grupa reda 13 djeluje bez fiksnih točaka. Dobiveni samoortogonalni kodovi prikazani su u tablici 4.23.

Teorem 2.1.15 primijenili smo i na orbitne matrice slabo 3-samoortogonalnih dizajna na 30 točaka konstruiranih iz grupe A_5 na koje cikličke grupe reda 3 i 5 djeluju bez fiksnih točaka. Dobiveni samoortogonalni kodovi prikazani su u tablici 4.24 i 4.25.

Teorem 2.1.16. Neka je $\mathscr{D}$ slabo samoortogonalan 1-dizajn s neparnim k i neparnim presječnim brojevima dva različita bloka. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka dizajna sa f_1 fiksnih točaka i n orbita duljine 2 i koja djeluje na skup blokova dizajna sa f_2 fiksnih blokova i m orbita duljine 2. Tada vrijedi sljedeće.

1. Binaran linearan kod razapet retcima matrice $[OM1, \mathbf{1}]$ je samoortogonalan kod duljine $f_1 + 1$.

2. Binaran linearan kod razapet retcima matrice $OM2$ je samoortogonalan kod duljine n.

Dokaz.

1. Obzirom da je k neparan, svaki blok sadrži neparan broj fiksnih točaka i obzirom da su presječni brojevi svaka dva različita bloka neparni, presjek svaka dva različita bloka sadrži neparan broj fiksnih točaka. Slijedi da retci matrice $[OM1, \mathbf{1}]$ razapinju binaran samoortogonalan kod duljine $f_1 + 1$.

2. Neka su $\mathscr{B}_t$ i $\mathscr{B}_s$ orbite duljine 2 za djelovanje grupe G na skup blokova dizajna $\mathscr{D}$. Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine 2, iz napomene 1.2.32 slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv 2 \pmod 2 \equiv 0 \pmod 2$$

   i za $s = t$, slijedi da je

$$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s,\ x \neq x'} |x \cap x'| \equiv 1 + 1 \pmod 2.$$

   Zaključujemo da je $\sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{t,j} \equiv 0 \pmod 2$, za $s \neq t$ i $\sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{s,j} \equiv 0 \pmod 2$ te da je binarni kod razapet retcima matrice $OM2$ samoortogonalan.

■

Prethodni teorem može se generalizirati kako bi konstruirali samoortogonalne kodove nad poljem $\mathbb{F}_q$, gdje je q potencija prostog broja.

Teorem 2.1.17. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv a \pmod p$ i $|B_i \cap B_j| \equiv d \pmod p$, za sve $i, j \in \{1, \ldots, b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka od $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$, i koja djeluje na skup blokova sa f_2 fiksnih blokova i m orbita duljine p^α. Tada vrijedi sljedeće.

- Ako je $a = d$, razlikujemo dva slučaja.

  1. Linearan kod nad poljem $\mathbb{F}$ generiran matricom $[OM1_p, \sqrt{-a} \cdot \mathbf{1}]$ je samoortogonalan kod duljine $f_1 + 1$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
  2. Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM2_p$ je samoortogonalan kod duljine n.

- Ako je $a \neq d$, razlikujemo dva slučaja.

  1. Linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{d-a} \cdot I_{f_2}, OM1_p, \sqrt{-d} \cdot \mathbf{1}]$ je samoortogonalan $[f_2 + f_1 + 1, f_2]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako su $d-a$ i $-d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
  2. Linearan kod nad poljem $\mathbb{F}$ generiran matricom $[\sqrt{d-a} \cdot I_m, OM2_p]$ je samoortogonalan $[m+n, m]$ kod, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $d-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Ako je $m = n$, dobiveni kod je samodualan.

Dokaz.

1. Obzirom da je $k \equiv a \pmod{p}$, svaki blok sadrži $p \cdot \beta + a,\ \beta \in \mathbb{N}$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv d \pmod{p}$, za sve $i, j \in \{1, \ldots, b\},\ i \neq j$, presjek svaka dva bloka sadrži $p \cdot \gamma + d,\ \gamma \in \mathbb{N}$ fiksnih točaka.
   Tada je za $s, t \in \{1, \ldots, f_2\},\ s \neq t$,

   $$OM1_p[s] \cdot OM1_p[s] = a$$

   i

   $$OM1_p[s] \cdot OM1_p[t] = d.$$

   Neka je $a = d$ i neka je $A = [OM1_p, \sqrt{-a} \cdot \mathbf{1}]$ matrica $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.
   Slijedi da je

   $$A[s] \cdot A[t] = 0,\ \forall s, t \in \{1, \ldots, f_2\},$$

   pa zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan kod duljine $f_1 + 1$.
   Neka je $a \neq d$ i neka je $A = [\sqrt{d-a} \cdot I_{f_2}, OM1, \sqrt{-d} \cdot \mathbf{1}]$ matrica nad poljem $\mathbb{F}$, gdje je

$\mathbb{F} = \mathbb{F}_q$ ako su $d-a$ i $-d$ kvadrati u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače.

Slijedi da je

$$A[s] \cdot A[t] = 0, \ \forall s,t \in \{1,\ldots,f_2\},$$

pa zaključujemo da retci matrice A razapinju samoortogonalan $[f_2+f_1+1, f_2]$ kod nad poljem $\mathbb{F}$.

2. Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv p^\alpha \cdot d \pmod{p} \equiv 0 \pmod{p}$$

i za $s = t$ slijedi da je

$$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s, \ x \neq x'} |x \cap x'| \equiv a + (p^\alpha - 1) \cdot d \pmod{p} \equiv a - d \pmod{p}.$$

Zaključujemo da je za $s,t \in \{1,\ldots,m\}, \ s \neq t$,

$$OM2_p[s] \cdot OM2_p[t] = 0$$

i

$$OM2_p[s] \cdot OM2_p[s] = a - d.$$

Ako je $a = d$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM2_p$ je samoortogonalan kod duljine n.

Neka je $a \neq d$ i neka je $A = [\sqrt{d-a} \cdot I_m, OM2_p]$ matrica nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{F}_q$ ako je $d-a$ kvadrat u polju $\mathbb{F}_q$ i $\mathbb{F} = \mathbb{F}_{q^2}$ inače. Slijedi da je

$$A[s] \cdot A[t] = 0, \ \forall s,t \in \{1,\ldots,m\},$$

pa zaključujemo da je linearan kod nad poljem $\mathbb{F}$ generiran matricom A samoortogonalan $[m+n, n]$ kod. Ako je $m = n$, dimenzija koda je upola manja od njegove duljine pa je dobiveni kod samodualan.

■

Teorem 2.1.17 primijenili smo na orbitne matrice slabo 3-samoortogonalnih dizajna na 364 točke konstruiranih iz grupe $O(7,3)$ na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni samoortogonalni kodovi prikazani su u tablici 4.29.

3. LCD KODOVI IZ SLABO p-SAMOORTOGONALNIH DIZAJNA

U ovom poglavlju opisat ćemo metodu konstrukcije LCD kodova nad konačnim poljem $\mathbb{F}_q$ iz slabo p-samoortogonalnih dizajna. Koristit ćemo proširenja matrice incidencije, orbitnih matrica i podmatrica orbitnih matrica slabo p-samoortogonalnih dizajna kako bismo generirali LCD kod. Cilj je modificirati uvedene algoritme za konstrukciju samoorotogonalnih kodova kako bi se konstruirali LCD kodovi iz slabo p-samoortogonalnih dizajna.

Lema 3.0.1. Neka su a i d elementi konačnog polja $\mathbb{F}_q$, gdje je $q = p^t$ potencija prostog broja. Tada je

$$\det \begin{bmatrix} a & d & \cdots & d \\ d & a & \cdots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & \cdots & a \end{bmatrix} = (a-d)^{n-1}[a+(n-1)d],$$

gdje je n red navedene matrice.

Dokaz. Indukcijom. Tvrdnja očito vrijedi za $n = 2$. Pretpostavimo da tvrdnja vrijedi za svaki prirodni broj $k < n$. Slijedi da je

$$\begin{vmatrix} a & d & d & \cdots & d \\ d & a & d & \cdots & d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d & d & d & \cdots & a \end{vmatrix}_{n\times n} = a \begin{vmatrix} a & d & \cdots & d \\ d & a & \cdots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & \cdots & a \end{vmatrix}_{(n-1)\times(n-1)} - d \begin{vmatrix} d & d & \cdots & d \\ d & a & \cdots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & \cdots & a \end{vmatrix}_{(n-1)\times(n-1)} +$$

$$
\begin{aligned}
&+d\begin{vmatrix} d & a & d & \cdots & d \\ d & d & d & \cdots & d \\ d & d & a & \cdots & d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d & d & d & \cdots & a \end{vmatrix}_{(n-1)\times(n-1)} + \ldots + (-1)^{n-1} d \begin{vmatrix} a & d & \cdots & d \\ d & a & \cdots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & \cdots & a \\ d & d & \cdots & d \end{vmatrix}_{(n-1)\times(n-1)} \\
&= a(a-d)^{n-2} \cdot [a+(n-2)d] - (n-1)d \begin{vmatrix} d & d & \cdots & d \\ d & a & \cdots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & \cdots & a \end{vmatrix}_{(n-1)\times(n-1)} \\
&= a(a-d)^{n-2} \cdot [a+(n-2)d] - (n-1)d \begin{vmatrix} d & d & \cdots & d \\ 0 & a-d & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a-d \end{vmatrix}_{(n-1)\times(n-1)} \\
&= a(a-d)^{n-2} \cdot [a+(n-2)d] - (n-1)d^2 \begin{vmatrix} a-d & 0 & \cdots & 0 \\ 0 & a-d & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a-d \end{vmatrix}_{(n-2)\times(n-2)} \\
&= a(a-d)^{n-2}[a+(n-2)d] - (n-1)d^2(a-d)^{n-2} \\
&= (a-d)^{n-2}\left[a+(n-2)d - d^2(n-1)\right] \\
&= (a-d)^{n-2}[(a-d)(a+dn-d)] \\
&= (a-d)^{n-1}[a+(n-1)d].
\end{aligned}
$$

■

Napomena 3.0.2. Neka je M $b \times v$ matrica incidencije 1-dizajna $\mathscr{D}$ s parametrima 1-(v,k,λ) i b blokova $x_1,...,x_b$. Označimo sa $B_{i,j}$ veličinu presjeka blokova x_i i x_j, za $i,j \in \{1,...,b\}$.

1. $M \cdot M^T = \begin{bmatrix} B_{1,1} & B_{1,2} & \cdots & B_{1,b} \\ B_{2,1} & B_{2,2} & \cdots & B_{2,b} \\ \vdots & \vdots & \ddots & \vdots \\ B_{b,1} & B_{b,2} & \cdots & B_{b,b} \end{bmatrix}$

2. $[M, x\cdot I_b]\cdot[M, x\cdot I_b]^T = \begin{bmatrix} B_{1,1}+x^2 & B_{1,2} & \cdots & B_{1,b} \\ B_{2,1} & B_{2,2}+x^2 & \cdots & B_{2,b} \\ \vdots & \vdots & \ddots & \vdots \\ B_{b,1} & B_{b,2} & \cdots & B_{b,b}+x^2 \end{bmatrix}$

3. $[M, y\cdot \mathbf{1}]\cdot[M, y\cdot \mathbf{1}]^T = \begin{bmatrix} B_{1,1}+y^2 & B_{1,2}+y^2 & \cdots & B_{1,b}+y^2 \\ B_{2,1}+y^2 & B_{2,2}+y^2 & \cdots & B_{2,b}+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ B_{b,1}+y^2 & B_{b,2}+y^2 & \cdots & B_{b,b}+y^2 \end{bmatrix}$

4. $[M, x\cdot I_b, y\cdot \mathbf{1}]\cdot[M, x\cdot I_b, y\cdot \mathbf{1}]^T = \begin{bmatrix} B_{1,1}+x^2+y^2 & B_{1,2}+y^2 & \cdots & B_{1,b}+y^2 \\ B_{2,1}+y^2 & B_{2,2}+x^2+y^2 & \cdots & B_{2,b}+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ B_{b,1}+y^2 & B_{b,2}+y^2 & \cdots & B_{b,b}+x^2+y^2 \end{bmatrix}$

Korolar 3.0.3. Neka je $q = p^l$ potencija prostog broja i neka je M $b \times v$ matrica incidencije p-samoortogonalnog 1-dizajna za kojeg je $k \equiv a \pmod p$ i $B_{i,j} \equiv d \pmod p$[1] te neka su x i y elementi polja $\mathbb{F}_q$. Neka je I_b jedinična matrica nad promatranim poljem i neka je $\mathbf{1}$ stupčana matrica čiji svi elementi su 1 u promatranom polju. Tada je:

1. $\det(M_p \cdot M_p^T) = (a-d)^{b-1}[a+(b-1)\cdot d]$,
2. $\det([M_p, x\cdot I_b]\cdot[M_p, x\cdot I_b]^T) = (a-d+x^2)^{b-1}[a+(b-1)\cdot d+x^2]$,
3. $\det([M_p, y\cdot \mathbf{1}]\cdot[M_p, y\cdot \mathbf{1}]^T) = (a-d)^{b-1}[a+(b-1)\cdot d+b\cdot y^2]$,
4. $\det([M_p, x\cdot I_b, y\cdot \mathbf{1}]\cdot[M_p, x\cdot I_b, y\cdot \mathbf{1}]^T) = (a-d+x^2)^{b-1}[a+(b-1)\cdot d+x^2+b\cdot y^2]$.

Dokaz. Direktno iz leme 3.0.1 i napomene 3.0.2.

■

Napomena. U daljnjem tekstu ćemo koristiti oznake I_b za jediničnu matricu nad promatranim poljem i $\mathbf{1}$ za stupčanu matrica čiji svi elementi su 1 u promatranom polju.

Iz činjenice da je matrica M generirajuća matrica LCD koda nad poljem $\mathbb{F}_q$ ako i samo ako je M punog ranga i ako je $\det(M_p \cdot M_p^T) \neq 0$ zaključujemo sljedeće.

[1] a i b su elementi polja $\mathbb{F}_p \hookrightarrow \mathbb{F}_q$

Teorem 3.0.4. Neka je $q = p^l$ potencija prostog broja i neka je M $b \times v$ matrica incidencije p-samoortogonalnog 1-dizajna za kojeg je $k \equiv a \pmod{p}$ i $B_{i,j} \equiv d \pmod{p}$ te neka su x i y nenula elementi polja $\mathbb{F}_q$.

1. Ako je $a = d = 0$, tada

   (a) matrica $[M, x \cdot I_b]$ i

   (b) matrica $[M, x \cdot I_b, y \cdot \mathbf{1}]$ za $x^2 + b \cdot y^2 \neq 0$

   generiraju LCD kod nad poljem $\mathbb{F}_q$.

2. Ako je $a = 0$ i $d \neq 0$ tada

   (a) ako je M punog ranga, matrica M,

   (b) matrica $[M, x \cdot I_b]$ za $x^2 - d \neq 0$ i $x^2 + (b-1) \cdot d \neq 0$,

   (c) ako je M punog ranga, matrica $[M, y \cdot \mathbf{1}]$ za $b \cdot y^2 + (b-1) \cdot d \neq 0$ i

   (d) matrica $[M, x \cdot I_b, y \cdot \mathbf{1}]$ za $x^2 - d \neq 0$ i $x^2 + b \cdot y^2 + (b-1) \cdot d \neq 0$

   generiraju LCD kod nad poljem $\mathbb{F}_q$.

3. Ako je $a \neq 0$ i $d = 0$ tada

   (a) ako je M punog ranga, matrica M,

   (b) matrica $[M, x \cdot I_b]$ za $x^2 + a \neq 0$,

   (c) ako je M punog ranga, matrica $[M, y \cdot \mathbf{1}]$ za $b \cdot y^2 + a \neq 0$,

   (d) matrica $[M, x \cdot I_b, y \cdot \mathbf{1}]$ za $x^2 + a \neq 0$ i $x^2 + b \cdot y^2 + a \neq 0$

   generiraju LCD kod nad poljem $\mathbb{F}_q$.

4. Ako je $a = d \neq 0$ tada

   (a) matrica $[M, x \cdot I_b]$ za $x^2 + ba \neq 0$ i

   (b) matrica $[M, x \cdot I_b, y \cdot \mathbf{1}]$ za $x^2 + b \cdot y^2 + b \cdot a \neq 0$

   generiraju LCD kod nad poljem $\mathbb{F}_q$.

5. Ako je $a \neq 0$, $d \neq 0$ i $a \neq d$ tada

(a) ako je M punog ranga, matrica M za $a+(b-1)\cdot d \neq 0$,

(b) matrica $[M, x\cdot I_b]$ za $x^2+a-d \neq 0$ i $x^2+a+(b-1)\cdot d \neq 0$,

(c) ako je M punog ranga, matrica $[M, y\cdot \mathbf{1}]$ za $b\cdot y^2+a+(b-1)\cdot d \neq 0$ i

(d) matrica $[M, x\cdot I_b, y\cdot \mathbf{1}]$ za $x^2+a-d \neq 0$ i $x^2+b\cdot y^2+a+(b-1)\cdot d \neq 0$,

generiraju LCD kod nad poljem $\mathbb{F}_q$.

Teorem 3.0.4 primijenili smo na slabo samoortogonalne dizajne konstruirane iz grupe A_5. Dobiveni binarni LCD kodovi prikazani su u tablicama 4.30, 4.31, 4.32, 4.35, 4.36, 4.37, 4.33, 4.34, 4.38, 4.39, 4.40, 4.41, 4.42, 4.43.

Primjenom gornjeg teorema možemo iz slabo samoortogonalnih dizajna konstruirati LCD kodove na sljedeći način.

1. Neka je M $b\times v$ matrica incidencije slabo samoortogonalnog 1-dizajna $\mathscr{D}$ s parametrima 1-(v,k,λ) i b blokova takvog da je M punog ranga, k je neparan i presječni brojevi dva različita bloka su parni. Tada M generira binarni LCD $[v,b]$-kod.

2. Neka je M $b\times v$ matrica incidencije slabo samoortogonalnog 1-dizajna $\mathscr{D}$ s parametrima 1-(v,k,λ) i b blokova takvog da je M punog ranga, k je paran i presječni brojevi dva različita bloka su neparni. Tada $[M,\mathbf{1}]$ generira binarni LCD $[v+1,b]$-kod.

3. Neka je M $b\times v$ matrica incidencije slabo samoortogonalnog 1-dizajna $\mathscr{D}$ s parametrima 1-(v,k,λ) i b blokova takvog da je k paran i presječni brojevi dva različita bloka su parni. Tada $[M,I_b]$ generira binarni LCD $[2v,b]$-kod.

4. Neka je M $b\times v$ matrica incidencije slabo samoortogonalnog 1-dizajna $\mathscr{D}$ s parametrima 1-(v,k,λ) i b blokova takvog da je k neparan i presječni brojevi dva različita bloka su neparni. Tada $[M,I_b,\mathbf{1}]$ generira binarni LCD $[2v+1,b]$-kod.

Uočimo da ako M nije punog ranga u slučajevima 1. ili 2., možemo definirati matricu M' tako da uzmemo maksimalan linearno nezavisan skup vektora redaka matrice M za retke matrice M'. Matricu M' možemo proširiti na gore opisan način kako bi generirali binarni LCD kod.

Napomena 3.0.5. Svaki t-dizajn je ujedno i 1-dizajn te u skladu s tim zaključujemo sljedeće.

1. Neka je $\mathscr{D}$ simetričan (v,k,λ) dizajn i neka je M njegova matrica incidencije.

(a) Ako je M punog ranga te ako je k neparan i λ paran, tada matrice M i M^T generiraju binarni LCD $[v,v]$-kod.

(b) Ako je M punog ranga te ako je k paran i λ neparan, tada matrice $[M,\mathbf{1}]$ i $[M^T,\mathbf{1}]$ generiraju binarni LCD $[v+1,v]$-kod.

(c) Ako su k i λ parni, tada matrice $[M,I_v]$ i $[M^T,I_v]$ generiraju binarni LCD $[2v,v]$-kod.

(d) Ako su k i λ neparni, tada matrice $[M,I_v,\mathbf{1}]$ i $[M^T,I_v,\mathbf{1}]$ generiraju binarni LCD $[2v+1,v]$-kod.

2. Neka je $\mathscr{D}$ 2-(v,k,λ) dizajn te neka je M njegova matrica incidencije.

(a) Ako je M punog ranga te ako je k neparan i λ paran, matrica M^T generira binarni LCD $[b,v]$-kod.

(b) Ako je M punog ranga te ako je k paran i λ neparan, tada matrica $[M^T,\mathbf{1}]$ generira binarni LCD $[b+1,v]$-kod.

(c) Ako su k i λ parni, tada matrica $[M^T,I_v]$ generira binarni LCD $[b+v,v]$-kod.

(d) Ako su k i λ neparni, tada matrica $[M^T,I_v,\mathbf{1}]$ generira binarni LCD $[b+v+1,v]$-kod.

3. Neka je $\mathscr{G}$ jako regularan graf s parametrima (v,k,λ,μ) te neka je A njegova matrica susjedstva.

(a) Ako je A punog ranga, k neparan i λ i μ parni, matrica A generira binarni LCD $[v,v]$-kod.

(b) Ako je A punog ranga, k paran i λ i μ neparni, matrica $[A,\mathbf{1}]$ generira binarni LCD $[v+1,v]$-kod.

(c) Ako su k, λ i μ parni, matrica $[A,I_v]$ generira binarni LCD $[2v,v]$-kod.

(d) Ako su k, λ i μ neparni, matrica $[A,I_v,\mathbf{1}]$ generira binarni LCD $[2v+1,v]$-kod.

Koristeći napomenu 3.0.5, konstruirali smo LCD kodove iz kvazisimetričnih dizajna preuzetih iz [34] za koje presječni brojevi daju isti ostatak pri dijeljenju s 2. Iz istih dizajna konstruirali smo jako regularne grafove (1.3.8) kao blokovne grafove dizajna i koristeći matricu susjedstva

pripadnih grafova, LCD kodove. Dobiveni kodovi prikazani su u tablici 4.44.

3.1. LCD KODOVI IZ ORBITNIH MATRICA

Opisat ćemo konstrukciju LCD kodova koristeći orbitne matrice i podmatrice orbitnih matrica slabo p-samoortogogalnih dizajna.

3.1.1. LCD kodovi iz orbitnih matrica slabo p-samoortogonalnih dizajna

Teorem 3.1.1. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,λ) dizajn za koji je $k \equiv 0 \pmod{p}$ i $|B_i \cap B_j| \equiv 0 \pmod{p}$, $\forall i,j \in \{1,\ldots,b\}, i \neq j$, gdje su B_i, B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja na skup točaka dizajna $\mathscr{D}$ djeluje u n orbita duljine w i koja na skup blokova dizajna $\mathscr{D}$ djeluje u m orbita duljine w te neka je O $m \times n$ orbitna matrica za djelovanje grupe G. Tada vrijedi sljedeće.

1. Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x \cdot I_m]$, za $x \neq 0$, je LCD kod.
2. Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x \cdot I_m, y \cdot \mathbf{1}]$, za $x \neq 0$ i $x^2 + m \cdot y^2 \neq 0$ je LCD kod.

Dokaz. Iz napomene 2.1.1 slijedi da je $O_p[s] \cdot O_p[t] = 0$ i $O_p[s] \cdot O_p[s] = 0$. Iz leme 3.0.1 slijedi da je

$$\det(O_p \cdot O_p^T) = \begin{vmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{vmatrix}_{m \times m} = 0,$$

$$\det([O_p, x \cdot I] \cdot [O_p, x \cdot I]^T) = \begin{vmatrix} x^2 & 0 & \ldots & 0 \\ 0 & x^2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x^2 \end{vmatrix}_{m \times m} = x^{2m},$$

$$\det([O_p, y\cdot\mathbf{1}]\cdot[O_p, y\cdot\mathbf{1}]^T) = \begin{vmatrix} y^2 & y^2 & \dots & y^2 \\ y^2 & y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & y^2 \end{vmatrix}_{m\times m} = 0,$$

$$\det([O_p, x\cdot I_m, y\cdot\mathbf{1}]\cdot[O_p, x\cdot I_m, y\cdot\mathbf{1}]^T) = \begin{vmatrix} x^2+y^2 & y^2 & \dots & y^2 \\ y^2 & x^2+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2 \end{vmatrix}_{m\times m}$$
$$= x^{2m-2}(x^2+m\cdot y^2).$$

Vidimo da matrice O_p i $[O_p, y\cdot\mathbf{1}]$ ne generiraju LCD kod, a promatrajući kada su preostale dvije determinante različite od 0, slijedi tvrdnja teorema.

■

Teorem 3.1.1 primijenili smo na orbitne matrice slabo 3-samoortogonalnih dizajne iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 5 djeluje bez fiksnih točaka. Dobiveni LCD kodovi prikazani su u tablici 4.45.

Teorem 3.1.2. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,λ) dizajn za koji je $k \equiv 0 \pmod p$ i $|B_i \cap B_j| \equiv d \pmod p$, $\forall i,j \in \{1,\dots,b\}, i \neq j$, gdje su B_i, B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja na skup točaka dizajna $\mathscr{D}$ djeluje u n orbita duljine w i koja na skup blokova dizajna $\mathscr{D}$ djeluje u m orbita duljine w te neka je O $m\times n$ orbitna matrica za djelovanje grupe G. Neka su x i y nenula elementi polja $\mathbb{F}_q$.

1. Ako je $mw-1 \neq 0$ i ako je O_p punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom O_p je LCD kod.

2. Ako je $x^2-d \neq 0$ i $x^2-d+mw\cdot d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x\cdot I]$ je LCD kod.

3. Ako je $m\cdot y^2-d+mw\cdot d \neq 0$ i ako je O_p matrica punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, y\cdot\mathbf{1}]$ je LCD kod.

4. Ako je $x^2-d\neq 0$ i $x^2+m\cdot y^2+d-mw\cdot d\neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x\cdot I_m, y\cdot \mathbf{1}]$ je LCD kod.

Dokaz. Iz napomene 2.1.1 slijedi da je $\forall s,t\in\{1,\ldots,m\},\ s\neq t$,

$$O_p[s]\cdot O_p[t]=w\cdot d$$

i

$$O_p[s]\cdot O_p[s]=(w-1)\cdot d.$$

Tada je

$$O_p\cdot O_p^T=\begin{bmatrix}(w-1)\cdot d & w\cdot d & \ldots & w\cdot d\\ w\cdot d & (w-1)\cdot d & \ldots & w\cdot d\\ \vdots & \vdots & \ddots & \vdots\\ w\cdot d & w\cdot d & \ldots & (w-1)\cdot d\end{bmatrix}_{m\times m}.$$

Iz leme 3.0.1 slijedi da je

$$\begin{aligned}\det(O_p\cdot O_p^T)&=(w\cdot d-d-w\cdot d)^{m-1}[w\cdot d-d+(m-1)w\cdot d]\\&=(-d)^{m-1}(w\cdot d-d+mw\cdot d-w\cdot d)\\&=(-1)^{m-1}\cdot d^m\cdot(1-mw).\end{aligned}$$

Tada je $\det(O_p\cdot O_p^T)\neq 0$ za $1-mw\neq 0$. Zaključujemo da ako je matrica O_p punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom O_p je LCD kod.

Dalje, iz leme 3.0.1 slijedi da je

$$\begin{aligned}\det([O_p,x\cdot I]\cdot[O_p,x\cdot I]^T)&=\begin{vmatrix}(w-1)\cdot d+x^2 & w\cdot d & \ldots & w\cdot d\\ w\cdot d & (w-1)\cdot d+x^2 & \ldots & w\cdot d\\ \vdots & \vdots & \ddots & \vdots\\ w\cdot d & w\cdot d & \ldots & (w-1)\cdot d+x^2\end{vmatrix}_{m\times m}\\&=(w\cdot d-d+x^2)^{m-1}[w\cdot d-d+x^2+(m-1)w\cdot d]\\&=(x^2-d)^{m-1}(w\cdot d-d+x^2+mw\cdot d-w\cdot d)\\&=(x^2-d)^{m-1}(x^2-d+mw\cdot d).\end{aligned}$$

Uočimo da je $\det([O_p,x\cdot I]\cdot[O_p,x\cdot I]^T)\neq 0$ za $x^2-d\neq 0$ i $x^2-d+mw\cdot d\neq 0$.

Zatim, iz leme 3.0.1 slijedi da je

$$\begin{aligned}\det([O_p, y\cdot\mathbf{1}]\cdot[O_p, y\cdot\mathbf{1}]^T) &= \begin{vmatrix} (w-1)\cdot d+y^2 & w\cdot d+y^2 & \dots & w\cdot d+y^2 \\ w\cdot d+y^2 & (w-1)\cdot d+y^2 & \dots & w\cdot d+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ w\cdot d+y^2 & w\cdot d+y^2 & \dots & (w-1)\cdot d+y^2 \end{vmatrix}_{m\times m} \\ &= (w\cdot d-d+y^2-w\cdot d-y^2)^{m-1}[w\cdot d-d+y^2+(m-1)(pd+y^2)] \\ &= (-d)^{m-1}(mw\cdot d+m\cdot y^2-d).\end{aligned}$$

Uočimo da je $\det([O_p, y\cdot\mathbf{1}]\cdot[O_p, y\cdot\mathbf{1}]^T)\neq 0$ za $m\cdot y^2-d+mw\cdot d\neq 0$. Dodatno, ako je O_p punog ranga, zaključujemo da je linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, y\cdot\mathbf{1}]$ LCD kod.

Također, iz leme 3.0.1 slijedi da je

$$\begin{aligned}&\det([O_p, x\cdot I_m, y\cdot\mathbf{1}]\cdot[O_p, x\cdot I_m, y\cdot\mathbf{1}]^T) = \\ &= \begin{vmatrix} (w-1)\cdot d+x^2+y^2 & w\cdot d+y^2 & \dots & w\cdot d+y^2 \\ w\cdot d+y^2 & (w-1)\cdot d+x^2+y^2 & \dots & w\cdot d+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ w\cdot d+y^2 & w\cdot d+y^2 & \dots & (w-1)\cdot d+x^2+y^2 \end{vmatrix}_{m\times m} \\ &= (w\cdot d-d+x^2+y^2-w\cdot d-y^2)^{m-1}[w\cdot d-d+x^2+y^2+(m-1)(w\cdot d+y^2)] \\ &= (x^2-d)^{m-1}(x^2+m\cdot y^2+mw\cdot d-d).\end{aligned}$$

Uočimo da je $\det([O_p, x\cdot I_m, y\cdot\mathbf{1}]\cdot[O_p, x\cdot I_m, y\cdot\mathbf{1}]^T)\neq 0$ za $x^2-d\neq 0$ i $x^2+m\cdot y^2-mw\cdot d+d\neq 0$. Zaključujemo da je linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x\cdot I_m, y\cdot\mathbf{1}]$ LCD kod.

■

Teorem 3.1.2 primijenili smo na orbitne matrice slabo 3-samoortogonalne dizajne iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 5 djeluje bez fiksnih točaka. Dobiveni LCD kodovi prikazani su u tablici 4.46.

Teorem 3.1.3. Neka je $q=p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,λ) dizajn za koji je $k\equiv a \pmod p$ i $|B_i\cap B_j|\equiv 0 \pmod p$, $\forall i,j\in\{1,\dots,b\}, i\neq j$, gdje su B_i, B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja na skup točaka dizajna $\mathscr{D}$ djeluje u n orbita duljine w i koja na skup blokova dizajna $\mathscr{D}$ djeluje u m orbita duljine

w te neka je O $m \times n$ orbitna matrica za djelovanje grupe G. Neka su x i y nenula elementi polja $\mathbb{F}_q$. Tada vrijedi sljedeće.

1. Ako je O_p punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom O_p je LCD kod.
2. Ako je $x^2 + a \neq 0$, tada je linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x \cdot I_m]$ LCD kod.
3. Ako je $m \cdot y^2 + a \neq 0$ i ako je O_p punog ranga, tada je linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, y \cdot \mathbf{1}]$ LCD kod.
4. Ako je $x^2 + a \neq 0$ i $x^2 + a + m \cdot y^2 \neq 0$, tada je linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x \cdot I_m, y \cdot \mathbf{1}]$ LCD kod.

Dokaz. Iz napomene 2.1.1 slijedi da je $\forall s,t \in \{1, \ldots m\},\ s \neq t$,

$$O_p[s] \cdot O_p[t] = 0$$

i

$$O_p[s] \cdot O_p[s] = a.$$

Iz leme 3.0.1 slijedi da je

$$\det(O_p \cdot O_p^T) = \begin{vmatrix} a & 0 & \ldots & 0 \\ 0 & a & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a \end{vmatrix}_{m \times m} = a^m,$$

$$\det([O_p, x \cdot I] \cdot [O_p, x \cdot I]^T) = \begin{vmatrix} a + x^2 & 0 & \ldots & 0 \\ 0 & a + x^2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a + x^2 \end{vmatrix}_{m \times m} = (a + x^2)^m,$$

$$\det([O_p, y \cdot \mathbf{1}] \cdot [O_p, y \cdot \mathbf{1}]^T) = \begin{vmatrix} a + y^2 & y^2 & \ldots & y^2 \\ y^2 & a + y^2 & \ldots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \ldots & a + y^2 \end{vmatrix}_{m \times m} = a^{m-1}(a + m \cdot y^2),$$

$$\det([O_p, x\cdot I_m, y\cdot \mathbf{1}]\cdot[O_p, x\cdot I_m, y\cdot \mathbf{1}]^T) = \begin{vmatrix} a+x^2+y^2 & y^2 & \dots & y^2 \\ y^2 & a+x^2+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & a+x^2+y^2 \end{vmatrix}_{m\times m}$$
$$= (a+x^2)^{m-1}(a+x^2+m\cdot y^2).$$

Promatrajući kada su navedene determinante različite od 0, slijedi tvrdnja teorema.

■

Teorem 3.1.3 primijenili smo na orbitne matrice slabo 3-samoortogonalne dizajne iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 5 djeluje bez fiksnih točaka. Dobiveni LCD kodovi prikazani su u tablici 4.47.

Teorem 3.1.4. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,λ) dizajn za koji je $k \equiv a \pmod p$ i $|B_i \cap B_j| \equiv d \pmod p$, $\forall i,j \in \{1,\dots,b\}, i \neq j$, gdje su B_i, B_j blokovi dizajna $\mathscr{D}$. Neka je G grupa automorfizama dizajna $\mathscr{D}$ koja na skup točaka dizajna $\mathscr{D}$ djeluje u n orbita duljine w i koja na skup blokova dizajna $\mathscr{D}$ djeluje u m orbita duljine w te neka je O $m\times n$ orbitna matrica za djelovanje grupe G. Neka su x i y nenula elementi polja $\mathbb{F}_q$. Tada vrijedi sljedeće.

1. Ako je $a = d$, tada vrijedi sljedeće.
   - Ako je $x^2 + mw\cdot d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x\cdot I]$ je LCD kod.
   - Ako je $x^2 + m\cdot y^2 + mw\cdot d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x\cdot I_m, y\cdot \mathbf{1}]$ je LCD kod.
2. Ako je $a \neq d$, tada vrijedi sljedeće.
   - Ako je $d - a - mw\cdot d \neq 0$ i ako je O_p punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom O_p je LCD kod.
   - Ako je $x^2 - d + a \neq 0$ i $x^2 + mw\cdot d - d + a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x\cdot I]$ je LCD kod.

- Ako je $mw \cdot d + m \cdot y^2 - d + a \neq 0$ i ako je O_p punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, y \cdot \mathbf{1}]$ je LCD kod.
- Ako je $x^2 - d + a \neq 0$ i $x^2 + mw \cdot d + m \cdot y^2 - d + a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[O_p, x \cdot I_m, y \cdot \mathbf{1}]$ je LCD kod.

Dokaz.

1. Iz napomene 2.1.1 slijedi da je $\forall s,t \in \{1,\dots m\},\ s \neq t$,

$$O_p[s] \cdot O_p[t] = w \cdot d$$

i

$$O_p[s] \cdot O_p[s] = w \cdot d.$$

Koristeći lemu 3.0.1, lako se vidi da je $\det(O_p \cdot O_p^T) = 0$ i $\det([O_p, y \cdot \mathbf{1}] \cdot [O_p, y \cdot \mathbf{1}]^T) = 0$, $\forall y \in \mathbb{F}_q$. Nadalje, vidimo da je

$$\begin{aligned}\det([O_p, x \cdot I] \cdot [O_p, x \cdot I]^T) &= \begin{vmatrix} w \cdot d + x^2 & w \cdot d & \dots & w \cdot d \\ w \cdot d & w \cdot d + x^2 & \dots & w \cdot d \\ \vdots & \vdots & \ddots & \vdots \\ w \cdot d & w \cdot d & \dots & w \cdot d + x^2 \end{vmatrix} \\ &= x^{2m-2}(x^2 + mw \cdot d),\end{aligned}$$

$$\begin{aligned}\det([O_p, x \cdot I_m, y \cdot \mathbf{1}] \cdot [O_p, x \cdot I_m, y \cdot \mathbf{1}]^T) &= \begin{vmatrix} w \cdot d + x^2 + y^2 & w \cdot d + y^2 & \dots & w \cdot d + y^2 \\ w \cdot d & w \cdot d + x^2 + y^2 & \dots & w \cdot d + y^2 \\ \vdots & \vdots & \ddots & \vdots \\ w \cdot d + y^2 & w \cdot d + y^2 & \dots & w \cdot d + x^2 + y^2 \end{vmatrix} \\ &= x^{2m-2}(x^2 + m \cdot y^2 + mw \cdot d).\end{aligned}$$

Promatranjem kada su navedene determinante različite od nule slijedi tvrdnja teorema.

2. Iz napomene 2.1.1 slijedi da je $\forall s,t \in \{1,\dots m\},\ s \neq t$

$$O_p[s] \cdot O_p[t] = w \cdot d$$

i

$$O_p[s] \cdot O_p[s] = a + (w-1) \cdot d.$$

Iz leme 3.0.1 slijedi:

$$\det(O_p \cdot O_p^T) = \begin{vmatrix} a+(w-1)\cdot d & w\cdot d & \dots & w\cdot d \\ w\cdot d & a+(w-1)\cdot d & \dots & w\cdot d \\ \vdots & \vdots & \ddots & \vdots \\ w\cdot d & w\cdot d & \dots & a+(w-1)\cdot d \end{vmatrix}$$
$$= (a-d)^{m-1}(a-d+mw\cdot d),$$

$$\det([O_p, x\cdot I]\cdot[O_p, x\cdot I]^T) = \begin{vmatrix} a+(w-1)\cdot d+x^2 & w\cdot d & \dots & w\cdot d \\ w\cdot d & a+(w-1)\cdot d+x^2 & \dots & w\cdot d \\ \vdots & \vdots & \ddots & \vdots \\ w\cdot d & w\cdot d & \dots & a+(w-1)\cdot d+x^2 \end{vmatrix}$$
$$= (a-d+x^2)^{m-1}(a-d+x^2+mw\cdot d),$$

$$\det([O_p, y\cdot \mathbf{1}]\cdot[O_p, y\cdot \mathbf{1}]^T) = \begin{vmatrix} a+(w-1)\cdot d+y^2 & w\cdot d+y^2 & \dots & w\cdot d+y^2 \\ w\cdot d+y^2 & a+(w-1)\cdot d++y^2 2 & \dots & w\cdot d+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ w\cdot d+y^2 & w\cdot d+y^2 & \dots & a+(w-1)\cdot d++y^2 \end{vmatrix}$$
$$= (a-d)^{m-1}(a-d+mw\cdot d+m\cdot y^2),$$

$$\det([O_p, x\cdot I_m, y\cdot \mathbf{1}]\cdot[O_p, x\cdot I_m, y\cdot \mathbf{1}]^T) = \begin{vmatrix} a+(w-1)\cdot d+x^2+y^2 & w\cdot d+y^2 & \dots & w\cdot d+y^2 \\ w\cdot d+y^2 & a+(w-1)\cdot d+x^2+y^2 & \dots & w\cdot d+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ w\cdot d+y^2 & w\cdot d+y^2 & \dots & a+(w-1)\cdot d+x^2+y^2 \end{vmatrix}$$
$$= (a-d+x^2)^{m-1}(a-d+x^2+m\cdot y^2+mw\cdot d).$$

Promatranjem kada su navedene determinante različite od nule slijedi tvrdnja teorema.

■

Teorem 3.1.4 primijenili smo na orbitne matrice slabo 3-samoortogonalnih dizajne iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 5 djeluje bez fiksnih točaka (slučaj 4.1) i na orbitne matrice slabo 5-samoortogonalnih dizajna na koje ciklička grupa reda 5 djeluje bez fiksnih točaka (slučaj 4.2). Dobiveni LCD kodovi prikazani su u tablicama 4.48 i 4.49.

3.1.2. LCD kodovi iz podmatrica orbitnih matrica slabo p-samoortogonalnih dizajna

Teorem 3.1.5. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv 0 \pmod{p}$ i $|B_i \cap B_j| \equiv 0 \pmod{p}$, za sve $i, j \in \{1,\ldots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka od $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$, i koja djeluje na skup blokova dizajna $\mathscr{D}$ sa f_2 fiksnih blokova i m orbita duljine p^α. Neka su x i y nenula elementi polja $\mathbb{F}_q$. Tada vrijedi sljedeće.

$OM1$)
- Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x \cdot I_{f_1}]$ je LCD kod.
- Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x \cdot I_{f_1}, y \cdot \mathbf{1}]$, za $x^2 + f_1 \cdot y^2 \neq 0$ je LCD kod.

$OM2$)
- Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x \cdot I_m]$ je LCD kod.
- Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x \cdot I_m, y \cdot \mathbf{1}]$, $x^2 + m \cdot y^2 \neq 0$ je LCD kod.

Dokaz.

$OM1$) Obzirom da je $k \equiv 0 \pmod{p}$, svaki blok sadrži $p \cdot \beta$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv 0 \pmod{p}$, za sve $i, j \in \{1,\ldots,b\}$, $i \neq j$, presjek svaka dva bloka sadrži $p \cdot \gamma$ fiksnih točaka.

Tada je za $s,t \in \{1,\ldots,f_1\}$,

$$OM1_p[s] \cdot OM1_p[t] = 0.$$

Iz leme 3.0.1 slijedi da je

$$\det(OM1_p \cdot OM1_p^T) = \begin{vmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{vmatrix}_{f_1 \times f_1} = 0,$$

$$\det([OM1_p, x\cdot I_{f_1}]\cdot[OM1_p, x\cdot I_{f_1}]^T) = \begin{vmatrix} x^2 & 0 & \dots & 0 \\ 0 & x^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x^2 \end{vmatrix}_{f_1\times f_1} = x^{2f_1},$$

$$\det([OM1_p, y\cdot \mathbf{1}]\cdot[OM1_p, y\cdot \mathbf{1}]^T) = \begin{vmatrix} y^2 & y^2 & \dots & y^2 \\ y^2 & y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & y^2 \end{vmatrix}_{f_1\times f_1} = 0,$$

$$\det([OM1_p, x\cdot I_{f_1}, y\cdot \mathbf{1}]\cdot[OM1_p, x\cdot I_{f_1}, y\cdot \mathbf{1}]^T) = \begin{vmatrix} x^2+y^2 & y^2 & \dots & y^2 \\ y^2 & x^2+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2 \end{vmatrix}_{f_1\times f_1}$$
$$= x^{2f_1-2}(x^2+f_1\cdot y^2).$$

Vidimo da matrice $OM1_p$ i $[OM1_p, y\cdot\mathbf{1}]$ ne generiraju LCD kod (neovisno o vrijednosti y), a promatrajući kada su preostale dvije determinante različite od 0, slijedi tvrdnja teorema.

OM2) Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je

$$\sum_{x'\in\mathscr{B}_t} |x\cap x'| \equiv p^\alpha \cdot d \pmod p \equiv 0 \pmod p$$

i da je za $s = t$

$$\sum_{x'\in\mathscr{B}_s} |x\cap x'| = |x\cap x| + \sum_{x'\in\mathscr{B}_s,\ x\neq x'} |x\cap x'| \equiv 0 + (p^\alpha - 1)\cdot 0 \pmod p \equiv 0 \pmod p.$$

Zaključujemo da je

$$OM2_p[s]\cdot OM2_p[t] = 0$$

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

Iz leme 3.0.1 slijedi da je

$$\det(OM2_p \cdot OM2_p^T) = \begin{vmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{vmatrix}_{m\times m} = 0,$$

$$\det([OM2_p, x\cdot I_m]\cdot[OM2_p, x\cdot I_m]^T) = \begin{vmatrix} x^2 & 0 & \dots & 0 \\ 0 & x^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x^2 \end{vmatrix}_{m\times m} = x^{2m},$$

$$\det([OM2_p, y\cdot \mathbf{1}]\cdot[OM2_p, y\cdot \mathbf{1}]^T) = \begin{vmatrix} y^2 & y^2 & \dots & y^2 \\ y^2 & y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & y^2 \end{vmatrix}_{m\times m} = 0,$$

$$\det([OM1_p, x\cdot I_m, y\cdot \mathbf{1}]\cdot[OM1_p, x\cdot I_m, y\cdot \mathbf{1}]^T) = \begin{vmatrix} x^2+y^2 & y^2 & \dots & y^2 \\ y^2 & x^2+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2 \end{vmatrix}_{m\times m}$$
$$= x^{2m-2}(x^2 + m\cdot y^2).$$

Vidimo da matrice $OM2_p$ i $[OM2_p, y\cdot\mathbf{1}]$ ne generiraju LCD kod (neovisno o vrijednosti y), a promatrajući kada su preostale dvije determinante različite od 0, slijedi tvrdnja teorema.

■

Teorem 3.1.5 primijenili smo na orbitne matrice slabo 3-samoortogonalne dizajne konstruirane iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni LCD kodovi prikazani su u tablici 4.50.

Teorem 3.1.6. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv 0 \pmod{p}$ i $|B_i \cap B_j| \equiv d \pmod{p}$, za sve $i,j \in \{1,\ldots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka od $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$, i koja djeluje na skup blokova dizajna $\mathscr{D}$ sa f_2 fiksnih blokova i m orbita duljine p^α. Neka su x i y nenula elementi polja $\mathbb{F}_q$. Tada vrijedi sljedeće.

*OM*1)
- Ako je $OM1_p$ punog ranga, za $(f_1-1)\cdot d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM1_p$ je LCD kod.
- Ako je $x^2 - d \neq 0$ i $x^2 + (f_1-1)\cdot d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x\cdot I_{f_1}]$ je LCD kod.
- Ako je $OM1_p$ punog ranga, za $f_1 \cdot y^2 + (f_1-1)\cdot d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, y\cdot \mathbf{1}]$ je LCD kod.
- Za $x^2 - d \neq 0$ i $x^2 + f_1\cdot y^2 + (f_1-1)\cdot d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x\cdot I_{f_1}, y\cdot \mathbf{1}]$ je LCD kod.

*OM*2)
- Ako je $OM2_p$ punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM2_p$ je LCD kod.
- Ako je $x^2 - d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x\cdot I_m]$ je LCD kod.
- Ako je $m\cdot y^2 - d \neq 0$ i ako je $OM2_p$ punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, y\cdot \mathbf{1}]$ je LCD kod.
- Ako je $x^2 - d \neq 0$ i $x^2 + m\cdot y^2 - d \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x\cdot I_m, y\cdot \mathbf{1}]$ je LCD kod.

Dokaz.

*OM*1) Obzirom da je $k \equiv 0 \pmod{p}$, svaki blok sadrži $p\cdot\beta$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv d \pmod{p}$, za sve $i,j \in \{1,\ldots,b\}$, $i \neq j$, presjek svaka dva bloka sadrži $p\cdot\gamma + d$ fiksnih točaka.

Tada je za $s,t \in \{1,\ldots,f_1\}$, $s \neq t$,

$$OM1_p[s]\cdot OM1_p[s] = 0$$

i

$$OM1_p[s] \cdot OM1_p[t] = d.$$

Iz leme 3.0.1 slijedi da je

$$\begin{aligned}\det(OM1_p \cdot {OM1_p}^T) &= \begin{vmatrix} 0 & d & \dots & d \\ d & 0 & \dots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & \dots & 0 \end{vmatrix}_{f_1 \times f_1} \\ &= (-d)^{f_1-1}[(f_1-1)\cdot d]\end{aligned}$$

$$\begin{aligned}\det([OM1_p, x\cdot I]\cdot[OM1_p, x\cdot I]^T) &= \begin{vmatrix} x^2 & d & \dots & d \\ d & x^2 & \dots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & \dots & x^2 \end{vmatrix}_{f_1 \times f_1} \\ &= (x^2-d)^{f_1-1}[x^2+(f_1-1)\cdot d]\end{aligned}$$

$$\begin{aligned}\det([OM1_p, y\cdot \mathbf{1}]\cdot[OM1_p, y\cdot \mathbf{1}]^T) &= \begin{vmatrix} y^2 & d+y^2 & \dots & d+y^2 \\ d+y^2 & y^2 & \dots & d+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ d+y^2 & d+y^2 & \dots & y^2 \end{vmatrix}_{f_1 \times f_1} \\ &= (y^2-d-y^2)^{f_1-1}[y^2+(f_1-1)\cdot(d+y^2)] \\ &= (-d)^{f_1-1}[(f_1-1)\cdot d + f_1\cdot y^2].\end{aligned}$$

$$\begin{aligned}\det([OM1_p, x\cdot I, y\cdot \mathbf{1}]\cdot[OM1_p, x\cdot I, y\cdot \mathbf{1}]^T) &= \begin{vmatrix} x^2+y^2 & d+y^2 & \dots & d+y^2 \\ d+y^2 & x^2+y^2 & \dots & d+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ d+y^2 & d+y^2 & \dots & x^2+y^2 \end{vmatrix}_{f_1 \times f_1} \\ &= (x^2+y^2-d-y^2)^{f_1-1}[x^2+y^2+(f_1-1)\cdot(d+y^2)] \\ &= (x^2-d)^{f_1-1}[x^2+f_1\cdot y^2+(f_1-1)\cdot d].\end{aligned}$$

Promatrajući kada su navedene determinante različite od 0, slijedi tvrdnja teorema.

*OM*2) Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv p^\alpha \cdot d \pmod{p} \equiv 0 \pmod{p}$$

i da je za $s = t$

$$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s,\ x \neq x'} |x \cap x'| \equiv 0 + (p^\alpha - 1) \cdot d \pmod{p} \equiv -d \pmod{p}.$$

Zaključujemo da je

$$OM2_p[s] \cdot OM2_p[s] = -d$$

i

$$OM2_p[s] \cdot OM2_p[t] = 0$$

za sve $s,t \in \{1,\ldots,m\},\ s \neq t$.

Iz leme 3.0.1 slijedi da je

$$\begin{aligned} \det(OM2_p \cdot OM2_p^T) &= \begin{vmatrix} -d & 0 & \ldots & 0 \\ 0 & -d & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & -d \end{vmatrix}_{m \times m} \\ &= (-d)^m \end{aligned}$$

$$\begin{aligned} \det([OM2_p, x \cdot I] \cdot [OM2_p, x \cdot I]^T) &= \begin{vmatrix} x^2 - d & 0 & \ldots & 0 \\ 0 & x^2 - d & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x^2 - d \end{vmatrix}_{m \times m} \\ &= (x^2 - d)^m, \end{aligned}$$

$$\det([OM2_p, y\cdot\mathbf{1}]\cdot[OM2_p, y\cdot\mathbf{1}]^T) = \begin{vmatrix} y^2-d & y^2 & \dots & y^2 \\ y^2 & y^2-d & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & y^2-d \end{vmatrix}_{m\times m}$$
$$= (-d)^{m-1}(m\cdot y^2 - d),$$

$$\det([OM1_p, x\cdot I, y\cdot\mathbf{1}]\cdot[OM1_p, x\cdot I, y\cdot\mathbf{1}]^T) = \begin{vmatrix} x^2+y^2-d & y^2 & \dots & y^2 \\ y^2 & x^2+y^2-d & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2-d \end{vmatrix}_{m\times m}$$
$$= (x^2-d)^{m-1}(x^2+m\cdot y^2-d).$$

Promatrajući kada su navedene determinante različite od 0, slijedi tvrdnja teorema.

■

Teorem 3.1.6 primijenili smo na orbitne matrice slabo 3-samoortogonalne dizajne konstruirane iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni LCD kodovi prikazani su u tablici 4.51.

Teorem 3.1.7. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv a \pmod p$ i $|B_i \cap B_j| \equiv 0 \pmod p$, za sve $i,j \in \{1,\dots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka od $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$, i koja djeluje na skup blokova dizajna $\mathscr{D}$ sa f_2 fiksnih blokova i m orbita duljine p^α. Neka su x i y nenula elementi polja $\mathbb{F}_q$. Tada vrijedi sljedeće.

*OM*1)
- Ako je $OM1_p$ punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM1_p$ je LCD kod.
- Ako je $x^2 + a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x\cdot I_{f_1}]$ je LCD kod.

- Ako je $OM1_p$ punog ranga i za $a + f_1 \cdot y^2 \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, y \cdot \mathbf{1}]$ je LCD kod.
- Za $x^2 + a \neq 0$ i $x^2 + f_1 \cdot y^2 + a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x \cdot I_{f_1}, y \cdot \mathbf{1}]$ je LCD kod.

$OM2$)
- Ako je $OM2_p$ punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM2_p$ je LCD kod.
- Ako je $x^2 + a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x \cdot I_m]$ je LCD kod.
- Ako je $OM2_p$ punog ranga i za $a + m \cdot y^2 \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, y \cdot \mathbf{1}]$ je LCD kod.
- Za $x^2 + a \neq 0$ i $x^2 + m \cdot y^2 + a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x \cdot I_m, y \cdot \mathbf{1}]$ je LCD kod.

Dokaz.

$OM1$) Obzirom da je $k \equiv a \pmod{p}$, svaki blok sadrži $p \cdot \beta + a$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv 0 \pmod{p}$, za sve $i, j \in \{1, \ldots, b\},\ i \neq j$, presjek svaka dva bloka sadrži $p \cdot \gamma$ fiksnih točaka.

Tada je za $s, t \in \{1, \ldots, f_1\},\ s \neq t$,

$$OM1_p[s] \cdot OM1_p[s] = a$$

i

$$OM1_p[s] \cdot OM1_p[t] = 0.$$

Iz leme 3.0.1 slijedi da je

$$\det(OM1_p \cdot {OM1_p}^T) = \begin{vmatrix} a & 0 & \ldots & 0 \\ 0 & a & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a \end{vmatrix}_{f_1 \times f_1}$$
$$= a^{f_1}$$

$$\det([OM1_p, x\cdot I]\cdot[OM1_p, x\cdot I]^T) = \begin{vmatrix} x^2+a & 0 & \dots & 0 \\ 0 & x^2+a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x^2+a \end{vmatrix}_{f_1\times f_1}$$
$$= (x^2+a)^{f_1}$$

$$\det([OM1_p, y\cdot \mathbf{1}]\cdot[OM1_p, y\cdot \mathbf{1}]^T) = \begin{vmatrix} a+y^2 & y^2 & \dots & y^2 \\ d+y^2 & a+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & a+y^2 \end{vmatrix}_{f_1\times f_1}$$
$$= a^{f_1-1}(a+f_1\cdot y^2).$$

$$\det([OM1_p, x\cdot I, y\cdot \mathbf{1}]\cdot[OM1_p, x\cdot I, y\cdot \mathbf{1}]^T) = \begin{vmatrix} a+x^2+y^2 & y^2 & \dots & y^2 \\ y^2 & a+x^2+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & a+x^2+y^2 \end{vmatrix}_{f_1\times f_1}$$
$$= (a+x^2)^{f_1-1}(a+x^2+f_1\cdot y^2).$$

Promatrajući kada su navedene determinante različite od 0, slijedi tvrdnja teorema.

*OM*2) Za $s\neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je

$$\sum_{x'\in\mathscr{B}_t} |x\cap x'| \equiv p^\alpha\cdot 0 \pmod p \equiv 0 \pmod p$$

i da je za $s=t$

$$\sum_{x'\in\mathscr{B}_s} |x\cap x'| = |x\cap x| + \sum_{x'\in\mathscr{B}_s,\ x\neq x'} |x\cap x'| \equiv a+(p^\alpha-1)\cdot 0 \pmod p \equiv a \pmod p.$$

Zaključujemo da je

$$OM2_p[s]\cdot OM2_p[s] = a$$

i

$$OM2_p[s] \cdot OM2_p[t] = 0$$

za sve $s,t \in \{1,\ldots,m\},\ s \neq t$.

Iz leme 3.0.1 slijedi da je

$$\det(OM2_p \cdot {OM2_p}^T) = \begin{vmatrix} a & 0 & \ldots & 0 \\ 0 & a & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a \end{vmatrix}_{m\times m}$$
$$= a^m$$

$$\det([OM2_p, x\cdot I]\cdot[OM2_p, x\cdot I]^T) = \begin{vmatrix} x^2+a & 0 & \ldots & 0 \\ 0 & x^2+a & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x^2+a \end{vmatrix}_{m\times m}$$
$$= (x^2+a)^m$$

$$\det([OM2_p, y\cdot \mathbf{1}]\cdot[OM2_p, y\cdot \mathbf{1}]^T) = \begin{vmatrix} a+y^2 & y^2 & \ldots & y^2 \\ y^2 & a+y^2 & \ldots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \ldots & a+y^2 \end{vmatrix}_{m\times m}$$
$$= a^{m-1}(a+m\cdot y^2).$$

$$\det([OM2_p, x\cdot I, y\cdot \mathbf{1}]\cdot[OM2_p, x\cdot I, y\cdot \mathbf{1}]^T) = \begin{vmatrix} a+x^2+y^2 & y^2 & \ldots & y^2 \\ y^2 & a+x^2+y^2 & \ldots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \ldots & a+x^2+y^2 \end{vmatrix}_{m\times m}$$
$$= (a+x^2)^{m-1}(a+x^2+m\cdot y^2).$$

Promatrajući kada su navedene determinante različite od 0, slijedi tvrdnja teorema.

■

Teorem 3.1.7 primijenili smo na orbitne matrice slabo 3-samoortogonalne dizajne konstruirane iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni LCD kodovi prikazani su u tablici 4.52.

Teorem 3.1.8. Neka je $q = p^l$ potencija prostog broja i neka je $\mathbb{F}_q$ konačno polje reda q. Neka je $\mathscr{D}$ 1-(v,k,r) dizajn za koji je $k \equiv a \pmod p$ i $|B_i \cap B_j| \equiv d \pmod p$, za sve $i,j \in \{1,\ldots,b\}$, $i \neq j$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$ te neka je G grupa automorfizama dizajna $\mathscr{D}$ koja djeluje na skup točaka od $\mathscr{D}$ sa f_1 fiksnih točaka i n orbita duljine p^α, $1 \leq \alpha \leq l$, i koja djeluje na skup blokova dizajna $\mathscr{D}$ sa f_2 fiksnih blokova i m orbita duljine p^α. Neka su x i y nenula elementi polja $\mathbb{F}_q$. Tada vrijedi sljedeće.

1. Ako je $a = d$, tada vrijedi sljedeće.

   $OM1$)
   - Ako je $x^2 + f_1 \cdot a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x \cdot I_{f_1}]$ je LCD kod.
   - Za $x^2 + f_1 \cdot y^2 + f_1 \cdot a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x \cdot I_{f_1}, y \cdot \mathbf{1}]$ je LCD kod.

   $OM2$)
   - Linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x \cdot I_m]$ je LCD kod.
   - Za $x^2 + m \cdot y^2 \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x \cdot I_m, y \cdot \mathbf{1}]$ je LCD kod.

2. Ako je $a \neq d$, tada vrijedi sljedeće.

   $OM1$)
   - Ako je $OM1_p$ punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM1_p$ je LCD kod.
   - Ako je $x^2 + a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x \cdot I_{f_1}]$ je LCD kod.
   - Ako je $OM1_p$ punog ranga i za $a + f_1 \cdot y^2 \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, y \cdot \mathbf{1}]$ je LCD kod.
   - Za $x^2 + a \neq 0$ i $x^2 + f_1 \cdot y^2 + f_1 \cdot a \neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM1_p, x \cdot I_{f_1}, y \cdot \mathbf{1}]$ je LCD kod.

   $OM2$)
   - Ako je $OM2_p$ punog ranga, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $OM2_p$ je LCD kod.

- Ako je $x^2+a-d\neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x\cdot I_m]$ je LCD kod.
- Ako je $OM2_p$ punog ranga i za $a-d+m\cdot y^2\neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, y\cdot \mathbf{1}]$ je LCD kod.
- Za $x^2+a-d\neq 0$ i $x^2+m\cdot y^2+a-d\neq 0$, linearan kod nad poljem $\mathbb{F}_q$ generiran matricom $[OM2_p, x\cdot I_m, y\cdot \mathbf{1}]$ je LCD kod.

Dokaz.

1. Neka je $a=d$.

$OM1$) Obzirom da je $k\equiv a \pmod p$, svaki blok sadrži $p\cdot\beta+a$ fiksnih točaka i obzirom da je $|B_i\cap B_j|\equiv a \pmod p$, za sve $i,j\in\{1,\ldots,b\},\ i\neq j$, presjek svaka dva bloka sadrži $p\cdot\gamma+a$ fiksnih točaka.
Tada je za $s,t\in\{1,\ldots,f_1\},\ s\neq t$,

$$OM1_p[s]\cdot OM1_p[s]=a$$

i

$$OM1_p[s]\cdot OM1_p[t]=a.$$

Iz leme 3.0.1 slijedi da je

$$\det(OM1_p\cdot {OM1_p}^T)=\begin{vmatrix} a & a & \ldots & a\\ a & a & \ldots & a\\ \vdots & \vdots & \ddots & \vdots\\ a & a & \ldots & a\end{vmatrix}_{f_1\times f_1}=0.$$

$$\begin{aligned}\det([OM1_p, x\cdot I]\cdot[OM1_p, x\cdot I]^T)&=\begin{vmatrix} x^2+a & a & \ldots & a\\ a & x^2+a & \ldots & a\\ \vdots & \vdots & \ddots & \vdots\\ a & a & \ldots & x^2+a\end{vmatrix}_{f_1\times f_1}\\ &=(x^2)^{f_1-1}(x^2+f_1\cdot a)\end{aligned}$$

$$\det([OM1_p, y\cdot\mathbf{1}]\cdot[OM1_p, y\cdot\mathbf{1}]^T) = \begin{vmatrix} a+y^2 & a+y^2 & \dots & a+y^2 \\ a+y^2 & a+y^2 & \dots & a+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ a+y^2 & a+y^2 & \dots & a+y^2 \end{vmatrix}_{f_1\times f_1} = 0$$

$$\det([OM1_p, x\cdot I, y\cdot\mathbf{1}]\cdot[OM1_p, x\cdot I, y\cdot\mathbf{1}]^T) = \begin{vmatrix} a+x^2+y^2 & a+y^2 & \dots & a+y^2 \\ a+y^2 & a+x^2+y^2 & \dots & a+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ a+y^2 & a+y^2 & \dots & a+x^2+y^2 \end{vmatrix}_{f_1\times f_1}$$
$$= x^{2f_1-2}(x^2+f_1\cdot y^2+f_1\cdot a).$$

Vidimo da matrice $OM1_p$ i $[OM1_p, y\cdot\mathbf{1}]$ ne generiraju LCD kod (neovisno o vrijednosti y). Promatrajući kada su preostale dvije determinante različite od 0, slijedi tvrdnja teorema.

$OM2$) Za $s\neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je

$$\sum_{x'\in\mathscr{B}_t} |x\cap x'| \equiv p^\alpha\cdot a \pmod p \equiv 0 \pmod p$$

i da je za $s=t$

$$\sum_{x'\in\mathscr{B}_s} |x\cap x'| = |x\cap x| + \sum_{x'\in\mathscr{B}_s,\ x\neq x'} |x\cap x'| \equiv a+(p^\alpha-1)\cdot a \pmod p \equiv 0 \pmod p.$$

Zaključujemo da je

$$OM2_p[s]\cdot OM2_p[s] = 0$$

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

Iz leme 3.0.1 slijedi da je

$$\det(OM2_p\cdot {OM2_p}^T) = \begin{vmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a \end{vmatrix}_{m\times m}$$
$$= a^m$$

$$\det([OM2_p, x\cdot I]\cdot[OM2_p, x\cdot I]^T) = \begin{vmatrix} x^2 & 0 & \dots & 0 \\ 0 & x^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x^2 \end{vmatrix}_{m\times m} = x^{2m}$$

$$\det([OM2_p, y\cdot \mathbf{1}]\cdot[OM2_p, y\cdot \mathbf{1}]^T) = \begin{vmatrix} y^2 & y^2 & \dots & y^2 \\ y^2 & y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & y^2 \end{vmatrix}_{m\times m} = 0.$$

$$\det([OM2_p, x\cdot I, y\cdot \mathbf{1}]\cdot[OM2_p, x\cdot I, y\cdot \mathbf{1}]^T) = \begin{vmatrix} x^2+y^2 & y^2 & \dots & y^2 \\ y^2 & x^2+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2 \end{vmatrix}_{m\times m}$$
$$= x^{2m-2}(x^2+m\cdot y^2).$$

Vidimo da matrice $OM2_p$ i $[OM2_p, y\cdot\mathbf{1}]$ ne generiraju LCD kod (neovisno o vrijednosti y). Promatrajući kada su preostale dvije determinante različite od 0, slijedi tvrdnja teorema.

2. Neka je $a \neq d$.

$OM1$) Obzirom da je $k \equiv a \pmod p$, svaki blok sadrži $p\cdot\beta + a$ fiksnih točaka i obzirom da je $|B_i \cap B_j| \equiv d \pmod p$, za sve $i, j \in \{1,\dots,b\},\ i \neq j$, presjek svaka dva bloka sadrži $p\cdot\gamma + d$ fiksnih točaka.
Tada je za $s,t \in \{1,\dots,f_1\},\ s \neq t$,

$$OM1_p[s]\cdot OM1_p[s] = a$$

i

$$OM1_p[s]\cdot OM1_p[t] = d.$$

Tvrdnja teorema slijedi direktno iz leme 3.0.1 i korolara 3.0.3.

*OM*2) Za $s \neq t$, obzirom da je $\mathscr{B}_t$ orbita duljine p^α, iz napomene 1.2.32 slijedi da je

$$\sum_{x' \in \mathscr{B}_t} |x \cap x'| \equiv p^\alpha \cdot 0 \pmod{p} \equiv 0 \pmod{p}$$

i da je za $s = t$

$$\sum_{x' \in \mathscr{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathscr{B}_s,\ x \neq x'} |x \cap x'| \equiv a + (p^\alpha - 1) \cdot d \pmod{p} \equiv a - d \pmod{p}.$$

Zaključujemo da je

$$OM2_p[s] \cdot OM2_p[s] = a - d$$

i

$$OM2_p[s] \cdot OM2_p[t] = 0$$

za sve $s,t \in \{1,\ldots,m\},\ s \neq t$.

Iz leme 3.0.1 slijedi da je

$$\begin{aligned} \det(OM2_p \cdot {OM2_p}^T) &= \begin{vmatrix} a-d & 0 & \ldots & 0 \\ 0 & a-d & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a-d \end{vmatrix}_{m \times m} \\ &= (a-d)^m \end{aligned}$$

$$\begin{aligned} \det([OM2_p, x \cdot I] \cdot [OM2_p, x \cdot I]^T) &= \begin{vmatrix} x^2+a-d & 0 & \ldots & 0 \\ 0 & x^2+a-d & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x^2+a-d \end{vmatrix}_{m \times m} \\ &= (x^2+a-d)^m \end{aligned}$$

$$\begin{aligned} \det([OM2_p, y \cdot \mathbf{1}] \cdot [OM2_p, y \cdot \mathbf{1}]^T) &= \begin{vmatrix} y^2+a-d & y^2 & \ldots & y^2 \\ y^2 & y^2+a-d & \ldots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \ldots & y^2+a-d \end{vmatrix}_{m \times m} \\ &= (a-d)^{m-1}(a-d+m \cdot y^2). \end{aligned}$$

$$\det([OM2_p, x\cdot I, y\cdot \mathbf{1}]\cdot[OM2_p, x\cdot I, y\cdot \mathbf{1}]^T) = \begin{vmatrix} x^2+y^2+a-d & y^2 & \dots & y^2 \\ y^2 & x^2+y^2+a-d & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2+a-d \end{vmatrix}_{m\times m}$$
$$= (x^2+a-d)^{m-1}(x^2+a-d+m\cdot y^2).$$

Promatrajući kada su navedene determinante različite od 0, slijedi tvrdnja teorema.

■

Teorem 3.1.8 primijenili smo na orbitne matrice slabo 3-samoortogonalne dizajne konstruirane iz grupe $S(4,9)$ na 1640 točaka na koje ciklička grupa reda 3 djeluje s fiksnim točkama. Dobiveni LCD kodovi prikazani su u tablici 4.53.

4. PRIMJERI

U ovom poglavlju dajemo tablice parametara samoortogonalnih i LCD kodova konstruiranih iz slabo p-samoortogonalnih dizajna koristeći konstrukcije uvedene u poglavljima 2 i 3.

4.1. SAMOORTOGONALNI KODOVI

4.1.1. Djelomična klasifikacija binarnih samoortogonalnih kodova konstruiranih iz slabo samoorotogonalnih dizajna iz grupe M_{11}

Opis konstrukcije

Primjenom teorema 1.2.33, za sve grupe G koje su slike svih tranzitivnih permutacijskih reprezentacija (do na ekvivalenciju) grupe M_{11} stupnja n, $n \leq 165$, definirajući osnovni blok dizajna kao uniju orbita stabilizatora za djelovanje grupe G na skupu $\{1,\ldots,n\}$, konstruirali smo sve slabo samoortogonalne 1-dizajne na n točaka na koje grupa $G \cong M_{11}$ djeluje kao grupa automorfizama.

Tranzitivne permutacijske reprezentacije grupe M_{11} dobili smo koristeći napomenu 1.1.15 u programskom paketu GAP ([28]).

Grupa M_{11} ima, do na konjugaciju, 39 podgrupa. Neka je H predstavnik klase konjugiranosti podgrupa indeksa n, $n \leq 165$. M_{11} djeluje tranzitivno na skup Γ_H lijevih suskupova podgrupe H u M_{11} lijevim množenjem. To djelovanje inducira vjernu permutacijsku reprezentaciju $F : M_{11} \to S(\Gamma_H)$ koja svakom elementu $g \in M_{11}$ pridružuje bijekciju $f_g : \Gamma_H \to \Gamma_H$, $f_g(g_1H) = g.g_1H = (gg_1)H$. Opisana je permutacijska reprezentacija grupe M_{11} na $|\Gamma_H| = [M_{11} : H] = n$ točaka te je $G = Im(F)$ tranzitivna permutacijska grupa izomorfna M_{11}. Grupu G u programskom paketu GAP možemo dobiti korištenjem naredbe

`G:=Image(FactorCosetAction(`M_{11}`,H)).`

Grupa M_{11} ima 12 neekvivalentnih tranzitivnih permutacijskih reprezentacija na n točaka, $n \leq 165$. Preciznije, jednu reprezentaciju na 11 točaka, jednu reprezentaciju na 12 točaka, jednu reprezentaciju na 22 točke, jednu reprezentaciju na 55 točaka, jednu reprezentaciju na 66 točaka, tri reprezentacije na 110 točaka, dvije reprezentacije na 132 točke, jednu reprezentaciju na 144 točke i jednu reprezentaciju na 165 točaka.

Slike svih, do na ekvivalenciju, tranzitivnih permutacijskih reprezentacije grupe M_{11} na n točaka, $n < 165$, dostupne su na

https://www.math.uniri.hr/∼inovak/TrRep.

Za svaku dobivenu tranzitivnu permutacijsku grupu G, primjenom teorema 1.2.33, konstruirali smo dizajne i izdvojili sve, do na izomorfizam, netrivijalne slabo samoortogonalne dizajne.

Napomena 4.1.1. Tranzitivne reprezentacije grupe M_{11} na 11 i 12 točaka su višestruko tranzitivne pa su duljine orbita stabilizatora za djelovanje grupe G jednake 1 i $k-1$, $k \in \{11,12\}$, odnsono primjenom teorema 1.2.33 na 11 i 12 točaka moguće je konstruirati samo trivijalne dizajne s parametrima 1-$(k,1,1)$ i $(k-1)$-$(k,k-1,1)$.

Sljedeća tablica prikazuje broj dobivenih netrivijalnih slabo samoortogonalnih dizajna za svaku promatranu tranzitivnu permutacijsku grupu G.

Stupanj	**Broj dizajna**
22	2
55	0
66	4
110	8
110	12
110	24
132	42
132	30
144	24
165	20

Tablica 4.1: Broj dobivenih netrivijalnih slabo samoortogonalnih dizajna za svaku promatranu tranzitivnu permutacijsku grupu G

Konstruirani slabo samoortogonalni dizajni, lista parametara dobivenih dizajna i presječni brojevi dostupni su na https://www.math.uniri.hr/∼inovak/Dizajni/M11.

Za svaku promatranu tranzitivnu parmutacijsku grupu G, za svaki konstruirani dizajn primjenom metoda konstrukcije opisanih u poglavlju 2, konstruirali smo samoortogonalne kodove. Za svaki konstruirani kod pokušali smo odrediti parametre i grupe automorfizama i je li ekvivalentan nekom prethodno konstruiranom kodu.

Dobiveni samoortogonalni kodovi

U nastavku prilažemo tablice s parametrima dobivenih kodova i dizajna iz kojih su dobiveni. Tablice konstruiranih kodova su poredane prema 4 slučaja slabo samoortogonalnih dizajna.

Slučaj 1. Kodovi iz samoortogonalnih dizajna.

Slučaj 2. Kodovi iz slabo samoortogonalnih dizajna s parnom veličinom bloka i neparnim presječnim brojevima dva različita bloka.

Slučaj 3. Kodovi iz slabo samoortogonalnih dizajna s neparnom veličinom bloka i parnim presječnim brojevima dva različita bloka.

Slučaj 4. Kodovi iz slabo samoortogonalnih dizajna s neparnom veličinom bloka i neparnim presječnim brojevima dva različita bloka.

Optimalni kodovi označeni su sa $*$, skoro optimalni sa $**$ i najbolji poznati kodovi označeni su sa $+$. Podaci o teoretskoj granici za minimalnu udaljenost za danu duljinu i dimenziju koda mogu se naći u [31]. Obzirom na računalna ograničenja, neke podatke u tablicama, kao npr. grupu automorfizama i minimalnu udaljenost pojedinih kodova ostavljamo prazno jer ih nismo bili u mogućnosti izračunati.

Parametri dizajna	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(22,20,10)$	$[22,10,4]$	$Z_2 \times (E_{2^{10}} : S_{11})$
1-$(22,2,1)$	$[22,11,2]$	$Z_2 \times (E_{2^{10}} : S_{11})$
1-$(66,20,20)$	$[66,10,20]$	S_{12}
1-$(66,46,46)$	$[66,11,20]$	S_{12}
1-$(110,72,36)$	$[110,44,8]$	$2^{55} \cdot 11!$
1-$(110,36,18)$	$[110,10,20]$	$2^{55} \cdot 11!$
1-$(110,108,54)$	$[110,54,4]$	$2^{55} \cdot 55!$
1-$(110,74,37)$	$[110,11,20]$	$2^{55} \cdot 11!$
1-$(110,38,19)$	$[110,45,6]$	$2^{55} \cdot 11!$
1-$(110,10,1)$	$[110,11,10]$	$11! \cdot (10!)^{11}$
1-$(110,18,9)$	$[110,55,6]$	S_{11}
1-$(110,74,37)$	$[110,11,20]$	$2^{55} \cdot 11!$
1-$(110,20,10)$	$[110,10,20]$	$11! \cdot (10!)^{11}$
1-$(110,28,28)$	$[110,54,8]$	S_{11}
1-$(132,20,20)$	$[132,54,16]$	M_{11}
1-$(132,6,1)$	$[132,22,6]$	$22! \cdot (6!)^{22}$
1-$(132,60,60)$	$[132,21,12]$	$22! \cdot (6!)^{22}$
1-$(132,40,40)$	$[132,65,12]$	M_{11}
1-$(132,26,26)$	$[132,66,6]$	M_{11}
1-$(132,12,1)$	$[132,11,12]$	$11! \cdot (12!)^{11}$
1-$(132,66,6)$	$[132,11,24]$	$61440 \cdot 12! \cdot (6!)^{21}$
1-$(132,46,46)$	$[132,55,16]$	M_{11}
1-$(132,46,46)$	$[132,55,16]$	M_{11}
1-$(132,32,32)$	$[132,45,20]$	M_{11}

Tablica 4.2: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi dobiveni iz samoortogonalnih dizajna koristeći teorem 2.0.1 (slučaj 1)

Parametri dizajna	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(132,100,100)$	$[132,44,24]$	M_{11}
1-$(132,120,10)$	$[132,10,24]$	$11!\cdot(12!)^{11}$
1-$(132,112,112)$	$[132,55,12]$	M_{11}
1-$(132,60,30)$	$[132,54,8]$	$2^{66}\cdot 12!$
1-$(132,30,15)$	$[132,22,22]$	$2^{66}\cdot 7920$
1-$(132,2,1)$	$[132,66,2]$	$2^{66}\cdot 66!$
1-$(132,20,20)$	$[132,65,4]$	$2^{66}\cdot 66!$
1-$(132,32,16)$	$[132,45,16]$	$2^{66}\cdot 7920$
1-$(132,80,80)$	$[132,21,32]$	$2^{66}\cdot 7920$
1-$(132,50,50)$	$[132,55,6]$	$2^{66}\cdot 12!$
1-$(132,92,46)$	$[132,11,40]$	$2^{66}\cdot 12!$
1-$(132,22,2)$	$[132,11,22]$	$2^{66}\cdot 12!$
1-$(132,110,10)$	$[132,11,40]$	$2^{66}\cdot 12!$
1-$(132,40,20)$	$[132,10,40]$	$2^{66}\cdot 12!$
1-$(132,82,82)$	$[132,55,8]$	$2^{66}\cdot 12!$
1-$(132,100,50)$	$[132,44,16]$	$2^{66}\cdot 7920$
1-$(132,72,36)$	$[132,55,8]$	$2^{66}\cdot 12!$
1-$(144,12,1)$	$[144,12,12]$	$945^{13}\cdot 7920^{13}\cdot 2^{78}$
1-$(144,56,56)$	$[144,56,20]$	$M_{12}:Z_2$
2-$(144,66,30)$	$[144,46,22]$	$M_{12}:Z_2$
1-$(165,48,48)$	$[165,54,20]$	M_{11}
1-$(165,72,72)$	$[165,44,32]$	M_{11}
1-$(165,80,80)$	$[165,10,72]$	S_{11}

Tablica 4.3: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi dobiveni iz samoortogonalnih dizajna koristeći teorem 2.0.1 (slučaj 1)

Parametri dizajna	**Parametri koda**
1-$(165,116,116)$	$[331,165,12]$
1-$(165,84,84)$	$[331,165,8]$
1-$(165,36,36)$	$[331,165,12]$

Tablica 4.4: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi dobiveni iz slabo samoortogonalnih dizajna koristeći teorem 2.0.1 (slučaj 2)

Parametri dizajna	**Parametri koda**
1-(66,21,21)	[132,66,6]
1-(66,45,45)	[132,66,8]
1-(110,73,73)	[220,110,4]
1-(110,37,37)	[220,110,4]
1-(110,73,73)	[220,110,4]
1-(110,37,37)	[220,110,4]
1-(110,9,9)	[220,110,4]
1-(110,73,73)	[220,110,4]
1-(110,81,81)	[220,110,8]
1-(110,29,29)	[220,110,8]
1-(110,37,37)	[220,110,4]
1-(110,101,101)	[220,110,4]
1-(132,5,5)	[264,132,4]
1-(132,11,1)	[144,12,12]
1-(132,21,21)	[264,132,12]
1-(132,7,7)	[264,132,4]
1-(132,25,25)	[264,132,10]
1-(132,11,11)	[264,132,4]
1-(132,27,27)	[264,132,12]
1-(132,55,5)	[144,12,56]
1-(132,31,31)	[264,132,12]
1-(132,101,101)	[264,132,12]
1-(132,77,7)	[144,12,58]
1-(132,105,105)	[264,132,12]
1-(132,121,121)	[264,132,4]
1-(132,107,107)	[264,132,12]
1-(132,125,125)	[264,132,4]
1-(132,111,111)	[264,132,12]
1-(132,121,11)	[144,12,22]
1-(132,127,127)	[264,132,4]
1-(132,61,61)	[264,132,4]
1-(132,11,1)	[144,12,12]
1-(132,31,31)	[264,132,4]
1-(132,91,91)	[264,132,4]

Tablica 4.5: Netrivijalni binarni samoortogonalni kodovi dobiveni iz slabo samoortogonalnih dizajna koristeći teorem 2.0.1 (slučaj 3)

Parametri dizajna	**Parametri koda**
1-$(132,41,41)$	$[264,132,4]$
1-$(132,101,101)$	$[264,132,4]$
1-$(132,121,11)$	$[144,12,22]$
1-$(132,71,71)$	$[264,132,4]$
1-$(144,11,11)$	$[288,144,4]$
1-$(144,11,11)$	$[288,144,12]$
1-$(144,55,55)$	$[288,144]$
1-$(144,23,23)$	$[288,144]$
1-$(144,23,23)$	$[288,144]$
1-$(144,67,67)$	$[288,144]$
1-$(144,67,67)$	$[288,144]$
1-$(144,67,67)$	$[288,144]$
1-$(144,67,67)$	$[288,144]$
1-$(144,77,77)$	$[288,144]$
1-$(144,77,77)$	$[288,144]$
1-$(144,77,77)$	$[288,144]$
1-$(144,77,77)$	$[288,144]$
1-$(144,121,121)$	$[288,144]$
1-$(144,121,121)$	$[288,144]$
1-$(144,89,89)$	$[288,144]$
1-$(144,133,133)$	$[288,144]$
1-$(144,133,133)$	$[288,144]$
1-$(165,129,129)$	$[330,165,12]$
1-$(165,81,81)$	$[330,165,8]$
1-$(165,49,49)$	$[330,165,12]$

Tablica 4.6: Netrivijalni binarni samoortogonalni kodovi dobiveni iz slabo samoortogonalnih dizajna koristeći teorem 2.0.1 (slučaj 3)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(165,109,109)$	$[166,55,20]$	M_{11}
1-$(165,61,61)$	$[166,45,26]$	M_{11}
1-$(165,85,85)$	$[166,11,46]$	S_{11}

Tablica 4.7: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi dobiveni iz slabo samoortogonalnih dizajna koristeći teorem 2.0.1 (slučaj 4)

Binarni kodovi iz orbitnih matrica i podmatrica orbitnih matrica slabo samoortogonalnih dizajna

Koristeći teoreme 2.1.2, 2.1.6, 2.1.10 i 2.1.14, konstruirali smo binarne samoortogonalne kodove iz orbitnih matrica netrivijalnih slabo samoortogonalnih 1-dizajna na n točaka, $n \leq 165$, dobivenih primjenom teorema 1.2.33 iz grupe M_{11}. Orbitne matrice dobivene su obzirom na djelovanje svih cikličkih podgrupa grupe M_{11} prostog reda koje na skup točaka dizajna djeluju u orbitama jednakih duljina (bez fiksnih točaka). Dobiveni samoortogonalni kodovi prikazani su u sljedećim tablicama, a poredani su prema 4 slučaja slabo samoortogonalnih dizajna.

Optimalni kodovi označeni su sa $*$, skoro optimalni sa $**$ i najbolji poznati kodovi označeni su sa $+$. Obzirom na računalna ograničenja, neke podatke u tablicama, kao npr. grupa automorfizama i minimalna udaljenost pojedinih kodova ostavljamo prazno jer ih nismo bili u mogućnosti izračunati.

Parametri dizajna	G	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(110,72,36)$	Z_5	$[22,8,4]$	$Z_2 \times ((((((Z_2 \times D_8) : Z_2) : Z_3) : Z_2) : Z_2) \times ((E_{2^4} : A_5) : Z_2) \times S_4)$
	Z_{11}	$[10,4,4]*$	$Z_2 \times ((E_{2^4} : A_5) : Z_2)$
1-$(110,36,18)$	Z_5	$[22,2,4]$	$S_{10} \times S_8 \times D_8$
1-$(110,2,1)$	Z_{11}	$[10,5,2]$	$Z_2 \times ((E_{2^4} : A_5) : Z_2)$
1-$(110,74,37)$	Z_5	$[22,3,4]$	$S_{10} \times S_8 \times D_8$
1-$(110,38,19)$	Z_5	$[22,9,2]$	$Z_2 \times ((((((Z_2 \times D_8) : Z_2) : Z_3) : Z_2) : Z_2) \times ((E_{2^4} : A_5) : Z_2) \times S_4)$
1-$(110,10,1)$	Z_5	$[22,3,2]$	$2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2$
1-$(110,18,9)$	Z_5	$[22,11,2]$	$Z_2 \times (((E_{2^5} : A_6) : Z_2) \times ((E_{2^4} : A_5) : Z_2)$
1-$(110,20,10)$	Z_5	$[22,2,12]$	$2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2$
1-$(132,20,20)$	Z_{11}	$[12,4,4]$	$E_{2^2} \times ((E_{2^4} : A_5) : Z_2)$
1-$(132,6,1)$	Z_{11}	$[12,2,6]$	$(S_6 \times S_6) : Z_2$
1-$(132,40,40)$	Z_{11}	$[12,5,4]*$	$((E_{2^5} : A_6) : Z_2) : Z_2$
1-$(132,46,46)$	Z_{11}	$[12,5,4]*$	$(E_{2^4} : A_5) : Z_2$
1-$(132,30,15)$	Z_{11}	$[12,2,2]$	$Z_2 \times S_{10}$
1-$(132,50,50)$	Z_{11}	$[12,5,2]$	$E_{2^2} \times ((E_{2^4} : A_5) : Z_2)$
1-$(132,22,2)$	Z_{11}	$[12,11,2]*$	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7$
1-$(132,11,40)$	Z_{11}	$[12,1,10]$	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7$
1-$(132,82,82)$	Z_{11}	$[12,5,2]$	$E_{2^2} \times ((E_{2^4} : A_5) : Z_2)$
1-$(144,12,1)$	Z_2	$[72,4,12]$	$7920^6 \cdot 2^{41} \cdot 3^{19} \cdot 5^6 \cdot 7^7 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
	Z_3	$[48,6,4]$	$2^{41} \cdot 3^{20} \cdot 5^6 \cdot 7^3 \cdot 11^3$
1-$(144,56,56)$	Z_2	$[72,4,12]$	$((E_{2^4} : Z_3) : Z_2) : Z_2$
	Z_3	$[48,20,8]$	$Z_2 \times (S_4 \times S_4) : Z_2)$
2-$(144,66,30)$	Z_2	$[72,22,12]$	$((E_{2^4} : Z_3) : Z_2) : Z_2$
	Z_3	$[48,16,8]$	$(S_3 \times S_3) : Z_2$
1-$(165,48,48)$	Z_5	$[33,10,4]$	2048
	Z_{11}	$[15,4,8]*$	A_8
1-$(165,72,72)$	Z_5	$[33,8,8]$	$E_{2^2} \times ((E_{2^5} \times D_8) : Z_2)$
1-$(165,80,80)$	Z_5	$[33,2,16]$	$2^{27} \cdot 3^{12} \cdot 5^5 \cdot 7^2 \cdot 11^2$

Tablica 4.8: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi konstruirani primjenom teorema 2.1.2 iz orbitnih matrica netrivijalnih samoortogonalnih 1-dizajna za djelovanje grupe G (slučaj 1)

Parametri dizajna	G	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(165,116,116)$	Z_5	$[67,33,4]$	2^{14}
	Z_{11}	$[31,15,8]*$	PSL$(5,2)$
1-$(165,84,84)$	Z_5	$[67,33,4]$	
	Z_{11}	$[31,15,4]$	$2^{25}\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13$
1-$(165,36,36)$	Z_5	$[67,33,4]$	$E_{2^3}\times((Z_2\times(Z_4\times Z_2):Z_2):Z_2))$

Tablica 4.9: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi konstruirani primjenom teorema 2.1.6 iz orbitnih matrica netrivijalnih slabo samoortogonalnih 1-dizajna na 165 točaka za djelovanje grupe G (slučaj 2a)

Parametri dizajna	G	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(66,21,21)$	Z_{11}	$[12,6,2]$	$((E_{2^5}:A_6):Z_2):Z_2$
1-$(66,45,45)$	Z_{11}	$[12,6,4]*$	$(E_{2^5}:A_6):Z_2)$
1-$(110,73,73)$	Z_5	$[44,22,4]$	$2^{19}\cdot 10!\cdot 8!\cdot 4!$
1-$(110,37,37)$	Z_5	$[44,22,2]$	$2^{20}\cdot 10!\cdot 8!\cdot 4!$
1-$(110,9,9)$	Z_5	$[44,22,2]$	$2^{20}\cdot 10!\cdot 15!\cdot 8!\cdot 4!$
1-$(110,81,81)$	Z_5	$[44,22,4]$	$2^{30}\cdot 3^4\cdot 5^2$
1-$(110,101,101)$	Z_5	$[44,22,4]$	$2^{37}\cdot 3^8\cdot 5^4\cdot 7^2$
1-$(132,5,5)$	Z_{11}	$[24,12,4]$	$E_{2^{10}}:(A_6\times A_6):D_8$
1-$(132,11,1)$	Z_{11}	$[14,2,2]$	$Z_2\times S_{12}$
1-$(132,21,21)$	Z_{11}	$[24,12,2]$	$D_8\times(E_{2^{10}}:S_5)$
1-$(132,7,7)$	Z_{11}	$[24,12,4]$	$E_{2^{10}}:(A_6\times A_6):D_8$
1-$(132,25,25)$	Z_{11}	$[24,12,6]$	$((E_{2^6}:(Z_2.A_6)):Z_2$
1-$(132,11,11)$	Z_{11}	$[24,12,4]$	$E_{2^{11}}\cdot S_{12}$
1-$(132,27,27)$	Z_{11}	$[24,12,8]*$	M_{24}
1-$(132,55,5)$	Z_{11}	$[14,12,6]$	$S_6\times S_8$
1-$(132,31,31)$	Z_{11}	$[24,12,4]$	$E_{2^{10}}:((Z_3.A_6):Z_2)$
1-$(132,61,61)$	Z_{11}	$[24,12,2]$	$2^{12}\cdot 10!$

Tablica 4.10: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi konstruirani primjenom teorema 2.1.10 iz orbitnih matrica netrivijalnih slabo samoortogonalnih 1-dizajna za djelovanje grupe G (slučaj 3a)

Parametri dizajna	G	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(144,11,11)$	Z_2	$[144,72,2]$	
	Z_3	$[96,48,4]$	$2^{83}\cdot 3^2 0\cdot 7^6\cdot 5^6\cdot 11^3$
1-$(144,11,11)$	Z_2	$[144,72,10]$	
	Z_3	$[96,48,12]$	$(S_2\times S_3):Z_2$
1-$(144,55,55)$	Z_2	$[144,72,12]$	
	Z_3	$[96,48,8]$	$Z_2\times Z_3\times S_3$
1-$(144,23,23)$	Z_2	$[144,72,12]$	
	Z_3	$[96,48,16]+$	D_{12}
1-$(144,67,67)$	Z_2	$[144,72,8]$	
	Z_3	$[96,48,8]$	$Z_2\times((S_3\times S_3):Z_2)$
1-$(144,67,67)$	Z_2	$[144,72,6]$	
	Z_3	$[96,48,4]$	
1-$(144,67,67)$	Z_3	$[96,48,8]$	$(E_{2^3}\times S_3):Z_2$
1-$(144,77,77)$	Z_2	$[144,72,6]$	
	Z_3	$[96,48,4]$	$2^{29}\cdot 3^2$
1-$(144,77,77)$	Z_3	$[96,48,8]$	$(E_{2^3}\times S_3):Z_2$
1-$(144,77,77)$	Z_2	$[144,72,8]$	
	Z_3	$[96,48,8]$	$Z_2\times((S_3\times S_3):Z_2)$
1-$(144,121,121)$	Z_2	$[144,72,12]$	
	Z_3	$[96,48,14]$	D_{12}
1-$(144,121,121)$	Z_2	$[144,72,12]$	
1-$(144,89,89$	Z_2	$[144,72,12]$	
	Z_3	$[96,48,8]$	$Z_2\times Z_2\times S_3$
1-$(144,133,133)$	Z_3	$[96,48,12]$	$(S_3\times S_3):Z_2$
1-$(144,133,133)$	Z_2	$[144,72,2]$	
	Z_3	$[96,48,4]$	
1-$(165,129,129)$	Z_5	$[66,33,2]$	$2^{64}\cdot 3^{15}\cdot 5^7\cdot 7^4\cdot 11^3\cdot 13^2\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31$
	Z_{11}	$[30,15,2]$	$2^{26}\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13$
1-$(165,81,81)$	Z_5	$[66,33,4]$	$E_{2^3}\times((Z_2\times(Z_4\times Z_2):Z_2):Z_2)):Z_2)$
	Z_{11}	$[30,15,6]$	$Z_2\times(E_{2^4}:A_8)$
1-$(165,49,49)$	Z_5	$[66,33,2]$	

Tablica 4.11: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi konstruirani primjenom teorema 2.1.10 iz orbitnih matrica netrivijalnih slabo samoortogonalnih 1-dizajna za djelovanje grupe G (slučaj 3a)

Parametri dizajna	G	**Parametri koda** C	$\mathbf{Aut}(C)$ ili $\lvert\mathbf{Aut}(C)\rvert$
1-$(165,109,109)$	Z_5	$[34,9,6]$	$E_{2^2} \times ((E_{2^2} \times ((Z_2 \times D_8) : Z_2)) : Z_2$
	Z_{11}	$[16,5,8]*$	$E_{2^4} : A_8$
1-$(165,61,61)$	Z_5	$[34,3,10]$	$2^{38} \cdot 3^{13} \cdot 5^5 \cdot 7^2 \cdot 11^2$
1-$(165,85,85)$	Z_5	$[34,11,4]$	$E_{2^2} \times ((E_{2^2} \times D_8) : Z_2)$

Tablica 4.12: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi konstruirani primjenom teorema 2.1.14 iz orbitnih matrica netrivijalnih slabo samoortogonalnih 1-dizajna na 165 točaka za djelovanje grupe G (slučaj 4a)

Koristeći teoreme 2.1.4 i 2.1.12, konstruirali smo binarne samoortogonalne kodove iz podmatrica orbitnih matrica netrivijalnih slabo samoortogonalnih 1-dizajna na 165 točaka i manje, dobivenih primjenom teorema 1.2.33 iz grupe M_{11}. Orbitne matrice dobivene su obzirom na djelovanje cikličke grupe reda 2 (Z_2) koja na skup točaka dizajna djeluje u orbitama duljina 1 i 2 (s fiksnim točkama). Dobiveni samoortogonalni kodovi prikazani su u sljedećim tablicama, a poredani su prema 4 slučaja slabo samoortogonalnih dizajna.

Optimalni kodovi označeni su sa $*$, skoro optimalni sa $**$ i najbolji poznati kodovi označeni su sa $+$. Obzirom na računalna ograničenja, neke podatke u tablicama, kao npr. grupa automorfizama i minimalna udaljenost pojedinih kodova ostavljamo prazno jer ih nismo bili u mogućnosti izračunati.

Parametri dizajna	**Parametri koda** C	$\mathbf{Aut}(C)$ ili $\lvert\mathbf{Aut}(C)\rvert$
1-$(22,10,10)$	$[6,2,4]*$	$Z_2 \times S_4$
	$[8,4,2]$	$Z_2 \times S_4$
1-$(22,2,1)$	$[6,3,2]**$	$Z_2 \times S_4$
1-$(66,20,20)$	$[10,2,4]$	$Z_2 \times S_4 \times S_4$
	$[28,4,10]$	509607936
1-$(66,46,46)$	$[10,3,4]**$	$Z_2 \times S_4 \times S_4$
1-$(110,72,36)$	$[52,20,4]$	$2^{40} \cdot 3^6$
1-$(110,36,18)$	$[52,4,18]$	$2^40 \cdot 3^{16} \cdot 5^4$
1-$(110,2,1)$	$[52,24,2]$	$2^{49} \cdot 3^{11} \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
1-$(110,36,18)$	$[14,2,4]$	$Z_2 \times S_8 \times S_4$
	$[48,4,18]$	$2^{37} \cdot 3^{15} \cdot 5^4$
1-$(110,2,1)$	$[14,7,2]$	$Z_2 \times ((E_{2^6} : A_7) : Z_2)$
	$[48,24,2]$	$2^{46} \cdot 3^{10} \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
1-$(110,36,36)$	$[14,4,4]$	$(((((Z_2 \times D_8) : Z_2) : Z_3) : Z_2) : Z_2) \times S_6$
	$[48,20,4]$	$2^{37} \cdot 3^5$
1-$(110,39,19)$	$[14,5,2]$	$(((((Z_2 \times D_8) : Z_2) : Z_3) : Z_2) : Z_2) \times S_6$
1-$(110,72,72)$	$[14,6,4]**$	$Z_2 \times (((E_{2^6} : A_7) : Z_2)$
1-$(110,74,37)$	$[14,3,4]$	$Z_2 \times S_8 \times S_4$
1-$(110,10,1)$	$[52,4,10]$	$2^{45} \cdot 3^{22} \cdot 5^{10} \cdot 7^5 \cdot 11$
1-$(110,18,9)$	$[52,24,2]$	$2^{27} \cdot 3^5$
1-$(132,20,20)$	$[60,24,8]$	$Z_2 \times S_4$
1-$(132,6,1)$	$[60,8,6]$	$2^{49} \cdot 3^{23} \cdot 5^{11} \cdot 7^2 \cdot 11$
1-$(132,40,40)$	$[60,28,6]$	S_4
1-$(132,12,1)$	$[12,3,4]$	$((((((A_4 \times A_4) : Z_2) \times A_4) : Z_2) : Z_3) : Z_2) : Z_2$
	$[60,4,12]$	$2^{53} \cdot 3^{26} \cdot 5^{10} \cdot 7^5 \cdot 11^5$
1-$(132,66,6)$	$[12,3,6]*$	$((((Z_2 \times (E_{2^4} : Z_2)) : Z_2) : Z_3) : Z_2) : Z_2$
1-$(132,32,32)$	$[60,20,12]$	S_4
1-$(132,100,100)$	$[12,2,8]*$	$((((((A_4 \times A_4) : Z_2) \times A_4) : Z_2) : Z_3) : Z_2) : Z_2$
1-$(132,32,16)$	$[12,4,4]$	$(((((Z_2 \times (E_{2^4} : Z_2)) : Z_2) : Z_3) : Z_2) : Z_2) : Z_2$
	$[60,20,8]$	$2^{34} \cdot 3^2$
1-$(132,60,30)$	$[60,24,4]$	$2^{52} \cdot 3^6$
1-$(132,30,15)$	$[60,8,20]$	$2^{34} \cdot 3^2$
1-$(132,2,1)$	$[60,28,2]$	$2^{56} \cdot 3^{14} \cdot 5^6 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23$
1-$(132,92,46)$	$[60,4,20]$	$((((((A_4 \times A_4) : Z_2) \times A_4) : Z_2) : Z_3) : Z_2) : Z_2$

Tablica 4.13: Netrivijalni binarni u parovima neekvivalentni samoortogonalni kodovi konstruirani primjenom teorema 2.1.4 iz podmatrica orbitnih matrica netrivijalnih samoortogonalnih 1-dizajna (slučaj 1)

Parametri dizajna	**Parametri koda C**	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(66,21,21)$	$[20,10,2]$	$((E_{2^5}:A_6):Z_2)\times(((((Z_2\times D_8):Z_2):Z_3):Z_2):Z_2)$
	$[56,28,4]$	$2^{39}\cdot 3^5$
1-$(66,45,45)$	$[20,10,4]$	$((((Z_2\times D_8):Z_2):Z_3):Z_2)\times((E_{2^5}):A_6):Z_2)$
1-$(110,73,73)$	$[104,52,2]$	
1-$(110,37,37)$	$[104,52,2]$	
1-$(110,37,37)$	$[28,14,2]$	$2^{24}\cdot 3^4\cdot 5^2\cdot 7$
	$[96,48,4]$	$2^{94}\cdot 3^{22}\cdot 5^{10}\cdot 7^6\cdot 11^4\cdot 13^3\cdot 17^2\cdot 19^2\cdot 23^2\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47$
1-$(110,73,73)$	$[28,14,4]$	$2^{23}\cdot 3^4\cdot 5^2\cdot 7$
	$[96,48,4]$	
1-$(110,9,9)$	$[104,52,2]$	
1-$(110,73,73)$	$[104,52,2]$	
1-$(110,81,81)$	$[104,52,4]$	
1-$(110,29,29)$	$[104,52,4]$	
1-$(110,37,37)$	$[104,52,2]$	
1-$(110,101,101)$	$[104,52,2]$	
1-$(132,5,5)$	$[120,60,2]$	
1-$(132,21,21)$	$[120,60,10]$	
1-$(132,7,7)$	$[120,60,2]$	
1-$(132,25,25)$	$[120,60,8]$	
1-$(132,11,11)$	$[120,60,2]$	
1-$(132,27,27)$	$[120,60,10]$	
1-$(132,55,5)$	$[64,4,32]**$	$(E_{2^{28}}:(E_{3^{14}}:(E_{2^{10}}:(Z_2\times(E_{2^6}:PSL(3,2))))))\times S_8$
1-$(132,31,31)$	$[120,60,8]$	
1-$(132,101,101)$	$[120,60,8]$	
1-$(132,105,105)$	$[120,60,10]$	
1-$(132,121,121)$	$[120,60,2]$	
1-$(132,107,107)$	$[120,60,8]$	
1-$(132,125,125)$	$[120,60,2]$	
1-$(132,111,111)$	$[120,60,10]$	
1-$(132,121,11)$	$[64,4,12]$	$2^{58}\cdot 3^{27}\cdot 5^{11}\cdot 7^6\cdot 11^5\cdot 13$
1-$(132,127,127)$	$[120,60,2]$	
1-$(132,61,61)$	$[120,60,2]$	
1-$(132,31,31)$	$[120,60,2]$	
1-$(132,91,91)$	$[120,60,2]$	
1-$(132,41,41)$	$[120,60,2]$	
1-$(132,101,10)$	$[120,60,2]$	
1-$(132,71,71)$	$[120,60,2]$	

Tablica 4.14: Netrivijalni binarni samoortogonalni kodovi konstruirani primjenom teorema 2.1.12 iz podmatrica orbitnih matrica netrivijalnih slabo samoortogonalnih 1-dizajna (slučaj 3)

4.1.2. Primjeri samoortogonalnih kodova iz slabo p-samoortogonalnih dizajna

Koristeći teorem 1.2.33, koristeći tranzitivnu reprezentaciju grupe A_5 na 30 točaka i koristeći tranzitivnu reprezentaciju grupe $U(3,4)$ na 416 točaka, konstruirali smo primjere slabo 3-samoortogonalnih dizajna. Iz konstruiranih dizajna, primjenom teorema 2.0.4, konstruirali smo samoortogonalne kodove. Dobiveni kodovi prikazani su u sljedećim tablicama, a raspoređeni su prema 5 slučajeva slabo 3-samoortogonalnih dizajna.

Neka je $\mathscr{D}$ slabo 3- samoortogonalan dizajn takav da je $k \equiv a \pmod 3$ i $|B_i \cap B_j| \equiv d \pmod 3$, za $i \neq j,\ i,j \in \{1,\ldots,b\}$, gdje su B_i i B_j blokovi dizajna $\mathscr{D}$. Tada razlikujemo sljedećih 5 slučajeva.

Slučaj 1. Kodovi iz 3-samoortogonalnih dizajna.

Slučaj 2. Kodovi iz slabo 3-samoortogonalnih dizajna za koje je $a = 0,\ d \neq 0$.

Slučaj 3. Kodovi iz slabo 3-samoortogonalnih dizajna za koje je $a \neq 0,\ d = 0$.

Slučaj 4.1 Kodovi iz slabo 3-samoortogonalnih dizajna za koje je $a = d \neq 0$.

Slučaj 4.2 Kodovi iz slabo 3-samoortogonalnih dizajna za koje je $a \neq 0,\ d \neq 0,\ a \neq d$.

Optimalni kodovi označeni su sa $*$, skoro optimalni sa $**$ i najbolji poznati kodovi označeni su sa $+$. Obzirom na računalna ograničenja, neke podatke u tablicama, kao npr. grupa automorfizama i minimalna udaljenost pojedinih kodova ostavljamo prazno jer ih nismo bili u mogućnosti izračunati.

Parametri dizajna	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(30,12,4)$	$[30,10,12]_3$	$Z_2 \times A_5$
1-$(30,12,2)$	$[30,5,12]_3$	$Z_2 \times (E_{3^{10}} : ((E_{2^9} : A_6) : E_{2^2}))$
1-$(30,15,3)$	$[30,5,15]_3$	$Z_2 \times (E_{3^{10}} : ((E_{2^9} : (A_6.Z_2)) : Z_2))$
1-$(30,18,3)$	$[30,4,18]_3 **$	$E_{3^{10}} : (E_{2^{10}} : ((A_6 : Z_4) : Z_2))$
1-$(30,18,6)$	$[30,4,12]_3$	46438023168000000
1-$(30,18,6)$	$[30,9,12]_3$	$Z_2 \times A_5$
1-$(30,24,4)$	$[30,5,6]_3$	743008370688000000
1-$(30,24,12)$	$[30,10,3]_3$	224685731296051200
1-$(30,27,9)$	$[30,9,6]_3$	$Z_2 \times (E_{2^{10}} : ((E_{2^9} : A_{10}) : E_{2^2}))$

Tablica 4.15: Samoortogonalni kodovi dobiveni primjenom teorema 2.0.4 (slučaj 1)

Parametri dizajna	**Parametri koda**
1-$(30,9,3)$	$[41,10,11]_9$
1-$(30,9,3)$	$[41,10,11]_9$
1-$(30,12,4)$	$[41,10,12]_9$
1-$(30,18,6)$	$[41,10,11]_9$
1-$(30,21,7)$	$[41,10,11]_9$
1-$(30,21,7)$	$[41,10,16]_9$

Tablica 4.16: Samoortogonalni kodovi dobiveni primjenom teorema 2.0.4 (slučaj 2)

Parametri dizajna	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(30,2,1)$	$[45,15,3]_3$	201473672003095936358154240000
1-$(30,5,1)$	$[36,6,6]_3$	6419592322744320000000
1-$(30,8,4)$	$[45,15,9]_3$	$Z_2 \times S_6$
1-$(30,14,7)$	$[45,15,9]_3$	$E_{2^2} \times (E_{2^{14}} : A_8)$
1-$(30,20,4)$	$[36,6,15]_3$	$E_{2^2} \times (E_{2^{14}} : S_6)$
1-$(30,4,4)$	$[60,30,4]_9$	
1-$(30,16,16)$	$[60,30,8]_9$	

Tablica 4.17: Samoortogonalni kodovi dobiveni primjenom teorema 2.0.4 (slučaj 3)

Parametri dizajna	**Parametri koda**
1-$(416,101,101)$	$[417,65]_3$

Tablica 4.18: Samoortogonalni kodovi dobiveni primjenom teorema 2.0.4 (slučaj 4.1)

Parametri dizajna	**Parametri koda** C	**Aut**(C) ili $\lvert$**Aut**$(C)\rvert$
1-$(30,10,2)$	$[37,6,12]_3$	$E_{2^2} \times (E_{2^{14}} : S_6)$
1-$(30,16,8)$	$[46,15,12]_3$	$E_{2^2} \times (E_{2^4} : (E_{2^{14}} : A_8))$
1-$(30,22,11)$	$[46,15,12]_3$	$Z_2 \times S_6$
1-$(30,25,5)$	$[37,6,12]_3$	4299816960000000
1-$(30,28,14)$	$[46,15,6]_3$	$E_{2^2} \times (E_{2^{14}} : S_{15})$
1-$(30,14,14)$	$[61,30,8]_9$	
1-$(30,26,26)$	$[61,30,4]_9$	

Tablica 4.19: Samoortogonalni kodovi dobiveni primjenom teorema 2.0.4 (slučaj 4.2)

Primjeri samoortogonalnih kodova nad poljem $\mathbb{F}_3/\mathbb{F}_9$ iz orbitnih matrica i podmatrica slabo p-samoortogonalnih dizajna

Konstruirali smo samoortogonalne kodove primjenom teorema 2.1.3, 2.1.7, 2.1.11 i 2.1.15 na orbitne matrice slabo 3-samoortogonalnih dizajna dobivenih primjenom teorema 1.2.33 za permutacijsku reprezentaciju grupe A_5 na 30 točaka i za permutacijsku reprezentaciju grupe $U(3,4)$ na 416 točaka (za slučaj 4.1). Orbitne matrice dobivene su za djelovanje cikličke grupe prostog reda koja na točke dizajna djeluje u orbitama jednake veličine (bez fiksnih točaka).

Dobiveni samoortogonalni kodovi prikazani su u sljedećim tablicama, a poredani su prema 5 slučajeva slabo 3-samoortogonalnih dizajna.

Optimalni kodovi označeni su sa $*$, skoro optimalni sa $**$ i najbolji poznati kodovi označeni su sa $+$. Obzirom na računalna ograničenja, neke podatke u tablicama, kao npr. grupe automorfizama pojedinih kodova ostavljamo prazno jer ih nismo bili u mogućnosti izračunati.

Parametri dizajna	**Parametri koda C**	**Aut(C)**
1-$(30,15,3)$	$[10,1,9]_3$	$E_{2^2} \times S_9$
1-$(30,24,12)$	$[10,3,3]_3$	$E_{2^2} \times ((((E_{2^2} \times (E_{3^3} : E_{2^2})) : Z_3) : Z_2) : Z_2)$

Tablica 4.20: Samoortogonalni kodovi dobiveni koristeći teorem 2.1.3 iz orbitnih matrica za djelovanje grupe Z_3 bez fiksnih točaka (slučaj 1)

Parametri dizajna	**Parametri koda C**	**Aut(C)**
1-$(30,18,6)$	$[9,2,3]_3$	$Z_2 \times S_3 \times D_8 \times S_4$
1-$(30,21,7)$	$[9,2,6]_3*$	$Z_2 \times ((((E_{3^3} : E_{2^2}) : C3) : C2) : C2)$
1-$(30,9,3)$	$[9,2,3]_9$	
1-$(30,21,7)$	$[9,2,4]_9$	

Tablica 4.21: Samoortogonalni kodovi dobiveni koristeći teorem 2.1.7 iz orbitnih matrica za djelovanje grupe Z_5 bez fiksnih točaka (slučaj 2c).

Parametri dizajna	**Parametri koda C**	**Aut**(C)
1-$(30,2,1)$	$[15,5,3]_3$	$Z_2 \times (E_{3^5} : (C2 \times (E_{2^4} : (E_{2^4} : S_5))))$
1-$(30,5,1)$	$[12,2,6]_3$	$(E_{2^2} : ((A_6 \times A_6) : D_8)$
1-$(30,8,4)$	$[15,5,6]_3$	$Z_2 \times S_4 \times D_8$
1-$(30,14,7)$	$[15,5,6]_3$	$E_{2^2} \times (E_{2^4} : S_5)$
1-$(30,20,4)$	$[12,2,6]_3$	$Z_2 \times (S_6 \times ((S_3 \times S_3) : Z_2))$
1-$(30,4,4)$	$[20,10,4]_9$	
1-$(30,16,16)$	$[20,10,4]_9$	

Tablica 4.22: Samoortogonalni kodovi dobiveni koristeći teorem 2.1.11 iz orbitnih matrica za djelovanje grupe Z_3 bez fiksnih točaka (slučaj 3)

Parametri dizajna	**Parametri koda C**	**Aut**(C)
1-$(416,101,101)$	$[33,5,15]_3$	$Z_2 \times (((((Z_2 \times ((Z_4 \times Z_2) : Z_2)) : Z_2) : Z_2) : Z_3) \times S_5)$

Tablica 4.23: Samoortogonalni kodovi dobiveni koristeći teorem 2.1.15 iz orbitnih matrica za djelovanje grupe Z_{13} bez fiksnih točaka (slučaj 4.1b)

Parametri dizajna	**Parametri koda C**	**Aut**(C)
1-$(30,10,2)$	$[12,2,6]_3$	$Z_2 \times (S_6 \times ((S_3 \times S_3) : Z_2))$
1-$(30,16,8)$	$[15,5,6]_3$	$E_{2^2} \times (E_{2^4} : S_5)$
1-$(30,22,11)$	$[15,5,6]_3$	$Z_2 \times S_4 \times D_8$
1-$(30,25,5)$	$[12,2,6]_3$	$E_{2^2} : ((A_6 \times A_6) : D_8)$
1-$(30,28,14)$	$[15,5,3]_3$	$Z_2 \times (E_{3^5} : (Z_2 \times (E_{2^4} : (E_{2^4} : S_5))))$
1-$(30,14,14)$	$[20,10,4]_9$	
1-$(30,26,26)$	$[20,10,4]_9$	

Tablica 4.24: Samoortogonalni kodovi dobiveni koristeći teorem 2.1.15 iz orbitnih matrica za djelovanje grupe Z_3 bez fiksnih točaka (slučaj 4.2a)

Parametri dizajna	**Parametri koda**
1-$(30,14,14)$	$[13,6,4]_9$
1-$(30,16,8)$	$[10,3,5]_9$
1-$(30,22,11)$	$[10,3,5]_9$
1-$(30,26,26)$	$[13,6,4]_9$
1-$(30,28,14)$	$[10,3,5]_9$

Tablica 4.25: Samoortogonalni kodovi dobiveni koristeći teorem 2.1.15 za djelovanje grupe Z_5 bez fiksnih točaka (slučaj 4.2c)

Konstruirali smo samoortogonalne kodove primjenom teorema 2.1.5, 2.1.9, 2.1.13 i 2.1.17 na orbitne matrice slabo 3-samoortogonalnih dizajna dobivenih primjenom teorema 1.2.33 za permutacijsku reprezentaciju grupe $O(7,3)$ na 364 točke i grupe $S(4,9)$ na 1640 točaka (slučaj 2 i 3). Orbitne matrice dobivene su za djelovanje cikličke grupe reda 3 koja na točke dizajna djeluje u orbitama veličine 1 i 3 (s fiksnim točkama).

Dobiveni samoortogonalni kodovi prikazani su u sljedećim tablicama, a poredani su prema 5 slučajeva slabo 3-samoortogonalnih dizajna.

Optimalni kodovi označeni su sa $*$, skoro optimalni sa $**$ i najbolji poznati kodovi označeni su sa $+$. Obzirom na računalna ograničenja, neke podatke u tablicama, kao npr. grupe automorfizama pojedinih kodova ostavljamo prazno jer ih nismo bili u mogućnosti izračunati.

Parametri dizajna	**Parametri koda** C	$\lvert\mathbf{Aut}(C)\rvert$
2-$(364,243,162)$	$[49,9,12]_3$	12999674453557248
	$[105,19,24]_3$	19426432782445054358694712993382400000

Tablica 4.26: Samoortogonalni kodovi dobiveni primjenom teorema 2.1.5 za djelovanje grupe Z_3 s fiksnim točkama (slučaj 1)

Parametri dizajna	**Parametri koda**
1-$(1640,1638,819)$	$[58,19,6]_9$
	$[801,267,3]_3$

Tablica 4.27: Samoortogonalni kodovi dobiveni primjenom teorema 2.1.9 za djelovanje grupe Z_3 s fiksnim točkama (slučaj 2)

Parametri dizajna	**Parametri koda** C	$\mathbf{Aut}(C)$ ili $\lvert\mathbf{Aut}(C)\rvert$
1-$(1640,2,1)$	$[57,19,3]_3$	$Z_2 \times (E_{3^{19}} : (Z_2 \times (E_{2^{18}} : (E_{2^{18}} : S_{19}))))$
	$[801,267,3]_3$	$2^{268} \cdot 267!$

Tablica 4.28: Samoortogonalni kodovi dobiveni primjenom teorema 2.1.13 za djelovanje grupe Z_3 s fiksnim točkama (slučaj 3)

Napomena. Kod $[801,267,3]_3$ iz tablice 4.28 ekvivalentan je onom iz tablice 4.27.

Parametri dizajna	**Parametri koda** C	$\mathbf{Aut}(C)$
2-$(364,121,40)$	$[32,10,5]_9$	
	$[111,6,54]_3$	$Z_2 \times (S_{30} \times (E_{3^4} : ((Z_2 \times (A_6.Z_2)) : Z_2)))$

Tablica 4.29: Samoortogonalni kodovi dobiveni primjenom teorema 2.1.17 za djelovanje grupe Z_3 s fiksnim točkama (slučaj 4.1)

4.2. LCD KODOVI

4.2.1. Djelomična klasifikacija binarnih LCD kodova konstruiranih iz slabo samoortogonalnih dizajna iz A_5

Teorema 1.2.35 primijenili smo za sve grupe G koje su slike svih neregularnih tranzitivnih permutacijskih reprezentacija grupe A_5 (do na ekvivalenciju) stupnja n, $n < 60$. Točnije, za sve $P < G$, $P \neq I$, definirajući osnovni blok dizajna kao uniju orbita podgrupe P za djelovanje na skupu $\{1,\ldots,n\}$, konstruirali smo sve slabo samoortogonalne 1-dizajne na koje grupa G djeluje kao grupa automorfizama.

Opis konstrukcije

Tranzitivne permutacijske reprezentacije grupe A_5 dobili smo koristeći napomenu 1.1.15 u programskom paketu GAP ([28]) na način opisan u poglavlju 4.1.1.

Grupa A_5 ima 7 neekvivalentnih neregularnih tranzitivnih reprezentacija, na 5, 6, 10, 12, 15 i 30 točaka.

Za sve grupe G koje su slike neregularnih tranzitivnih reprezentacija od A_5 (do na ekvivalenciju), primjenom teorema 1.2.35, konstruirali smo dizajne i izdvojili sve, do na izomorfizam, netrivijalne slabo samoortogonalne dizajne.

Konstruirali smo 183 netrivijalna slabo samoortogonalna 1-dizajna. Preciznije, 95 dizajna na 30 točaka, 66 dizajna na 20 točaka, 10 dizajna na 15 točaka, 9 dizajna na 12 točaka i 3 dizajna na 10 točaka.

Konstruirani slabo samoortogonalni dizajni i lista njihovih parametara dostupni su na

https://www.math.uniri.hr/∼inovak/Dizajni/A5.

Za svaku promatranu neregularnu tranzitivnu permutacijsku grupu G, za svaki netrivijalni konstruirani dizajn, primjenom teorema 3.0.4 konstruirali smo LCD kod. Za svaki konstruirani kod odredili smo njegove parametre i grupu automorfizama i ispitali je li ekvivalentan nekom prethodno konstruiranom kodu iz iste permutacijske grupe G.

Dobiveni binarni LCD kodovi

Dobiveni LCD kodovi prikazani su u sljedećim tablicama, a poredani su prema 4 slučaja slabo samoortogonalnih dizajna.

Slučaj 1. Kodovi iz samoortogonalnih dizajna.

Slučaj 2. Kodovi iz slabo samoortogonalnih dizajna s parnom veličinom bloka i neparnim presječnim brojevima dva različita bloka.

Slučaj 3. Kodovi iz slabo samoortogonalnih dizajna s neparnom veličinom bloka i parnim presječnim brojevima dva različita bloka.

Slučaj 4. Kodovi iz slabo samoortogonalnih dizajna s neparnom veličinom bloka i neparnim presječnim brojevima dva različita bloka.

Optimalni kodovi označeni su sa $*$, skoro optimalni sa $**$ i najbolji poznati kodovi označeni su sa $+$. Granice za minimalnu udaljenost binarnih i ternarnih LCD kodova mogu biti više ograničavajuće nego za linearne kodove općenito, obzirom da LCD kodovi zadovoljavaju dodatna ograničenja. Podaci o granicama za minimalnu udaljenost LCD kodova duljine 40 ili manje mogu se pronaći u [8]. Za LCD kodove duljine veće od 40 za provjeru optimalnosti koristili smo [31]. Obzirom na računalna ograničenja, neke podatke u tablicama, kao npr. grupe automorfizama pojedinih kodova ostavljamo prazno jer ih nismo bili u mogućnosti izračunati.

Parametri dizajna	**Parametri koda** C	**Aut**(C) or $\lvert$**Aut**$(C)\rvert$
1-$(30,24,4)$	$[35,5,5]$	23219011584000000
1-$(30,6,1)$	$[35,5,7]$	390241927692288000000
1-$(30,10,2)$	$[36,6,6]$	23592960
1-$(30,20,4)$	$[36,6,6]$	23592960
1-$(30,24,8)$	$[40,10,10]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,12,4)$	$[40,10,3]$	23219011584000000
1-$(30,12,4)$	$[40,10,4]$	23592960
1-$(30,18,6)$	$[40,10,4]$	23219011584000000
1-$(30,18,6)$	$[40,10,4]$	23592960
1-$(30,6,2)$	$[40,10,7]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$

Tablica 4.30: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz samoortogonalnih dizajna na 30 točaka (slučaj 1a)

Parametri dizajna	**Parametri koda** C	**Aut**(C) or $\lvert$**Aut**$(C)\rvert$
1-$(30,2,1)$	$[45,15,3]$	614848852548510547968000
1-$(30,4,2)$	$[45,15,3]$	30576476160
1-$(30,16,8)$	$[45,15,3]$	660602880
1-$(30,20,10)$	$[45,15,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,14,7)$	$[45,15,4]$	660602880
1-$(30,8,4)$	$[45,15,5]$	11796480
1-$(30,10,5)$	$[45,15,6]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,22,11)$	$[45,15,6]$	11796480
1-$(30,26,13)$	$[45,15,6]$	30576476160
1-$(30,28,14)$	$[45,15,6]$	42849873690624000
1-$(30,12,6)$	$[45,15,9]$	23592960
1-$(30,18,9)$	$[45,15,9]$	23592960
1-$(30,12,8)$	$[50,20,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,18,12)$	$[50,20,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,4,4)$	$[60,30,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,8,8)$	$[60,30,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(60,12,12)$	$[60,30,3]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,12,12)$	$[60,30,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,12,12)$	$[60,30,3]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,16,16)$	$[60,30,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,16,16)$	$[60,30,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,16,16)$	$[60,30,3]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,16,16)$	$[60,30,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,20,20)$	$[60,30,3]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,20,20)$	$[60,30,3]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,8,8)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,10,10)$	$[60,30,4]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,10,10)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,12,12)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,14,14)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,14,14)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,14,14)$	$[60,30,4]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,14,14)$	$[60,30,4]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,14,14)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$

Tablica 4.31: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz samoortogonalnih dizajna na 30 točaka (slučaj 1a)

Parametri dizajna	**Parametri koda** C	$\mathbf{Aut}(C)$ or $\lvert\mathbf{Aut}(C)\rvert$
1-$(30,16,16)$	$[60,30,4]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,18,18)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,18,18)$	$[60,30,4]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,18,18)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,20,20)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,22,22)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,22,22)$	$[60,30,4]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,6,6)$	$[60,30,5]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,8,8)$	$[60,30,5]$	23592960
1-$(30,8,8)$	$[60,30,5]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,12,12)$	$[60,30,5]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,16,16)$	$[60,30,5]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,16,16)$	$[60,30,5]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,16,16)$	$[60,30,5]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,20,20)$	$[60,30,5]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,24,24)$	$[60,30,5]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,10,10)$	$[60,30,6]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,10,10)$	$[60,30,6]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,14,14)$	$[60,30,6]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$
1-$(30,14,14)$	$[60,30,6]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,14,14)$	$[60,30,6]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,18,18)$	$[60,30,6]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,18,18)$	$[60,30,6]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,22,22)$	$[60,30,6]$	23592960
1-$(30,22,22)$	$[60,30,6]$	$E_{2^{11}} : (E_{2^4} : A_5)$
1-$(30,26,26)$	$[60,30,6]$	$E_{2^{11}} : ((E_{2^4} : A_5) : Z_2)$

Tablica 4.32: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz samoortogonalnih dizajna na 30 točaka (slučaj 1a)

Parametri dizajna	**Parametri koda** C	$\mathbf{Aut}(C)$ or $\lvert\mathbf{Aut}(C)\rvert$
1-$(20,12,3)$	$[25,5,11]*$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,4,1)$	$[25,5,5]$	$A_5^5 : (Z_2 \times (E_{2^4} : A_5) : Z_2)$
1-$(20,8,2)$	$[25,5,5]$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,16,4)$	$[25,5,5]$	$A_4^5 : (Z_2 \times (E_{2^4} : A_5) : Z_2)$
1-$(20,10,3)$	$[26,6,9]$	61440
1-$(20,2,1)$	$[30,10,3]$	219419659468800
1-$(20,8,4)$	$[30,10,3]$	$A_4^5 : (Z_2 \times (E_{2^4} : A_5) : Z_2)$
1-$(20,12,6)$	$[30,10,3]$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,6,3)$	$[30,10,4]$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,8,4)$	$[30,10,4]$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,12,6)$	$[30,10,4]$	$A_4^5 : (Z_2 \times (E_{2^4} : A_5) : Z_2)$
1-$(20,14,7)$	$[30,10,4]$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,18,9)$	$[30,10,6]$	$(E_{2^9} : A_{10}) : E_{2^2}$
1-$(20,6,3)$	$[30,10,7]$	S_5
1-$(20,14,7)$	$[30,10,9]**$	S_5

Tablica 4.33: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz samoortogonalnih dizajna na 20 točaka (slučaj 1a)

Parametri dizajna	**Parametri koda** C	**Aut**(C) or $\lvert$**Aut**$(C)\rvert$
1-$(20,10,6)$	$[32,12,4]$	S_5
1-$(20,8,6)$	$[35,15,3]$	737280
1-$(20,12,9)$	$[35,15,3]$	737280
1-$(20,8,6)$	$[35,15,5]$	S_5
1-$(20,12,9)$	$[35,15,5]$	S_5
1-$(20,4,3)$	$[35,15,5]$	122880
1-$(20,16,12)$	$[35,15,5]$	122880
1-$(20,6,6)$	$[40,20,4]$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,6,6)$	$[40,20,4]$	A_5
1-$(20,10,10)$	$[40,20,4]$	S_5
1-$(20,10,10)$	$[40,20,4]$	A_5
1-$(20,10,10)$	$[40,20,4]$	S_5
1-$(20,10,10)$	$[40,20,4]$	A_5
1-$(20,10,10)$	$[40,20,4]$	S_5
1-$(20,10,10)$	$[40,20,4]$	S_5
1-$(20,14,14)$	$[40,20,4]$	$E_{2^4} : (E_{2^4} : S_5)$
1-$(20,14,14)$	$[40,20,4]$	A_5
1-$(20,4,6)$	$[50,30,3]$	122880
1-$(20,8,12)$	$[50,30,3]$	61440
1-$(20,8,12)$	$[50,30,3]$	A_5
1-$(20,8,12)$	$[50,30,3]$	S_5
1-$(20,12,18)$	$[50,30,3]$	A_5
1-$(20,12,18)$	$[50,30,3]$	61440
1-$(20,6,9)$	$[50,30,4]$	S_5
1-$(20,6,9)$	$[50,30,4]$	122880
1-$(20,6,9)$	$[50,30,4]$	S_5
1-$(20,6,9)$	$[50,30,4]$	61440
1-$(20,10,15)$	$[50,30,4]$	122880
1-$(20,10,15)$	$[50,30,4]$	A_5
1-$(20,10,15)$	$[50,30,4]$	A_5
1-$(20,10,15)$	$[50,30,4]$	61440
1-$(20,10,15)$	$[50,30,4]$	A_5
1-$(20,10,15)$	$[50,30,4]$	122880
1-$(20,12,18)$	$[50,30,4]$	S_5
1-$(20,14,21)$	$[50,30,4]$	61440
1-$(20,14,21)$	$[50,30,4]$	S_5
1-$(20,14,21)$	$[50,30,4]$	S_5
1-$(20,14,21)$	$[50,30,4]$	122880
1-$(20,16,24)$	$[50,30,4]$	122880

Tablica 4.34: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz samoortogonalnih dizajna na 20 točaka (slučaj 1a)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
2-$(15,8,4)$	$[30,15,3]$	A_8
1-$(15,6,4)$	$[25,10,4]$	S_6
1-$(15,10,4)$	$[21,6,6]$	S_6

Tablica 4.35: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz samoortogonalnih dizajna na 15 točaka (slučaj 1a)

Parametri dizajna	**Parametri koda** C	**Aut**(C) or $\lvert$**Aut**$(C)\rvert$
1-$(12,2,1)$	$[18,6,3]$	33592320
1-$(12,10,5)$	$[18,6,6]**$	$((E_{2^5} : A_6) : Z_2) : Z_2$
1-$(12,6,6)$	$[24,12,4]$	S_5
1-$(12,4,5)$	$[27,15,3]$	$((E_{2^5} : A_6) : Z_2) : Z_2$
1-$(12,6,5)$	$[22,10,4]$	$((E_{2^5} : A_5) : Z_2)$
1-$(12,8,10)$	$[27,15,3]$	$((E_{2^5} : A_6) : Z_2) : Z_2$
1-$(12,6,10)$	$[32,20,4]$	$Z_2 \times A_5$

Tablica 4.36: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz samoortogonalnih dizajna na 12 točaka (slučaj 1a)

Parametri dizajna	**Parametri koda** C	$\lvert$**Aut**$(C)\rvert$
1-$(30,12,2)$	$[31,5,1]$	$(E_{3^{10}}) : (E_{2^6} : (E_{2^4} : S_5))$
1-$(30,18,3)$	$[31,5,12]$	$(E_{3^{10}}) : (E_{2^6} : (E_{2^4} : S_5))$

Tablica 4.37: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz slabo samoortogonalnih dizajna na 30 točaka (slučaj 2c)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(10,4,2)$	$[11,5,1]$	S_5
1-$(10,6,3)$	$[11,5,4]*$	S_5

Tablica 4.38: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz slabo samoortogonalnih dizajna na 10 točaka (slučaj 2a)

Parametri dizajna	**Parametri koda** C	**Aut**(C) or $\lvert$**Aut**$(C)\rvert$
1-$(30,27,9)$	$[30,10,3]$	219419659468800
1-$(30,21,7)$	$[30,10,5]$	A_5
1-$(30,15,5)$	$[30,10,8]$	S_5
1-$(30,25,5)$	$[30,6,5]$	2149908480000000
1-$(30,15,3)$	$[30,6,9]$	$E_{3^{10}} : (E_{2^6} : (E_{2^4} : S_5))$

Tablica 4.39: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz slabo samoortogonalnih dizajna na 30 točaka (slučaj 3a)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(20,15,9)$	$[20,12,4]*$	$Z_2 \times S_5$

Tablica 4.40: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz slabo samoortogonalnih dizajna na 20 točaka (slučaj 3a)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(10,5,3)$	$[10,6,3]*$	S_5

Tablica 4.41: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz slabo samoortogonalnih dizajna na 10 točaka (slučaj 3a)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(15,12,4)$	$[16,5,1]$	$(((Z_3 \times (((E_{3^2} : Z_2) \times (E_{3^2} : Z_2)) : Z_2)) : Z_2) : A_5) : Z_2) : Z_2$
1-$(15,3,1)$	$[15,5,3]$	$(((Z_3 \times (((E_{3^2} : Z_2) \times (E_{3^2} : Z_2)) : Z_2)) : Z_2) : A_5) : Z_2) : Z_2$
2-$(15,7,3)$	$[31,15,4]$	A_8
1-$(15,5,2)$	$[22,6,6]$	S_6
1-$(15,9,6)$	$[26,10,4]$	S_6

Tablica 4.42: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz slabo samoortogonalnih dizajna na 15 točaka (slučaj 2c,3a,4b)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(30,15,6)$	$[43,12,10]$	A_5
1-$(30,15,10)$	$[51,20,4]$	A_5
1-$(30,15,10)$	$[51,20,4]$	S_5
1-$(30,15,10)$	$[51,20,4]$	S_5
1-$(30,15,10)$	$[51,20,4]$	S_5
1-$(30,15,10)$	$[51,20,4]$	S_5
1-$(30,15,10)$	$[51,20,8]$	S_5
1-$(30,15,10)$	$[51,20,8]$	S_5

Tablica 4.43: Netrivijalni binarni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.0.4 iz slabo samoortogonalnih dizajna na 30 točaka (slučaj 4b)

Binarni LCD kodovi iz kvazisimetričnih dizajna

Konstruirali smo LCD kodove iz kvazisimetričnih dizajna, preuzetih sa [34], za koje presječni brojevi daju isti ostatak pri dijeljenju sa 2. Iz navedenih dizajna, koristeći definiciju 1.3.8, konstruirali smo jako regularne grafove i koristeći napomenu 3.0.5, LCD kodove koristeći matrice susjedstva jako regularnih grafova. Dobiveni LCD kodovi konstruiani iz dizajna prikazani su u sljedećoj tablici. U trećem stupcu su prikazani parametri jako regularnih grafova dobivenih kao blokovni grafovi kvazisimetričnih dizajna iz prvog stupca.

Parametri 2-dizajna: (v,k,λ,b,x,y)	**Parametri koda**	$SRG(v,k,\lambda,\mu)$
$(21,6,4,56,0,2)$	$[77,56,4]$ $[78,56,4]$	$SRG(56,45,36,36)$
$(21,7,12,120,1,3)$	$[141,120,4]$ $[142,120,4]$	$SRG(120,77,52,44)$
$(22,6,5,77,0,2)$	$[99,77,4]$	$SRG(77,60,47,45)$
$(22,7,16,176,1,3)$	$[198,176,4]$ $[199,176,4]$	$SRG(176,105,68,54)$
$(23,7,21,253,1,3)$	$[277,253,4]$	$SRG(253,140,87,65)$
$(31,7,7,155,1,3)$	$[187,155,4]$ $[187,155,4]$ $[187,155,4]$ $[187,155,4]$ $[187,155,4]$	$SRG(155,42,17,9)$
$(45,9,8,220,1,3)$	$[265,220,4]$ $[266,220,4]$	$SRG(220,84,38,28)$
$(56,16,18,231,4,8)$	$[287,231,3]$ $[287,231,3]$ $[287,231,3]$ $[287,231,3]$	$SRG(231,30,9,3)$

Tablica 4.44: Binarni LCD kodovi konstruirani iz kvazisimetričnih dizajna i pripadni blokovni jako regularni grafovi

Napomena 4.2.1. Jedini netrivijalni dobiveni LCD kod konstruiran iz jako regularnog grafa je kod s parametrima $[440,220]$ konstruiran koristeći matricu susjedstva jako regularnog grafa (napomena 3.0.5) s parametrima $SRG(220,84,38,28)$ koji je blokovni graf kvazisimetričnog dizajna s parametrima $(45,9,8,220,1,3)$.

4.2.2. Primjeri LCD kodova iz orbitnih matrica slabo p-samoortogonalnih dizajna

Koristeći teorem 1.2.33, konstruirali smo primjere slabo 3-samoortogonalnih dizajna iz grupe $S(4,9)$ na 1640 točaka i slabo 5-samoortogonalnih dizajne iz iste grupe (slučaj 4.2). Iz konstruiranih dizajna, primjenom teorema 3.1.1, 3.1.2, 3.1.3 i 3.1.4 konstruirali smo LCD kodove nad poljem $\mathbb{F}_3$ i $\mathbb{F}_5$. Orbitne matrice navedenih dizajna dobivene su obzirom na djelovanje cikličke grupe reda 5 (Z_5) koja na skup točaka dizajna djeluje u orbitama duljine 5 (bez fiksnih točaka).

Dobiveni kodovi prikazani su u sljedećim tablicama, a poredani su prema 5 slučajeva slabo p-samoortogonalnih dizajna ($p \in \{3,5\}$).

Slučaj 1. Kodovi iz p-samoortogonalnih dizajna.

Slučaj 2. Kodovi iz slabo p-samoortogonalnih dizajna za koje je $a = 0,\ d \neq 0$.

Slučaj 3. Kodovi iz slabo p-samoortogonalnih dizajna za koje je $a \neq 0,\ d = 0$.

Slučaj 4.1 Kodovi iz slabo p-samoortogonalnih dizajna za koje je $a = d \neq 0$.

Slučaj 4.2 Kodovi iz slabo p-samoortogonalnih dizajna za koje je $a \neq 0,\ d \neq 0,\ a \neq d$.

Parametri dizajna	**Parametri koda**
1-$(1640,729,729)$	$[657,328,2]_3$
1-$(1640,1458,729)$	$[492,164,2]_3$ $[493,164,2]_3$

Tablica 4.45: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.1 iz 3-samoortogonalnih dizajna na 1640 točaka (slučaj 1)

Parametri dizajna	**Parametri koda**
1-$(1640,1638,819)$	$[329,164,1]_3$

Tablica 4.46: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.2 iz 3-samoortogonalnih dizajna na 1640 točaka (slučaj 2)

Parametri dizajna	**Parametri koda**
1-$(1640,2,1)$	$[328,164,2]_3$ $[329,164,3]_3$

Tablica 4.47: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.3 iz 3-samoortogonalnih dizajna na 1640 točaka (slučaj 3)

Parametri dizajna	**Parametri koda**
1-$(1640,182,91)$	$[493,164,4]_3$
1-$(1640,911,911)$	$[656,328]_3$

Tablica 4.48: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.4 iz 3-samoortogonalnih dizajna na 1640 točaka (slučaj 4.1)

Parametri dizajna	**Parametri koda**
1-$(1640,1458,729)$	$[328,164,2]_5$
	$[492,164,12]_5$
	$[493,164,12]_5$
	$[329,164,3]_5$
1-$(1640,1638,819)$	$[493,164,3]_5$
	$[493,164,4]_5$

Tablica 4.49: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.4 iz 5-samoortogonalnih dizajna na 1640 točaka (slučaj 4.2)

4.2.3. LCD kodovi iz podmatrica orbitnih matrica slabo 3-samoortogonalnih dizajna

Koristeći teorem 1.2.33, konstruirali smo primjere slabo 3-samoortogonalnih dizajna iz grupe $S(4,9)$ na 1640 točaka i iz konstruiranih dizajna, primjenom teorema 3.1.5, 3.1.6, 3.1.7 i 3.1.8 LCD kodove. Orbitne matrice slabo 3-samoortogonalnih dizajna dobivene su obzirom na djelovanje cikličke grupe reda 3 (Z_3) koja na skup točaka dizajna djeluje u orbitama duljine 1 i 3 (s fiksnim točkama). Dobiveni kodovi prikazani su u sljedećim tablicama, a poredani su prema 5 slučajeva slabo 3-samoortogonalnih dizajna.

Parametri dizajna	**Parametri koda**
1-$(1640,182,91)$	$[57,19,1]_3$
	$[58,19,2]_3$
	$[1068,534]_3$
	$[1069,534]_3$
1-$(1640,729,729)$	$[76,38,1]_3$
	$[801,267]_3$
	$[802,267]_3$

Tablica 4.50: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.5 iz 3-samoortogonalnih dizajna na 1640 točaka (slučaj 1)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(1640,1638,819)$	$[39,19,1]_3$	$E_{2^2} \times (E_{2^{18}} : ((E_{2^{18}} : S_{19}))$
	$[534,267,2]_3$	
	$[535,267,3]_3$	

Tablica 4.51: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.6 iz slabo 3-samoortogonalnih dizajna na 1640 točaka (slučaj 2)

Parametri dizajna	**Parametri koda** C	**Aut**(C)
1-$(1640,2,1)$	$[38,19,2]_3$	$E_{2^2} \times (E_{2^{18}} : (E_{2^{18}} : S_{19}))$
	$[534,267,2]_3$	
	$[535,267,3]_3$	

Tablica 4.52: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.7 iz slabo 3-samoortogonalnih dizajna na 1640 točaka (slučaj 3)

Napomena. Kodovi$[534,267,2]_3$ i $[535,267,3]_3$ iz tablice 4.52 ekvivalentni su kodovima iz tablice 4.51.

Parametri dizajna	**Parametri koda**
1-$(1640, 182, 91)$	$[58, 19, 2]_3$
	$[801, 267]_3$
	$[802, 267]_3$
1-$(1640, 911, 911)$	$[76, 38, 2]_3$
	$[77, 38, 2]_3$
	$[1068, 534]_3$
	$[1069, 534]_3$

Tablica 4.53: Netrivijalni u parovima neekvivalentni LCD kodovi dobiveni primjenom teorema 3.1.8 iz slabo 3-samoortogonalnih dizajna na 1640 točaka (slučaj 4.1)

ZAKLJUČAK

Konstrukcija linearnih kodova iz blokovnih dizajna i orbitnih matrica je jako proučavana tema. U drugom poglavlju disertacije uvedena su proširenja i poopćenja postojećih metoda konstrukcija samoortogonalnih kodova koristeći matrice incidencije, orbitne matrice i podmatrice orbitnih matrica slabo samoortogonalnih dizajna. Uvedene su konstrukcije samoortogonalnih kodova nad proizvoljnim konačnim poljem iz slabo p-samoortogonalnih dizajna.

U trećem poglavlju uvedene konstrukcije su prilagođene s ciljem konstrukcije LCD kodova nad proizvoljnim konačnim poljem. Opisane su konstrukcije LCD kodova koristeći proširenja matrica incidencije, orbitnih matrica i podmatrica orbitnih matrica slabo p-samoortogonalnih dizajna.

Razvijene metode potkrijepljene su parcijalnim klasifikacijama i konkretnim primjerima. U posljednjem, četvrtom poglavlju opisana su i analizirana svojstva dobivenih samoortogonalnih i LCD kodova. Primjenom metoda konstrukcije opisanih u poglavlju 2 dobiveno je 13 optimalnih samoortogonalnih kodova, 5 skoro optimalnih samoortogonalnih kodova i 1 najbolji poznati samodualan kod. Parametri dobivenih kodova prikazani su u tablici 4.54, uz napomenu iz kojih dizajna su konstruirani i primjenom kojeg teorema. Optimalni binarni samoortogonalni kodovi duljine n, $n \leq 25$, su klasificirani u [7]. Također, u istom članku su klasificirani binarni samoortogonalni kodovi duljine n i dimenzije k za $n \leq 40$ i $k \leq 10$.

Primjenom metoda konstrukcije opisanih u poglavlju 3 dobivena su 4 optimalna LCD koda 2 skoro optimalna LCD koda, a njihovi parametri prikazani su u tablici 4.55, uz napomenu iz kojih dizajna su konstruirani i primjenom kojeg teorema.

Parametri koda	Parametri dizajna iz kojih je dobiven	Metoda konstrukcije
$[6,2,4]*$	1-$(22,10,10)$	Teorem 2.1.4
$[10,4,4]*$	1-$(110,72,36)$	Teorem 2.1.2
$[12,2,8]*$	1-$(132,100,100)$	Teorem 2.1.4
$[12,3,6]*$	1-$(132,66,6)$	Teorem 2.1.4
$[12,5,4]*$	1-$(132,40,40)$	Teorem 2.1.2
$[12,5,4]*$	1-$(132,46,46)$	Teorem 2.1.2
$[12,6,4]*$	1-$(66,45,45)$	Teorem 2.1.10
$[12,11,2]*$	1-$(132,22,2)$	Teorem 2.1.2
$[15,4,8]*$	1-$(165,48,48)$	Teorem 2.1.2
$[24,12,8]*$	1-$(132,27,27)$	Teorem 2.1.10
$[16,5,8]*$	1-$(165,109,109)$	Teorem 2.1.14
$[31,15,8]*$	1-$(165,116,116)$	Teorem 2.1.6
$[9,2,6]_3*$	1-$(30,21,7)$	Teorem 2.1.7
$[6,3,2]**$	1-$(22,2,1)$	Teorem 2.1.4
$[10,3,4]**$	1-$(66,46,46)$	Teorem 2.1.4
$[14,6,4]**$	1-$(110,72,72)$	Teorem 2.1.4
$[64,4,32]**$	1-$(132,55,5)$	Teorem 2.1.12
$[30,4,18]_3**$	1-$(30,18,3)$	Teorem 2.0.4
$[96,48,16]+$	1-$(144,23,23)$	Teorem 2.1.10

Tablica 4.54: Optimalni $(*)$, skoro optimalni $(**)$ i najbolji poznati $(+)$ samoortogonalni kodovi

Parametri koda	Parametri dizajna iz kojih je dobiven	Metoda konstrukcije
$[10,6,3]*$	1-$(10,5,3)$	Teorem 3.0.4
$[11,5,4]*$	1-$(10,6,3)$	Teorem 3.0.4
$[20,12,4]*$	1-$(20,15,9)$	Teorem 3.0.4
$[25,5,11]*$	1-$(20,12,3)$	Teorem 3.0.4
$[18,6,6]**$	1-$(12,10,5)$	Teorem 3.0.4
$[30,10,9]**$	1-$(20,14,7)$	Teorem 3.0.4

Tablica 4.55: Optimalni $(*)$ i skoro optimalni $(**)$ LCD kodovi

BIBLIOGRAFIJA

[1] Assmus, E. F. i J. D. Key: *Designs and their codes*. Cambridge University Press, Cambridge, 1992. ↑ 1, 10.

[2] Baartmans, A., I. Landjev i V. D. Tonchev: *On the binary codes of Steiner triple systems*. Des. Codes Cryptogr., 8:29–43, 1996. ↑ 1.

[3] Balakrishnan, R. i K. Ranganathan: *A Textbook of Graph Theory*. Springer, New York, 2012. ↑ 22.

[4] Biggs, N. L. i A. L. White: *Permutation Groups and Combinatorial Structures*. Cambridge University Press, Cambridge, 1979. ↑ 9, 10, 12.

[5] Bose, R. C.: *Strongly regular graphs, partial geometries and partially balanced designs*. Pacific J. Math., 13:389–419, 1963. ↑ 23.

[6] Bosma, Wieb, John Cannon i Catherine Playoust: *The Magma algebra system. I. The user language*. J. Symbolic Comput., 24(3-4):235–265, 1997, ISSN 0747-7171. http://dx.doi.org/10.1006/jsco.1996.0125, Computational algebra and number theory (London, 1993). ↑ iii, iv.

[7] Bouyukliev, I., S. Bouyuklieva, T. A. Gulliver i P. R. J. Ostergard: *Classification of optimal binary self-orthogonal codes*. Journal of Combinatorial Mathematics and Combinatorial Computing, 59:33–87, 2006. ↑ 114.

[8] Bouyuklieva, S.: *Optimal binary LCD codes*. Des. Codes Cryptogr., https://doi.org/10.1007/s10623-021-00929-w, 2021. ↑ 2, 101.

[9] Cameron, P. J.: *Extending symmetric designs*. J. Combinatorial Theory Ser. A, 14:215–220, 1973. ↑ 19.

[10] Cameron, P. J.: *Near-regularity conditions for designs*. Geometriae Dedicata, 2:213–223, 1973. ↑ 18.

[11] Cameron, P. J.: *Permutation Groups*. Cambridge University Press, 1999. ↑ 6.

[12] Cameron, P. J. i J. H. Van Lint: *Designs, Graphs, Codes and their Links*. Cambridge University Press, 1991. ↑ 17.

[13] Carlet, C. i S. Guilley: *Complementary dual codes for counter-measures to side-channel attacks*. Adv. Math. Commun., 10:131–150, 2016. ↑ 2.

[14] Carlet, C., S. Mesnager, C. Tang i Y. Qi: *Linear codes over Fq which are equivalent to LCD codes*. IEEE Trans. Inform. Theory, 64:3010–3017, 2018. ↑ 2.

[15] Chigira, N., M. Harada i M. Kitazume: *Permutation groups and binary self-orthogonal codes*. J. Algebra, 309:610–621, 2007. ↑ 1.

[16] Crnković, D., R. Egan, B. G. Rodrigues i A. Švob: *LCD codes from weighing matrices*. Appl. Algebra Engrg. Comm. Comput., 32:175–189, 2021. ↑ 2.

[17] Crnković, D., V. Mikulić Crnković i B. G. Rodrigues: *On self-orthogonal designs and codes related to Held's simple group*. Adv. Math. Commun., 12:607–628, 2018. ↑ 1, 2, 31, 32, 39, 40.

[18] Crnković, D., V. Mikulić Crnković i A. Švob: *On some transitive combinatorial structures constructed from the unitary group $U(3,3)$*. J. Statist. Plann. Inference, 144:19–40, 2014. ↑ 1, 20.

[19] Crnković, D., D. Dumičić Danilović i S. Rukavina: *On symmetric (78,22,6) designs and related self-orthogonal codes*. Util. Math., 109:227–253, 2018. ↑ 1.

[20] Crnković, D., R. Egan i A. Švob: *Constructing self-orthogonal and Hermitian self-orthogonal codes via weighing matrices and orbit matrices*. Finite Fields Appl., 55:64–77, 2019. ↑ 1.

[21] Crnković, D. i N. Mostarac: *Self-dual codes from orbit matrices and quotient matrices of combinatorial designs*. Discrete Mathematics, 341:3331–3343, 2018. ↑ 1.

[22] Crnković, D., B. G. Rodrigues, L. Simčić i S. Rukavina: *Self-orthogonal codes from orbit matrices of 2-designs*. Adv. Math. Commun., 7:161–174, 2013. ↑ 1.

[23] Crnković, D. i S. Rukavina: *Self-dual codes from extended orbit matrices of symmetric designs*. Des. Codes Cryptogr., 79:113–120, 2016. ↑ 1.

[24] Ding, C., C. Li i S. Li: *LCD Cyclic codes over finite fields*. IEEE Trans. Inform. Theory, 63:4344–4356, 2017. ↑ 2.

[25] Dixon, J. D. i B. Mortimer: *Permutation groups*. Springer, New York, 1996. ↑ 7.

[26] Dougherty, S. T., J L. Kim, B. Ozkaya, L. Sok i P. Solé: *The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices*. Int. J. Inf. Coding Theory, 4:116–128, 2017. ↑ 2.

[27] Dumičić Danilović, D.: *Poopćenje i profinjenje nekih algoritama za konstrukciju blokovnih dizajna i istraživanje njihovih podstruktura*. Doktorska disertacija, 2014. ↑ 20.

[28] The GAP Group: *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021. https://www.gap-system.org. ↑ iii, iv, 80, 100.

[29] Goethals, J. M. i J. Seidel: *Strongly regular graphs derived from combinatorial designs*. Canad. J. Math., 22:597–614, 1970. ↑ 23.

[30] Golay, M. J. E.: *Notes on digital coding*. In Proceedings of the I. R. E., 37:657, 1949. ↑ 24.

[31] Grassl, M.: *Tables of Bounds on Linear and Quantum Error-Correcting Codes at www.codetables.de*. ↑ 82, 101.

[32] Hamming, R. W.: *Error detecting and error correcting codes*. Bell Syst. Tech. J., 29:147–160, 1950. ↑ 24.

[33] Harada, M. i V. D. Tonchev: *Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms*. Discrete Math., 264:81–90, 2003. ↑ 1.

[34] Krčadinac, V.: *Quasi-symmetric designs, https://web.math.pmf.unizg.hr/ krcko/results/quasisym.html*. ↑ 55, 108.

[35] Lang, S.: *Algebra*. Revised Third Edition, Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2005. ↑ 8.

[36] MacWilliams, F. J. i N. J. A. Sloane: *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1998. ↑ 25.

[37] Massey, J. L.: *Linear codes with complementary duals*. Discrete Math., 106/107:337–342, 1992. ↑ 1, 26.

[38] Mikulić Crnković, V. i I. Traunkar: *Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of M_{11}*. AAECC, https://doi.org/10.1007/s00200-020-00484-2, 2021. ↑ 27.

[39] Shannon, C. E.: *A mathematical theory of communication*. The Bell System Technical Journal, Springer-Verlag, 27:379–423, 623–656, 1948. ↑ 1, 24.

[40] Shrikhande, S. S.: *Quasi-symmetric designs, Handbook of combinatorial designs*. Discrete Mathematics and its Applications (Boca Raton), 2:578–582, 2007. ↑ 19.

[41] Soicher, L. H.: *DESIGN, The Design Package for GAP, Version 1.7*. https://gap-packages.github.io/design, Mar 2019. Refereed GAP package. ↑ iii, iv.

[42] Stinson, D. R.: *Combinatorial Designs: Construction and Analysis*. Springer-Verlag, New York, 2004. ↑ 16, 17, 18.

[43] Tonchev, V. D.: *Self-Orthogonal Designs and Extremal Doubtly-Even Codes*. Journal of Combinatorial Theory, Series A 52:197–205, 1989. ↑ 1, 2, 27.

[44] Tonchev, V. D.: *Quantum Codes from Finite Geometry and Combinatorial Designs, Finite Groups, Vertex Operator Algebras, and Combinatorics*. Research Institute for Mathematical Sciences, 1656:44–54, 2009. ↑ 1.

[45] Yang, X. i J. L. Massey: *The condition for a cyclic code to have a complementary dual*. Discrete Math., 126:391–393, 1994. ↑ 2.

[46] Yorgova, R.: *On decoding of a specific type of self-dual codes*. arXiv: 2106.11146. ↑ 1.

ŽIVOTOPIS

Ivona Traunkar rođena je 10.10.1989. godine u Rijeci gdje je završila osnovnu školu i prirodoslovno - matematičku gimnaziju. Završila je preddiplomski studij matematike 2011. godine na Odjelu za matematiku Sveučilišta u Rijeci. Iste godine upisala je diplomski studij matematike Diskretna matematika i primjene i završila ga 2013. godine. Nakon završetka studija upisala je zajednički sveučilišni doktorski studij matematike sveučilišta u Osijeku, Rijeci, Splitu i Zagrebu, čiji je nositelj Matematički odsjek Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Od listopada 2013. godine radi kao asistent na Odjelu za matematiku Sveučilišta u Rijeci, gdje je članica Zavoda za diskretnu matematiku.

Znanstveno se usavršavala sudjelujući na međunarodnim ljetnim školama matematike "2021 PhD Summer School in Discrete Mathematics" (lipanj 2021., Rogla, Slovenija) i "Summer school of finite geometry: Finite Geometry and Friends" (lipanj 2019., Brisel, Belgija). Aktivno je sudjelovala na međunarodimm znanstvenim skupovima "HyGraDe - Hypergraphs, Graphs and Designs" (lipanj 2017., Sicilija, Italija) i "6th Croatian Mathematical Congress" (lipanj 2016., Zagreb).

Koautorica je jednog znanstvenog članka: Mikulić Crnković, V. , Traunkar, I.: *Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of* M_{11}, AAECC (2021) (https://doi.org/10.1007/s00200-020-00484-2).

Članica je Društva matematičara i fizičara, Alumni kluba Odjela za matematiku i Seminara za konačnu matematiku, u sklopu kojega je održala niz seminara.