Dizajni tranzitivni po incidencijama

Šubašić, Aljoša

ZAJEDNIČKI SVEUČILIŠNI POSLIJEDIPLOMSKI

DOKTORSKI STUDIJ MATEMATIKE

Aljoša Šubašić

DIZAJNI TRANZITIVNI PO INCIDENCIJAMA

DOKTORSKI RAD

Zagreb, 2017.

CROATIAN DOCTORAL PROGRAM IN
MATHEMATICS

Aljoša Šubašić

FLAG-TRANSITIVE DESIGNS

DOCTORAL THESIS

Zagreb, 2017

ZAJEDNIČKI SVEUČILIŠNI POSLIJEDIPLOMSKI

DOKTORSKI STUDIJ MATEMATIKE

ALJOŠA ŠUBAŠIĆ

DIZAJNI TRANZITIVNI PO INCIDENCIJAMA

DOKTORSKI RAD

Mentor:
izv. prof. dr. sc. Joško Mandić

Zagreb, 2017.

CROATIAN DOCTORAL PROGRAM IN

MATHEMATICS

ALJOŠA ŠUBAŠIĆ

FLAG-TRANSITIVE DESIGNS

DOCTORAL THESIS

Supervisor:
assoc. prof. dr. sc. Joško Mandić

Zagreb, 2017

ZAHVALE

Prije svega veliko hvala mom mentoru, hodajućoj matematičkoj enciklopediji, profesoru Jošku Mandiću na svim idejama, savjetima i strpljenju koji su, u konačnici, doveli do ove disertacije. Teško bi bilo pobrojati sve kave koje smo popili radeći zajedno pri čemu je bio nepresušan izvor znanja i inspiracije za samostalni rad.

Zahvaljujem profesorima Tanji Vučičić, Vedranu Krčadincu, Mariu-Osvinu Pavčeviću te svim članovima Seminara za diskretnu matematiku u Splitu na korisnim savjetima, primjedbama i idejama.

Nadalje, hvala i osobi koju sam s ponosom nekad nazivao svojim profesorom, a danas prijateljem - Jurici Ćudini, što je svojim entuzijazmom i strašću za matematikom i mene skrenuo na ovaj put na kojem se danas nalazim.

Konačno, želim se zahvaliti svim kolegama, među kojima bih posebno istaknuo Nikolu Koceića Bilana i Snježanu Braić, te obitelji i prijateljima na neizostavnoj podršci i razumijevanju tijekom izrade ove disertacije. Ovaj rad je za njih.

Sažetak

U ovoj disertaciji izloženo je istraživanje iz područja teorije dizajna. Pri konstrukciji dizajna koristimo permutacijske grupe za koje pretpostavljamo da djeluju tranzitivno po točkama i blokovima traženog dizajna. Istražujemo posebno one dizajne koji imaju grupu automorfizama koja djeluje tranzitivno po incidencijama. Elementarna podjela tranzitivnih grupa je na primitivne i imprimitivne pa s obzirom na djelovanje po točkama razlikujemo primitivne i imprimitivne dizajne s obzirom na danu grupu automorfizama. U radu su konstruirani i popisani svi primitivni dizajni tranzitivni po incidencijama koji imaju do 30 točaka.

Nadalje, među imprimitivnim dizajnima, potraženi su oni simetrični i tranzitivni po incidencijama kojima je parametar λ manji ili jednak 10. Ključni teorem u toj potrazi dali su Praeger i Zhou u [18] pri čemu su ograničili izbor parametara takvih dizajna. U ovom radu istraživani su dosad neistraženi slučajevi. Za dani imprimitivni dizajn i sustav imprimitivnosti grupe automorfizama definiramo kvocijentni dizajn te poddizajn s obzirom na blok imprimitivnosti danog sustava. Neegzistencija jednog od njih povlači i neegzistenciju traženog imprimitivnog dizajna. Također, razvijena je teorija pomoću koje se analiziraju i eliminiraju neki od preostalih slučajeva. Pritom je korištena teorija permutacijskih grupa, proširenja grupa te njihovih linearnih reprezentacija nad konačnim poljima.

Pri konstrukciji dizajna i analizi pojedinih slučajeva korištena je podrška programskog paketa MAGMA [3] te su dani i algoritmi uz pomoć kojih je ta konstrukcija odnosno analiza provedena.

Abstract

In this thesis, research in the field of design theory is presented. For the construction of designs we use permutation groups that we assume are transitive on points and blocks of the required design. Specifically, we investigated those designs that have a group of automorphisms that is flag-transitive. Among transitive groups we distinguish primitive and imprimitive ones, and depending on the action on points we distinguish primitive and imprimitive designs with respect to the given group of automorphisms. All flag-transitive primitive designs with up to 30 points have been constructed and listed.

Furthermore, among imprimitive designs, we looked for the symmetric flag-transitive ones when parameter λ is less than or equal to 10. The key theorem in this quest was given by Praeger and Zhou in [18], limiting the choice of parameters of such designs. In this thesis, we provide insight into the previously unexplored cases. For the given imprimitive design and system of imprimitivity of the group of automorphisms, we define the quotient design and subdesign with respect to the block of imprimitivity of the given system. The non-existence of one of them entails the non-existence of the required imprimitive design. Furthermore, we developed a theory to analyze and eliminate some of the remaining cases. Theory of permutation groups, group extensions and their linear representations on finite fields was used.

For constructing and analyzing certain cases, the support of the MAGMA software package [3] was used, and the algorithms with which the construction or analysis was carried out are given.

Sadržaj

Poglavlje 1

Uvod

1.1 Grupe

U uvodu ćemo dati neke pojmove i rezultate iz teorije grupa koji se koriste u radu u svrhu lakšeg razumijevanja teksta kao i upoznavanja s uvedenim oznakama. Većina pojmova iz teorije grupa može se pronaći u [1, 21]. Također je važno napomenuti da za sve grupe u radu pretpostavljamo da su konačne, jer samo takve i koristimo pri konstrukciji dizajna.

Teorem 1.1 (Prvi teorem o izomorfizmu) *Neka je $f : G \to H$ homomorfizam grupa. Tada je $Kerf \trianglelefteq G$, $\operatorname{Im} f \leq H$ i preslikavanje*

$$f' : G/Kerf \to \operatorname{Im} f, \text{ dano s } f'(gKerf) := f(g),$$

je izomorfizam grupa, to jest

$$G/Kerf \cong \operatorname{Im} f.$$

Teorem 1.2 (Drugi teorem o izomorfizmu) *Neka je G grupa, $A \leq G$ neka podgrupa od G i $N \trianglelefteq G$ neka normalna podgrupa od G. Tada je*

$$A/(A \cap N) \cong AN/N.$$

Teorem 1.3 (Treći teorem o izomorfizmu) *Neka je G grupa i neka su $M, N \trianglelefteq G$ dvije normalne podgrupe od G takve da je $N \leq M$. Tada je*

$$(G/N)/(M/N) \cong G/M.$$

Za grupu G, sa $C(G) = \langle xyx^{-1}y^{-1} \mid x, y \in G\rangle$ označavamo **komutatorsku podgrupu grupe** G. Induktivno definiramo podgrupu $C^k(G)$, za svaki $k \in \mathbb{N}$, s

$$C^1(G) = C(G) \text{ i } C^k(G) = C(C^{k-1}(G)), \text{ za } k \geq 2.$$

Definicija 1.4 *Kažemo da je grupa G **rješiva** ako postoji prirodan broj n takav da je $C^n(G) = 1_G$.*

Teorem 1.5 *Neka je G grupa, H podgrupa od G i N normalna podgrupa od G. Tada vrijedi:*

a) Ako je grupa G rješiva, onda je i grupa H rješiva.

b) Ako je grupa G rješiva, onda je i grupa G/N rješiva.

c) Ako su grupe G/N i N rješive, onda je i grupa G rješiva.

Definicija 1.6 *Neka je G grupa, A neki podskup od G i $x \in G$ bilo koji element iz G. Definiramo **centralizator elementa** x kao*

$$C_G(x) := \{g \in G \mid gx = xg\},$$

*i općenitije **centralizator skupa** A kao*

$$C_G(A) := \{g \in G \mid gx = xg, \text{ za svaki } x \in A\}.$$

Definicija 1.7 *Neka je p prost broj. Podgrupu H grupe G nazivamo **p-podgrupom** od G ako je H reda p^n za neki prirodan broj n.*

Definicija 1.8 *Podgrupu H konačne grupe G nazivamo **Sylowljevom p-podgrupom** od G ako je H p-podgrupa od G i indeks $[G : H]$ nije djeljiv s p.*

Teorem 1.9 (Prvi Sylowljev teorem) *Neka je G konačna grupa reda n i p prost broj koji dijeli n. Tada postoji Sylowljeva p-podgrupa grupe G.*

Teorem 1.10 (Drugi Sylowljev teorem) *Neka je G konačna grupa reda n i p prost broj koji dijeli n. Tada vrijedi:*

a) Svaka p-podgrupa grupe G sadržana je u nekoj Sylowljevoj p-podgrupi grupe G.

b) Sve Sylowljeve p-podgrupe od G međusobno su konjugirane.

Teorem 1.11 (Treći Sylowljev teorem) *Neka je G konačna grupa reda n, p prost broj koji dijeli n i syl_p broj Sylowljevih p-podgrupa od G. Tada je*

$$syl_p \equiv 1 \pmod p \ \ i \ \ syl_p \mid n.$$

Definicija 1.12 *Podgrupu H konačne grupe G nazivamo **Hallovom** ako su $|H|$ i $[G : H]$ relativno prosti brojevi. Kažemo da je H **p'-Hallova** podgrupa od G ako je Hallova i $[G : H] = p^n$ za neki $n \in \mathbb{N}$.*

Propozicija 1.13 ([11]) *Neka je G rješiva grupa reda n i $d \mid n$ takav da su d i $\frac{n}{d}$ relativno prosti. Tada postoji Hallova podgrupa od G reda d.*

Definicija 1.14 *Neka su H, K grupe. Za grupu G kažemo da je **proširenje grupe** H **grupom** K i pišemo $G = H.K$ ako postoji $N \trianglelefteq G$ takva da je $N \cong H$ i $G/N \cong K$.*

Za dane grupe H, K uvijek postoji proširenje $H.K$ (barem $H \times K$), međutim takvo proširenje ne mora biti jedinstveno.

1.2 Djelovanja grupa

Definicija 1.15 *Neka je G grupa i Ω skup.* ***Djelovanje grupe** G **na skup** Ω je preslikavanje $\pi : G \times \Omega \to \Omega$ koje zadovoljava sljedeća svojstva:*

1) $\pi(g, \pi(h, \omega)) = \pi(gh, \omega)$ za sve $g, h \in G$ i sve $\omega \in \Omega$;

2) $\pi(1_G, \omega) = \omega$ za sve $\omega \in \Omega$.

Primjer 1.16 *Neka je G grupa. Preslikavanje $\pi : G \times G \to G$ dano s $\pi(g, x) = gx$, za sve $g, x \in G$, je djelovanje grupe G na samu sebe. Nazivamo ga **lijevim množenjem u grupi**.*

Primjer 1.17 *Neka je G grupa. Preslikavanje $\pi : G \times G \to G$ dano s $\pi(g, x) = gxg^{-1}$, za sve $g, x \in G$, je djelovanje grupe G na samu sebe. Nazivamo ga **konjugacijom**.*

Često ćemo, na mjestima gdje je jasno ili nebitno o kojem je djelovanju riječ, radi jednostavnosti zapisa, sliku djelovanja $\pi(g, \omega)$ zapisivati s $g\omega$. Također, za svaki $\Delta \subseteq \Omega$ uvodimo oznaku $g\Delta := \{\pi(g, \delta) \mid \delta \in \Delta\}$.

U narednim definicijama fiksne točke, stabilizatora i orbite jasno je da one ovise o samom djelovanju pa bi umjesto primjerice "fiksna točka skupa S" bilo ispravno reći "fiksna točka skupa S s obzirom na djelovanje π". Međutim, zbog jednostavnosti zapisa i konteksta samih definicija, koristit ćemo prvi zapis.

Definicija 1.18 *Neka je $\pi : G \times \Omega \to \Omega$ djelovanje grupe G na skup Ω, $S \subseteq G$ neki podskup od G i $\omega \in \Omega$. Kažemo da je ω **fiksna točka skupa** S ako je $\pi(g, \omega) = \omega$ za svaki $g \in S$. Posebice, ako je $S = \{g\}$, onda kažemo da je ω **fiksna točka elementa** g.*

Skup svih fiksnih točaka elementa $g \in G$ s obzirom na dano djelovanje π označavamo s F_g, tj.

$$F_g = \{\omega \in \Omega \mid \pi(g, \omega) = \omega\}.$$

Definicija 1.19 *Neka je $\pi : G \times \Omega \to \Omega$ djelovanje grupe G na skup Ω. Skup*

$$K_\pi = \{g \in G \mid F_g = \Omega\}$$

*nazivamo **jezgrom djelovanja** π. Djelovanje π nazivamo **vjernim** ako je $K_\pi = \{1_G\}$.*

Primijetimo da je lijevo množenje u grupi vjerno djelovanje.

Definicija 1.20 *Neka je $\pi : G \times \Omega \to \Omega$ djelovanje grupe G na skup Ω i neka je $\omega \in \Omega$ i $\Delta \subseteq \Omega$. Skup*

$$G_\omega = \{g \in G \mid \pi(g, \omega) = \omega\}$$

*nazivamo **stabilizatorom točke** ω.*

Skup

$$G_\Delta = \{g \in G \mid \pi(g, \Delta) = \Delta\}$$

*nazivamo **stabilizatorom skupa** Δ.*

Skup

$$G_{(\Delta)} = \{g \in G \mid \pi(g, \delta) = \delta, \textit{za svaki } \delta \in \Delta\}$$

*nazivamo **stabilizatorom skupa Δ po točkama**.*

Za svaki $\omega \in \Omega$ vrijedi $1_G \in G_\omega$. Također, lako se vidi da su G_ω, G_Δ i $G_{(\Delta)}$ podgrupe grupe G.

Definicija 1.21 *Neka je $\pi : G \times \Omega \to \Omega$ djelovanje grupe G na skup Ω, $H \leq G$ i $\Delta \subseteq \Omega$. Za skup Δ kažemo da je H-skup ako je $H \leq G_\Delta$.*

Definicija 1.22 *Neka je $\pi : G \times \Omega \to \Omega$ djelovanje grupe G na skup Ω i neka je $\omega \in \Omega$. Skup*

$$G\omega = \{\pi(g, \omega) \mid g \in G\}$$

*nazivamo G-**orbitom** ili **stazom** točke ω. Broj $|G\omega|$ nazivamo **duljinom** G-orbite točke ω.*

Relacija na skupu Ω definirana s

$$\omega_1 \sim \omega_2 \Leftrightarrow (\exists g \in G)\ g\omega_1 = \omega_2$$

je relacija ekvivalencije čije su klase

$$[\omega] = \{\omega' \in \Omega \mid \omega \sim \omega'\} = \{g\omega \mid g \in G\} = G\omega,$$

pa je skup svih G-orbita na Ω particija skupa Ω koju označavamo s

$$\Omega \mid G = \{G\omega \mid \omega \in \Omega\}.$$

Propozicija 1.23 *Neka grupa G djeluje na skup Ω. Tada je*

$$|G\omega| = [G : G_\omega] = \frac{|G|}{|G_\omega|}, \text{ za svaki } \omega \in \Omega.$$

Dokaz. Pokažimo da je pravilom $f(g\omega) = gG_\omega$ dobro definirana funkcija $f : G\omega \to G/G_\omega$. Neka je $g\omega = g'\omega$. Tada je $g^{-1}g'\omega = \omega$ pa je $g^{-1}g' \in G_\omega$ tj. $g' \in gG_\omega$. Sada je $gG_\omega = g'G_\omega$. Kako se lako vidi da je ta funkcija bijekcija, to su skupovi $G\omega$ i G/G_ω ekvipotentni. ■

Propozicija 1.24 *Neka grupa G djeluje na skup Ω i neka je $H \leq G$. Tada je svaka G-orbita na Ω unija nekih H-orbita na Ω.*

Dokaz. Neka je $[G : H] = k$. Tada je $G = \bigcup_{i=1}^{k} Hg_i$ za neke $g_i \in G$, pa za proizvoljni $\omega \in \Omega$ vrijedi

$$G\omega = \bigcup_{i=1}^{k} Hg_i\omega = \bigcup_{i=1}^{k} H(g_i\omega)$$

čime je tvrdnja dokazana. ■

Propozicija 1.25 *Neka grupa G djeluje na skup Ω i neka je o broj različitih G-orbita na Ω. Tada je*

$$o = \frac{1}{|G|} \sum_{g \in G} |F_g| \, .$$

Dokaz. Prebrojimo skup $\{(g, \omega) \mid g \in G, \omega \in \Omega, g\omega = \omega\}$. S jedne strane,

$$|\{(g, \omega) \mid g \in G, \omega \in \Omega, g\omega = \omega\}| = \sum_{g \in G} |F_g| \, .$$

S druge strane,

$$\begin{aligned} |\{(g, \omega) \mid g \in G, \omega \in \Omega, g\omega = \omega\}| &= \sum_{\omega \in \Omega} |G_\omega| \\ &= \sum_{\omega \in \Omega} \frac{|G|}{|G\omega|} \\ &= |G| \sum_{\omega \in \Omega} \frac{1}{|G\omega|} \\ &= |G| \cdot o. \end{aligned}$$

Izjednačavanjem desnih strana ovih jednakosti dobivamo traženu relaciju.

■

Definicija 1.26 *Kažemo da je djelovanje grupe G* ***tranzitivno*** *na skupu Ω ako za svaka dva elementa $\omega_1, \omega_2 \in \Omega$ postoji $g \in G$ takav da je $g\omega_1 = \omega_2$.*

Alternativno možemo reći da je djelovanje grupe G tranzitivno na skupu Ω ako je skup Ω G-orbita bilo koje svoje točke.

Definicija 1.27 *Kažemo da je djelovanje grupe G* ***semiregularno*** *na skupu Ω ako je $G_\omega = \{1_G\}$, za svaki $\omega \in \Omega$.*

Definicija 1.28 *Kažemo da je djelovanje grupe G* ***regularno*** *na skupu Ω ako je tranzitivno i semiregularno na Ω.*

Definicija 1.29 *Za grupu koja djeluje tranzitivno (semiregularno, regularno) na skupu* Ω *kažemo da je* ***tranzitivna (semiregularna, regularna)*** *na* Ω.

Propozicija 1.30 *Neka je* G *grupa koja djeluje tranzitivno na* Ω, $H \leq G$, *i* G_ω *stabilizator točke* $\omega \in \Omega$. *Tada vrijedi*

$$G = G_\omega H = HG_\omega \Leftrightarrow H \text{ je tranzitivna na } \Omega.$$

Posebno, jedina tranzitivna podgrupa od G *koja sadrži* G_ω *je sama grupa* G.

Dokaz. Budući da za $H, K \leq G$ vrijedi $HK \leq G \Leftrightarrow HK = KH$ onda iz $G = HG_\omega$ slijedi $G_\omega H = HG_\omega$.

Neka je $G = HG_\omega$. Kako je G tranzitivna na Ω vrijedi $G\omega = \Omega$. Kako je $G = HG_\omega$, to je $HG_\omega\omega = H\omega = \Omega$ pa je H tranzitivna na Ω.

Obratno, neka je H tranzitivna na Ω i $g \in G$. Zbog tranzitivnosti od H postoji $h \in H$ takav da je $h\omega = g\omega$. Onda je $h^{-1}g \in G_\omega$ pa je $g \in HG_\omega$. ∎

Definicija 1.31 *Neka je* $\pi : G \times \Omega \to \Omega$ *tranzitivno djelovanje grupe* G *na skup* Ω. *Particiju* $\{\Delta_i \subseteq \Omega : i \in \{1, .., d\}\}$ *skupa* Ω *takvu da za svaki* $i \in \{1, .., d\}$ *i za svaki* $g \in G$ *postoji* $j \in \{1, .., d\}$ *takav da je* $g\Delta_i = \Delta_j$ *nazivamo* ***blokovnim sustavom*** *djelovanja* π.

Svako tranzitivno djelovanje ima bar dva trivijalna blokovna sustava: particiju na jednočlane skupove i cijeli skup Ω.

Netrivijalni blokovni sustav nazivamo **sustavom imprimitivnosti**. Njegove elemente nazivamo **blokovima imprimitivnosti**.

Propozicija 1.32 *Neka je* $\pi : G \times \Omega \to \Omega$ *tranzitivno djelovanje grupe* G *na skup* Ω *i neka je* $N \trianglelefteq G$ *normalna podgrupa grupe* G. *Tada skup svih* N*-orbita na* Ω *tvori blokovni sustav.*

Dokaz. Neka su $g \in G$ i $\omega \in \Omega$ proizvoljni. Vrijedi $gN\omega = Ng\omega$, tj. g preslikava N-orbitu točke ω u N-orbitu točke $g\omega$. Dakle, svaki $g \in G$ čuva skup N-orbita. ■

Definicija 1.33 *Vjerno tranzitivno djelovanje nazivamo* ***primitivnim*** *ako dopušta samo trivijalne blokovne sustave. Inače ga nazivamo* ***imprimitivnim****.*

Propozicija 1.34 *Svaka netrivijalna normalna podgrupa primitivne grupe je tranzitivna.*

Dokaz. Tvrdnja slijedi direktno iz Propozicije 1.32. ■

Definicija 1.35 *Neka je Ω konačan skup. Grupu svih bijekcija (permutacija) $f : \Omega \to \Omega$, obzirom na kompoziciju kao binarnu operaciju, nazivamo* ***simetričnom grupom*** *na Ω i označavamo sa $Sym(\Omega)$. Podgrupu $G \leq Sym(\Omega)$ nazivamo* ***permutacijskom grupom*** *na Ω.*

Propozicija 1.36 *Neka permutacijska grupa G djeluje tranzitivno na skup Ω koji ima barem dva elementa. Tada je G primitivna ako i samo ako je za svaki $\omega \in \Omega$ stabilizator G_ω maksimalna podgrupa od G.*

Dokaz. Neka je H podgrupa od G koja sadrži G_ω. Prvo pokažimo da orbite podgrupe H tvore blokovni sustav. Dovoljno je pokazati da za svaki $g \in G$ iz $gH\omega \cap H\omega \neq \emptyset$ slijedi $gH\omega = H\omega$. Pretpostavimo da je $gH\omega \cap H\omega \neq \emptyset$, tj. da postoje h_1,$h_2 \in H$ takvi da je $gh_1\omega = h_2\omega$. No tada je $h_2^{-1}gh_1 \in G_\omega$, tj. $g \in h_2G_\omega h_1^{-1}$ pa je $g \in H$, a onda je i $gH\omega = H\omega$.

Dakle, orbite od H tvore blokovni sustav koji je, po Propoziciji 1.30, trivijalan ako i samo ako je $H = G$ ili G_ω pa slijedi tvrdnja. ■

Primjer 1.37 *Neka grupa G djeluje tranzitivno na skup Ω. Kažemo da je G* ***ranga*** *r ako G_ω za neki $\omega \in \Omega$ ima r orbita. Dokažimo da su grupe ranga 2 primitivne. Pretpostavimo da je Δ blok imprimitivnosti i $\omega \in \Delta$. Budući da je Δ G_ω-skup, on je unija orbita od G_ω, a one su u našem slučaju $\{\omega\}$ i $\Omega \setminus \{\omega\}$ pa je moguće konstruirati samo trivijalne blokovne sustave, tj. grupa ranga 2 je primitivna.*

Permutacijska grupa $Sym(\Omega)$ je grupa ranga 2 pa je primitivna. Na skup $\Omega^{(2)} = \{(\omega_1, \omega_2) \mid \omega_1, \omega_2 \in \Omega,\ \omega_1 \neq \omega_2\}$ grupa $Sym(\Omega)$ djeluje imprimitivno jer je skup svih

$$\Delta_\omega = \{(\omega_1, \omega) \mid \omega_1 \in \Omega,\ \omega_1 \neq \omega\} \text{ za svaki } \omega \in \Omega$$

netrivijalni blokovni sustav.

Definicija 1.38 *Neka je G grupa i $Sym(\Omega)$ simetrična grupa na Ω. Svaki homomorfizam $p : G \to Sym(\Omega)$ nazivamo* ***permutacijskom reprezentacijom*** *grupe G na skupu Ω. Reprezentacija je* ***vjerna*** *ako je p monomorfizam, tj. ako je $Ker p = \{1_G\}$.*

Primijetimo da svako djelovanje $\pi : G \times \Omega \to \Omega$ inducira jednu permutacijsku reprezentaciju $p : G \to Sym(\Omega)$ grupe G na skup Ω, pravilom $p(g) = f : \Omega \to \Omega$, $f(\omega) = \pi(g, \omega)$, za sve $g \in G$ i $\omega \in \Omega$. I obratno, svaka reprezentacija $p : G \to Sym(\Omega)$ inducira jedno djelovanje $\pi : G \times \Omega \to \Omega$, pravilom $\pi(g, \omega) = p(g)(\omega)$, za sve $g \in G$ i $\omega \in \Omega$.

Primjer 1.39 *Neka je G grupa. Preslikavanje $p : G \to Sym(G)$ dano pravilom $p(g) = f : G \to G$, $f(x) = gx$, inducirano djelovanjem iz Primjera 1.16, je vjerna reprezentacija grupe G na samu sebe, pa je $G \cong \{p(g) \mid g \in G\} \leq Sym(G)$ tj. svaka grupa je izomorfna nekoj permutacijskoj grupi.*

1.3 Linearne reprezentacije

Sljedeće definicije i rezultate možemo pronaći u [1, 20, 21].

Definicija 1.40 *Neka je G grupa i V konačnodimenzionalni vektorski prostor nad poljem F.* ***Linearna reprezentacija*** *grupe G nad poljem F je homomorfizam iz G u $GL(V)$. Tada V zovemo G-**modulom**, a dimenziju od V nad F nazivamo **stupnjem** linearne reprezentacije.*

Dakle, linearna reprezentacija grupe G nad F je svako preslikavanje ρ koje zadovoljava sljedeća svojstva:

i) za svaki $x \in G$, $\rho(x)$ je linearni regularni operator na V;

ii) $\rho(xy) = \rho(x)\rho(y)$ za sve $x, y \in G$.

Iz definicije je očito da je linearna reprezentacija ujedno i permutacijska reprezentacija jer je $GL(V) < Sym(V)$.

Definicija 1.41 *Neka je $\rho : G \to GL(V)$ linearna reprezentacija. Za potprostor $W \leq V$ kažemo da je G-**podmodul** ako je $\rho(g)W = W$ za svaki $g \in G$.*

Definicija 1.42 *Neka je $\rho : G \to GL(V)$ linearna reprezentacija. Ako V ne sadrži netrivijalne G-podmodule, kažemo da je ρ **ireducibilna** linearna reprezentacija, a V **ireducibilan** G-**modul**. U suprotnom, kažemo da je ρ **reducibilna** linearna reprezentacija, a V **reducibilan** G-**modul**.*

Propozicija 1.43 *Neka je $\rho : G \to GL(V)$ linearna reprezentacija i $W \leq V$ G-podmodul. Tada je $\rho_W : G \to GL(V/W)$ linearna reprezentacija definirana s $\rho_W(g)(v+W) = \rho(g)v+W$. G-modul V/W nazivamo **kvocijentnim** G-**modulom** od V po W.*

Definicija 1.44 ***Kompozicijski niz*** G***-modula*** *V je niz $V_0, V_1, ..., V_m$ G-podmodula od V za koje vrijedi*

$$\{0\} = V_0 < V_1 < ... < V_m = V$$

i za svaki $i = 1, ..., m$ kvocijentni G-moduli V_i / V_{i-1} su ireducibilni.

Svaki G-modul V ima kompozicijski niz. Ako odaberemo bazu od V_1 $\{v_1, ..., v_{\dim V_1}\}$, bazu od V_2 odaberemo tako da proširimo bazu od V_1 do $\{v_1, ..., v_{\dim V_2}\}$ te konačno odaberemo bazu od V kao proširenje baze od V_{m-1}, onda je matrični zapis od $\rho(g)$ gornje trokutasta blok-matrica pri čemu su blokovi na dijagonali matrični zapisi $R_i(g)$ linearnih operatora $\rho_i(g)$ na kvocijentima V_i / V_{i-1}. Prikaz $\rho(g)$ možemo vidjeti u sljedećoj matrici pri čemu su $A_{i,j}$ matrice tipa $(\dim V_i, \dim V_j)$.

$$\begin{bmatrix} R_1(g) & A_{1,2} & \cdots & A_{1,m} \\ 0 & R_2(g) & \cdots & A_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R_m(g) \end{bmatrix}$$

Linearne reprezentacije ćemo upotrebljavati na sljedeći način.

Neka je $N \trianglelefteq G$ normalna podgrupa grupe G i neka je $\phi : N \to F_p^n$ izomorfizam grupa. Tada je s

$$\rho(g)(v) = \phi(g\phi^{-1}(v)g^{-1}),$$

za svaki $v \in F_p^n$ i za svaki $g \in G$, definirana linearna reprezentacija $\rho : G \to GL(F_p^n)$ grupe G nad poljem F_p.

Za jezgru od ρ vrijedi:

$$\begin{aligned}
Ker\rho &= \{g \in G \mid \rho(g)(v) = v \text{ za svaki } v \in F_p^n\} \\
&= \{g \in G \mid \phi(g\phi^{-1}(v)g^{-1}) = v \text{ za svaki } v \in F_p^n\} \\
&= \{g \in G \mid g\phi^{-1}(v)g^{-1} = \phi^{-1}(v) \text{ za svaki } v \in F_p^n\} \\
&= \{g \in G \mid ghg^{-1} = h \text{ za svaki } h \in N\} \\
&= C_G(N).
\end{aligned}$$

Napomena 1.45 *Neka su $\varphi_1, ..., \varphi_s$ sve, do na izomorfizam, različite ireducibilne reprezentacije grupe G stupnja manjeg od n i neka su $J_i = Ker(\varphi_i)$, za svaki $i \in \{1, ..., s\}$. Pretpostavimo da postoji element $x \in G$ takav da je $x \in J_i$ za svaki $i = 1, ..., s$ i neka p ne dijeli red od x. Matrični zapis $\varphi_i(x)$ je jedinična matrica za svaki $i = 1, ..., s$ pa je matrični zapis $\rho(x)$ gornje trokutasta matrica s jedinicama na dijagonali. U teoriji grupa se pokazuje da je Sylowljeva p-podgrupa grupe $GL(n, p) \cong GL(F_p^n)$ grupa svih gornje trokutastih matrica s jedinicama na dijagonali (vidi [20]) pa je $\rho(x)$ u Sylowljevoj p-podgrupi tj. $\rho(x)$ je identiteta odnosno $x \in C_G(N)$. Ovo je razmatranje na koje ćemo se u kasnijim dokazima pozivati.*

1.4 Afine grupe

Definicije i rezultati iz afinih grupa mogu se pronaći u [10].

Definicija 1.46 ***Generalna afina grupa*** *$AGL(n, q)$ je skup svih (x, A) pri čemu je $x \in F_q^n$, $A \in GL(n, q)$, a množenje je dano s*

$$(x, A)(y, B) = (x + Ay, AB) \text{ za sve } x, y \in F_q^n \text{ i sve } A, B \in GL(n, q).$$

Skup $T = \{(x, I) \mid x \in F_q^n\}$ je normalna podgrupa grupe $AGL(n, q)$ i nazivamo ga podgrupom **translacija**. Pokaže se da vrijedi $AGL(n, q) = F_q^n \rtimes GL(n, q)$, pri čemu je $\rtimes$ oznaka za poludirektni produkt grupa.

Prirodno djelovanje afine grupe na F_q^n dano je sa:

$$(x, A)y = x + Ay \text{ za svaki } (x, A) \in AGL(n, q) \text{ i svaki } y \in F_q^n.$$

Definicija 1.47 *Za svaku grupu H takvu da je $T \leq H \leq AGL(n, q)$ kažemo da je* ***grupa afinog tipa****.*

Propozicija 1.48 *Za svaku grupu afinog tipa H postoji $H_0 \leq GL(n, q)$ takva da je $H = F_q^n \rtimes H_0$. Pri tome je $H_0 = \{A \in GL(n, q) \mid \exists x \in F_q^n \ (x, A) \in H\}$.*

Propozicija 1.49 *Neka je $H = F_q^n \rtimes H_0$ grupa afinog tipa. Grupa H je primitivna grupa ako i samo ako je H_0 ireducibilna podgrupa od $GL(n, q)$.*

Propozicija 1.50 *Neka je H primitivna grupa afinog tipa. Tada je T jedinstvena minimalna normalna podgrupa od H.*

1.5 Incidencijske strukture

Definicija 1.51 *Neka su P i $\mathcal{B}$ neprazni disjunktni skupovi i $I \subseteq P \times \mathcal{B}$. Uređenu trojku $\Gamma = (P, \mathcal{B}, I)$ nazivamo* ***incidencijskom strukturom****. Elemente od P nazivamo* ***točkama****, elemente od $\mathcal{B}$* ***blokovima****, a elemente od I* ***incidencijama*** *(eng.* ***flag****).*

Definicija 1.52 *Za incidencijske strukture $\Gamma_1 = (P_1, \mathcal{B}_1, I_1)$ i $\Gamma_2 = (P_2, \mathcal{B}_2, I_2)$ kažemo da su* ***izomorfne*** *ako postoji bijekcija $\varphi : P_1 \cup \mathcal{B}_1 \to P_2 \cup \mathcal{B}_2$ za koju vrijedi $\varphi(P_1) = P_2$, $\varphi(\mathcal{B}_1) = \mathcal{B}_2$ i ako za svaku točku $p \in P_1$ i svaki blok $B \in \mathcal{B}_1$ vrijedi:*

$$(p, B) \in I_1 \Leftrightarrow (\varphi(p), \varphi(B)) \in I_2.$$

Funkciju φ nazivamo ***izomorfizmom*** *incidencijskih struktura. Skup svih izomorfizama incidencijske strukture Γ u samu sebe nazivamo* ***punom grupom***

automorfizama *incidencijske strukture* Γ *i označavamo s* $Aut\Gamma$*.* ***Grupa automorfizama*** *incidencijske strukture je svaka podgrupa pune grupe automorfizama.*

Za incidencijsku strukturu $\Gamma = (P, \mathcal{B}, I)$, točku $p \in P$ i blok $B \in \mathcal{B}$ uvodimo oznake:

$\Gamma(p) = \{B \in \mathcal{B} : (p, B) \in I\}$,

$\Gamma(B) = \{p \in P : (p, B) \in I\}$.

Definicija 1.53 *Za incidencijsku strukturu* $\Gamma = (P, \mathcal{B}, I)$*, točku* $p \in P$ *(blok* $B \in \mathcal{B}$*) broj* $|\Gamma(p)|$ *(*$|\Gamma(B)|$*) nazivamo* ***stupnjem točke*** p *(****bloka*** B*).*

Definicija 1.54 *Za točku (blok)* $p \in P$ *(*$B \in \mathcal{B}$*) incidencijske strukture* $\Gamma = (P, \mathcal{B}, I)$ *kažemo da je* ***izolirana točka (blok)*** *ako je stupanj točke (bloka) jednak nuli.*

Definicija 1.55 *Kažemo da* ***grupa*** G ***djeluje na incidencijsku strukturu*** $\Gamma = (P, \mathcal{B}, I)$ *ako* G *djeluje na* P *i* $\mathcal{B}$ *te za svaki* $g \in G$ *vrijedi*

$$gI = I,$$

pri čemu je djelovanje na I *definirano na prirodan način s* $g(p, B) = (gp, gB)$ *za svaki* $(p, B) \in I$*.*

Definicija 1.56 *Neka* G *djeluje na incidencijsku strukturu* Γ *koja nema izoliranih točaka ni blokova. Kažemo da je incidencijska struktura* Γ G*-****tranzitivna po točkama (blokovima, incidencijama)*** *ako* G *djeluje tranzitivno na skup točaka (blokova, incidencija).*

Alternativno kažemo da je Γ **točkovno tranzitivna (blokovno tranzitivna, flag-tranzitivna)** incidencijska struktura s obzirom na grupu G.

Definicija 1.57 *Kažemo da je incidencijska struktura* Γ ***tranzitivna po točkama (blokovima, incidencijama)*** *ako postoji grupa automorfizama* G *incidencijske strukture* Γ *takva da je* Γ G*-tranzitivna po točkama (blokovima, incidencijama).*

Ako neka grupa djeluje tranzitivno na neki skup, onda i svaka njena nadgrupa djeluje tranzitivno na isti skup pa bi bilo ekvivalentno reći da je Γ tranzitivna po točkama (blokovima, incidencijama) ako $Aut\Gamma$ djeluje tranzitivno na skup točaka (blokova, incidencija).

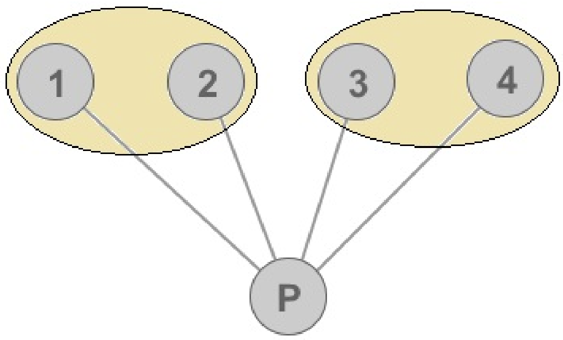
Definicija 1.58 *Neka* G *djeluje na incidencijsku strukturu* Γ *koja nema izoliranih točaka ni blokova. Kažemo da je incidencijska struktura* Γ ***G-primitivna (G-imprimitivna) po točkama*** *ako* G *djeluje primitivno (imprimitivno) na skup točaka.*

Definicija 1.59 *Kažemo da je incidencijska struktura* Γ ***primitivna (imprimitivna) po točkama*** *ako postoji podgrupa* $G \leq Aut\Gamma$ *takva da je* Γ G*-primitivna (*G*-imprimitivna) po točkama.*

Primijetimo da incidencijska struktura može istovremeno biti i primitivna i imprimitivna.

Primjer 1.60 *Promotrimo jednostavnu incidencijsku strukturu* $\Gamma = (P, \mathcal{B})$ *s* $P = \{1, 2, 3, 4\}$ $\mathcal{B} = \{P\}$. *Dana incidencijska struktura prikazana je na Slici 1.1 bipartitnim grafom.*

Na ovu incidencijsku strukturu simetrična grupa S_4 *djeluje primitivno po točkama, dakle dana incidencijska struktura je* S_4*-primitivna, a samim time i primitivna. S druge strane, na ovu incidencijsku strukturu djeluje i grupa* $C_2^2 = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ *generirana dvjema permutacijama i to imprimitivno. Primijetimo da djelovanje te grupe čuva svaku od particija*



Slika 1.1: Incidencijska struktura

$\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$, $\{\{1,4\},\{2,3\}\}$ *(na slici je prikazana prva particija). Dakle, te su particije sustavi imprimitivnosti te je dana incidencijska struktura* C_2^2*-imprimitivna, a samim time i imprimitivna.*

Poglavlje 2

Incidencijske strukture tranzitivne po incidencijama

Propozicija 2.1 *Neka grupa G djeluje na incidencijsku strukturu $\Gamma = (P, \mathcal{B}, I)$ bez izoliranih točaka i blokova i neka je $p \in P$, $B \in \mathcal{B}$. Tada su sljedeće tvrdnje ekvivalentne:*

$i)$ Grupa G je tranzitivna po incidencijama na Γ.

$ii)$ Grupa G je tranzitivna po točkama i G_p je tranzitivna na $\Gamma(p)$.

$iii)$ Grupa G je tranzitivna po blokovima i G_B je tranzitivna na $\Gamma(B)$.

Dokaz.

$i) \Rightarrow ii)$

Neka su $p_1, p_2 \in P$. Kako su svi stupnjevi točaka pozitivni brojevi, postoje $B_1, B_2 \in \mathcal{B}$ takvi da je $(p_1, B_1), (p_2, B_2) \in I$. Sada, zbog tranzitivnosti po incidencijama, postoji $g \in G$ takav da je $g(p_1, B_1) = (p_2, B_2)$, to jest $gp_1 = p_2$, pa je G tranzitivna po točkama. Nadalje, neka su $B_1, B_2 \in \Gamma(p)$. Tada je $(p, B_1), (p, B_2) \in I$. Zbog tranzitivnosti po incidencijama, postoji $g \in G$ takav da je $g(p, B_1) = (p, B_2)$, to jest $gp = p$ i $gB_1 = B_2$, pa je $g \in G_p$ te je dokazana tranzitivnost na $\Gamma(p)$.

ii) $\Rightarrow$ *iii)*

Neka su $B_1, B_2 \in \mathcal{B}$. Kako su svi stupnjevi blokova pozitivni brojevi, postoje $p_1, p_2 \in P$ takvi da je $(p_1, B_1), (p_2, B_2) \in I$. Zbog tranzitivnosti po točkama, postoje $h_1, h_2 \in G$ takvi da je $h_1 p_1 = p$ i $h_2 p_2 = p$. Sada je $h_1(p_1, B_1) = (p, h_1 B_1)$ te $h_2(p_2, B_2) = (p, h_2 B_2)$. Kako su $h_1 B_1, h_2 B_2 \in \Gamma(p)$, zbog tranzitivnosti G_p na $\Gamma(p)$, postoji $g \in G_p$ takav da je $g h_1 B_1 = h_2 B_2$. Konačno, $h_2^{-1} g h_1 B_1 = B_2$, čime je dokazana tranzitivnost po blokovima. Nadalje, neka su $p_1, p_2 \in \Gamma(B)$. Tada je $(p_1, B), (p_2, B) \in I$. Zbog tranzitivnosti po točkama, postoje $h_1, h_2 \in G$ takvi da je $h_1 p_1 = p$ i $h_2 p_2 = p$. Sada je $h_1(p_1, B) = (p, h_1 B)$ te $h_2(p_2, B) = (p, h_2 B)$. Kako su $h_1 B, h_2 B \in \Gamma(p)$, zbog tranzitivnosti G_p na $\Gamma(p)$, postoji $g \in G_p$ takav da je $g h_1 B = h_2 B$, to jest $h_2^{-1} g h_1 B = B$, pa je $h_2^{-1} g h_1 \in G_B$. Konačno $h_2^{-1} g h_1 p_1 = h_2^{-1} g p = h_2^{-1} p$ $= p_2$.

iii) $\Rightarrow$ *i)*

Neka su $(p_1, B_1), (p_2, B_2) \in I$. Zbog tranzitivnosti po blokovima, postoje $h_1, h_2 \in G$ takvi da je $h_1 B_1 = B$ i $h_2 B_2 = B$. Sada je $h_1(p_1, B_1) = (h_1 p_1, B)$ te $h_2(p_2, B_2) = (h_2 p_2, B)$. Kako su $h_1 p_1, h_2 p_2 \in \Gamma(B)$, zbog tranzitivnosti G_B na $\Gamma(B)$, postoji $g \in G_B$ takav da je $g h_1 p_1 = h_2 p_2$, to jest $h_2^{-1} g h_1 p_1 = p_2$. Također, $h_2^{-1} g h_1 B_1 = h_2^{-1} g B = h_2^{-1} B = B_2$. Konačno, $h_2^{-1} g h_1 (p_1, B_1) = (p_2, B_2)$ pa je dana incidencijska struktura tranzitivna po incidencijama na Γ. ■

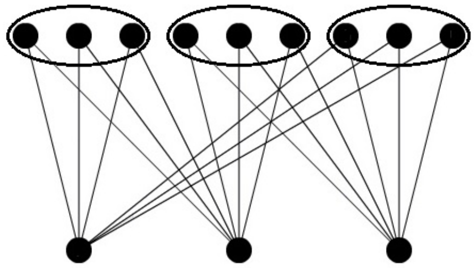
2.1 Incidencijska podstruktura i kvocijentna incidencijska struktura

U ovom dijelu ćemo definirati incidencijske podstrukture i kvocijentne incidencijske strukture. Takve konstrukcije za posebne incidencijske strukture (dizajne) opisane su u [8, 22], a ovdje poopćavamo tu konstrukciju na sve incidencijske strukture tranzitivne po incidencijama i imprimitivne po točkama.

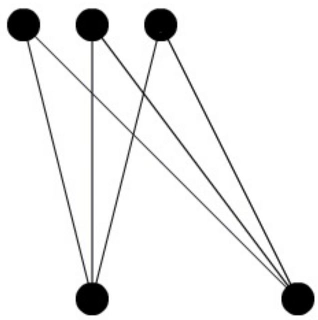
Definicija 2.2 *Neka je G grupa, $\Gamma = (P, \mathcal{B}, I)$ incidencijska struktura G-tranzitivna po incidencijama i G-imprimitivna po točkama, Σ sustav imprimitivnosti za G na skupu točaka i $\Delta \in \Sigma$. Incidencijsku strukturu $\Gamma_\Delta = (\Delta, \mathcal{B}_\Delta, I_\Delta)$, pri čemu je $\mathcal{B}_\Delta = \{B \in \mathcal{B} : \Delta \cap \Gamma(B) \neq \emptyset\}$, a $I_\Delta = I \cap (\Delta \times \mathcal{B}_\Delta)$ nazivamo* ***incidencijskom podstrukturom od Γ s obzirom na blok imprimitivnosti Δ.***

Primjer 2.3 *Na Slici 2.1 je prikazana incidencijska struktura tranzitivna po incidencijama bipartitnim grafom, pri čemu se gore nalaze točke, dolje blokovi, a skup incidencija je prikazan bridovima između točaka i blokova koji su međusobno incidentni. Također, grupa automorfizama ove incidencijske strukture čuva particiju točaka na tri bloka imprimitivnosti koji su naznačeni na slici.*

Incidencijska podstruktura ove incidencijske strukture s obzirom na prvi (s lijeva) blok imprimitivnosti je prikazana na Slici 2.2. Dakle, uzete su samo točke iz prvog bloka imprimitivnosti i oni blokovi koji su incidentni s bilo kojom od tih točaka. Incidencije su naslijeđene iz polazne incidencijske strukture.



Slika 2.1: Incidencijska struktura tranzitivna po incidencijama



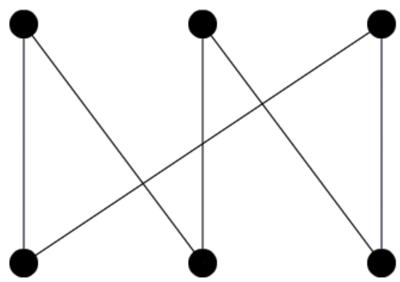
Slika 2.2: Incidencijska podstruktura

Propozicija 2.4 *Neka je G grupa, $\Gamma = (P, \mathcal{B}, I)$ incidencijska struktura G-tranzitivna po incidencijama i G-imprimitivna po točkama, Σ sustav imprimitivnosti za G na skupu točaka i $\Delta \in \Sigma$. Tada je Γ_Δ incidencijska struktura G_Δ-tranzitivna po incidencijama.*

Dokaz. Pokažimo da za svake dvije incidencije (p_1, B_1) i (p_2, B_2) iz I_Δ postoji $g \in G_\Delta$ takav da je $g(p_1, B_1) = (p_2, B_2)$. Kako su (p_1, B_1) i (p_2, B_2) iz I_Δ, one su svakako incidencije i u I. Zbog G-tranzitivnosti po incidencijama od Γ, postoji $g \in G$ takav da je $g(p_1, B_1) = (p_2, B_2)$. Kako je $gp_1 = p_2$, a p_1 i p_2 su iz Δ, to je, zbog G-imprimitivnosti od Γ, $g\Delta = \Delta$ pa je $g \in G_\Delta$. ■

Definicija 2.5 *Neka je G grupa, $\Gamma = (P, \mathcal{B}, I)$ incidencijska struktura G-tranzitivna po incidencijama i G-imprimitivna po točkama, Σ sustav imprimitivnosti za G na skupu točaka i $\Delta \in \Sigma$. Incidencijsku strukturu $\Gamma/\Sigma = (\Sigma, \mathcal{B}, I_\Sigma)$, pri čemu je $(\Delta, B) \in I_\Sigma$ ako je $\Delta \cap \Gamma(B) \neq \emptyset$, nazivamo* ***kvocijentnom incidencijskom strukturom od*** Γ ***po sustavu imprimitivnosti*** Σ.

Primjer 2.6 *Za incidencijsku strukturu iz Primjera 2.3 prikažimo kvocijentnu incidencijsku strukturu po danom sustavu imprimitivosti. Vizualizacije radi, možemo zamisliti da se sve točke unutar istog bloka imprimitivnosti "spajaju" u jednu "novu" točku, a blokovi su incidentni s onim "novim" točkama ako su bili incidentni s bilo kojom točkom od onih koje su se spojile u tu "novu" točku. Kvocijentna struktura prikazana je na Slici 2.3.*



Slika 2.3: Kvocijentna incidencijska struktura

Propozicija 2.7 *Neka je G grupa, $\Gamma = (P, \mathcal{B}, I)$ incidencijska struktura G-tranzitivna po incidencijama i G-imprimitivna po točkama, Σ sustav imprimitivnosti za G na skupu točaka. Tada je Γ/Σ incidencijska struktura G-tranzitivna po incidencijama.*

Dokaz. Pokažimo da za svake dvije incidencije (Δ_1, B_1) i (Δ_2, B_2) iz I_Σ postoji $g \in G$ takav da je $g(\Delta_1, B_1) = (\Delta_2, B_2)$. Kako su (Δ_1, B_1) i (Δ_2, B_2) incidencije u I_Σ, to znači da postoje $p_1 \in \Delta_1$ i $p_2 \in \Delta_2$ takvi da su (p_1, B_1) i (p_2, B_2) incidencije u I. Kako je Γ G-tranzitivna po incidencijama, to postoji $g \in G$ takav da je $g(p_1, B_1) = (p_2, B_2)$ pa je $gp_1 = p_2$ što, zbog G-imprimitivnosti od Γ, povlači $g\Delta_1 = \Delta_2$ pa je sada $g(\Delta_1, B_1) = (\Delta_2, B_2)$. ■

2.2 Pojednostavnjenje incidencijske strukture

Definicija 2.8 *Za incidencijsku strukturu $\Gamma = (P, \mathcal{B}, I)$ kažemo da je* ***jednostavna*** *ako za sve $B_1, B_2 \in \mathcal{B}$ iz $\Gamma(B_1) = \Gamma(B_2)$ slijedi $B_1 = B_2$.*

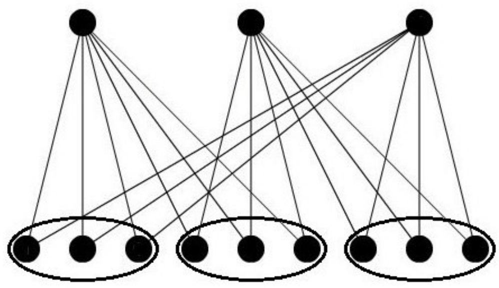
Propozicija 2.9 *Svaka jednostavna incidencijska struktura $\Gamma = (P, \mathcal{B}, I)$ izomorfna je incidencijskoj strukturi $\Gamma' = (P, \mathcal{B}', I')$ gdje je $\mathcal{B}'$ neprazna familija poskupova od P, a I' incidencija dana sa:*

$$(p, B) \in I' \Leftrightarrow \ p \in B, \text{ za svaki } p \in P \text{ i } B \in \mathcal{B}'.$$

Nadalje ćemo jednostavne incidencijske strukture $\Gamma = (P, \mathcal{B}, I)$ u kojima je $\mathcal{B} \subseteq 2^P$, a incidencija dana relacijom "biti element" označavati s $\Gamma = (P, \mathcal{B})$.

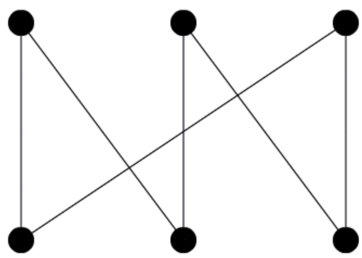
Definicija 2.10 *Neka je $\Gamma = (P, \mathcal{B}, I)$ incidencijska struktura. Incidencijsku strukturu $\Gamma^S = (P, \{\Gamma(B), B \in \mathcal{B}\})$ nazivamo* ***pojednostavnjenjem*** *incidencijske struktrure Γ.*

Primjer 2.11 *Na Slici 2.4 je prikazana incidencijska struktura tranzitivna po incidencijama s tri točke i devet blokova. Blokovi koji su incidentni s istim skupom točaka grupirani su na način kako je prikazano na slici.*



Slika 2.4: Incidencijska struktura tranzitivna po incidencijama

Pojednostavnjenje te incidencijske strukture prikazano je na Slici 2.5. Primijetimo da smo pojednostavnjenje dobili tako što smo od svakog skupa blokova incidentnih s istim skupom točaka odabrali samo jednog predstavnika.



Slika 2.5: Pojednostavnjenje incidencijske strukture

Propozicija 2.12 *Neka je* G *grupa i* $\Gamma = (P, \mathcal{B}, I)$ *incidencijska struktura* G*-tranzitivna po blokovima. Tada vrijedi:*

i) Za svaki $B \in \mathcal{B}$ *i* $g \in G$ *je* $g\Gamma(B) = \Gamma(gB)$*.*

ii) Za svaki $B \in \mathcal{B}$ *broj* $|\{B' \in \mathcal{B} | \Gamma(B) = \Gamma(B')\}|$ *je konstanta i jednaka je* $\frac{|G_{\Gamma(B)}|}{|G_B|}$*. Ovaj broj nazivamo* ***multiplicitetom*** *incidencijske strukture* Γ*.*

iii) Incidencijska struktura $\Gamma = (P, \mathcal{B}, I)$ *izomorfna je incidencijskoj strukturi* $\Gamma' = (P, \{(\Gamma(B), B \in \mathcal{B}\} \times \{1, ..., \frac{|G_{\Gamma(B)}|}{|G_B|}\}, I')$ *pri čemu je* $(p, (\Gamma(B), i)) \in$

I' ako je $(p, B) \in I$.

Dokaz.

i)

Neka su $B \in \mathcal{B}$ i $g \in G$ proizvoljni i $a \in g\Gamma(B)$.

To znači da postoji točka $p \in P$ incidentna bloku B takva da je $a = gp$. Kako je $(p, B) \in I$, to je $(gp, gB) \in I$, tj. $(a, gB) \in I$, pa je $a \in \Gamma(gB)$. Dakle, $g\Gamma(B) \subset \Gamma(gB)$.

Neka su $B \in \mathcal{B}$ i $g \in G$ proizvoljni i $a \in \Gamma(gB)$.

To znači da je $(a, gB) \in I$ pa je i $(g^{-1}a, g^{-1}gB) = (g^{-1}a, B) \in I$, tj. $g^{-1}a \in \Gamma(B)$, pa je $a \in g\Gamma(B)$. Dakle, $\Gamma(gB) \subset g\Gamma(B)$ pa je $\Gamma(gB) = g\Gamma(B)$.

ii)

Neka su B_1 i B_2 dva proizvoljna bloka iz $\mathcal{B}$. Zbog tranzitivnosti po blokovima od G postoji $g \in G$ takav da je $gB_1 = B_2$. Označimo s $T(B_1)$ skup:

$$T(B_1) = \{B' \in \mathcal{B} : \Gamma(B_1) = \Gamma(B')\}.$$

Sada je

$$\begin{aligned}
gT(B_1) &= \{gB' \mid B' \in \mathcal{B},\, \Gamma(B_1) = \Gamma(B')\} \\
&= \{gB' \in \mathcal{B} \mid g\Gamma(B_1) = g\Gamma(B')\} \\
&= \{gB' \in \mathcal{B} \mid \Gamma(gB_1) = \Gamma(gB')\} \\
&= \{gB' \in \mathcal{B} \mid \Gamma(B_2) = \Gamma(gB')\} \\
&= T(B_2).
\end{aligned}$$

Pokazali smo da su za svaki $B \in \mathcal{B}$ skupovi $T(B)$ ekvipotentni. Pokažimo da je njihova kardinalnost $\frac{|G_{\Gamma(B)}|}{|G_B|}$.

Neka je $B \in \mathcal{B}$ proizvoljan. Prvo pokažimo da je djelovanje grupe $G_{\Gamma(B)}$ na $T(B)$ dobro definirano.

Neka je $g \in G_{\Gamma(B)}$ te neka je $B' \in T(B)$. Kako je $B' \in T(B)$, to je

$$\begin{aligned} \Gamma(B') &= \Gamma(B) \\ g\Gamma(B') &= g\Gamma(B) \\ \Gamma(gB') &= \Gamma(B), \end{aligned}$$

pa je $gB' \in T(B)$.

Sada pokažimo da je djelovanje grupe $G_{\Gamma(B)}$ na $T(B)$ tranzitivno. Neka su B_1 i B_2 dva proizvoljna bloka iz $T(B)$. Zbog blokovne tranzitivnosti od G postoji $g \in G$ takav da je $gB_1 = B_2$. Onda je $\Gamma(gB_1) = \Gamma(B_2)$ pa je $g\Gamma(B_1) = \Gamma(B_2)$, a kako je $\Gamma(B_1) = \Gamma(B_2) = \Gamma(B)$, to je $g\Gamma(B) = \Gamma(B)$ pa je $g \in G_{\Gamma(B)}$.

Još pokažimo da je $G_B \leq G_{\Gamma(B)}$. Neka je $g \in G_B$ tj. $gB = B$. Tada je $\Gamma(gB) = \Gamma(B)$, tj. $g\Gamma(B) = \Gamma(B)$, pa je $g \in G_{\Gamma(B)}$.

Sada vrijedi da je $|T(B)| = [G_{\Gamma(B)} : G_B] = \frac{|G_{\Gamma(B)}|}{|G_B|}$.

iii)

Definirajmo relaciju $\sim$ na skupu $\mathcal{B}$ tako da za $B_1, B_2 \in \mathcal{B}$ vrijedi $B_1 \sim B_2$ ako i samo ako je $\Gamma(B_1) = \Gamma(B_2)$. $\sim$ je očito relacija ekvivalencije i particionira skup $\mathcal{B}$ na klase ekivalencije veličine $\frac{|G_{\Gamma(B)}|}{|G_B|}$ (zbog ii).

Označimo s $\mathcal{B}_1, ..., \mathcal{B}_k$ te klase ekvivalencije. Sada, za svaku klasu $\mathcal{B}_i$ definirajmo funkciju $\lambda_i : \mathcal{B}_i \to \{1, ..., \frac{|G_{\Gamma(B)}|}{|G_B|}\}$ tako da λ_i bude proizvoljna bijekcija. To je moguće jer su $\mathcal{B}_i$ i $\{1, ..., \frac{|G_{\Gamma(B)}|}{|G_B|}\}$ ekvipotentni.

Sada je funkcija $\lambda : P \cup \mathcal{B} \to P \cup \{(\Gamma(B), B \in \mathcal{B}\} \times \{1, ..., \frac{|G_{\Gamma(B)}|}{|G_B|}\}$ definirana s

$$\lambda(p) = p; \text{ za svaki } p \in P$$

$$\lambda(B) = (\Gamma(B), \lambda_i(B)); \text{ za svaki } B \in \mathcal{B}_i$$

izomorfizam danih struktura.

Pokažimo to. Takva funkcija je očito bijekcija. Nadalje, neka su $p \in P$ i $B \in \mathcal{B}$ takvi da je $(p, B) \in I$. Neka se B nalazi u $\mathcal{B}_i$. Tada je $(\lambda(p), \lambda(B)) = (p, (\Gamma(B), j))$ za neki $j \in \{1, ..., \frac{|G_{\Gamma(B)}|}{|G_B|}\}$. A kako je $(p, B) \in I$, to je $(p, (\Gamma(B), j)) = (\lambda(p), \lambda(B)) \in I'$. ∎

Propozicija 2.13 *Neka je $\Gamma = (P, \mathcal{B}, I)$ incidencijska struktura G-tranzitivna po incidencijama. Tada je Γ^S G-tranzitivna po incidencijama.*

Dokaz. Neka su (p_1, B_1) i (p_2, B_2) incidencije u Γ^S tj. $p_1 \in B_1$ i $p_2 \in B_2$. To znači da je postoje blokovi $B_1', B_2' \in \mathcal{B}$ takvi da je $B_1 = \Gamma(B_1')$ i $B_2 = \Gamma(B_2')$ i $(p_1, B_1'), (p_2, B_2') \in I$. Sada zbog G-tranzitivnosti po incidencijama od Γ postoji $g \in G$ takav da je $g(p_1, B_1') = (p_2, B_2')$. No kako je $gB_1 = g\Gamma(B_1')$, a po Propoziciji 2.12 $g\Gamma(B_1') = \Gamma(gB_1') = \Gamma(B_2') = B_2$, to je $g(p_1, B_1) = (p_2, B_2)$. ∎

Propozicija 2.14 *Neka je $\Gamma = (P, \mathcal{B})$ incidencijska struktura G-tranzitivna po incidencijama i $\Gamma_n = \{P, \mathcal{B} \times \{1, .., n\}, I_n\}$ pri čemu je $I_n = \{(p, (B, i)) : p \in B, i \in \{1, .., n\}\}$. Tada je Γ_n $(G \times S_n)$-tranzitivna po incidencijama.*

Dokaz. Definirajmo djelovanje grupe $G \times S_n$ na točke i blokove incidencijske strukture Γ_n. Neka je $(g, \pi) \in G \times S_n$. Tada je $(g, \pi)\, p = gp$, za svaki $p \in P$ i $(g, \pi)\,(B, i) = (gB, \pi(i))$, za svaki $(B, i) \in \mathcal{B} \times \{1, .., n\}$. Pokažimo prvo da $G \times S_n$ djeluje na incidencijsku strukturu Γ_n. Neka je $(g, \pi) \in G \times S_n$ i

$(p,(B,i)) \in I_n$. Tada je $(g,\pi)\,(p,(B,i)) = (gp,(gB,\pi(i)))$, a kako je $gp \in gB$, to je $G \times S_n$ grupa automorfizama od Γ_n.

Neka su $(p_1,(B_1,i_1))$,$(p_2,(B_2,i_2)) \in I_n$. Zbog $p_1 \in B_1$ i $p_2 \in B_2$ i G-tranzitivnosti po incidencijama od Γ postoji $g \in G$ takav da je $gp_1 = p_2$ i $gB_1 = gB_2$. Također, postoji $\pi \in S_n$ takav da je $\pi(i_1) = i_2$. Sada je $(g,\pi)\,(p_1,(B_1,i_1)) = (p_2,(B_2,i_2))$ pa je tvrdnja dokazana. ■

Poglavlje 3

Dizajni tranzitivni po incidencijama

3.1 Dizajni

Sljedeće definicije i rezultati iz teorije dizajna mogu se pronaći u [2, 6, 9, 15].

Definicija 3.1 *Incidencijsku strukturu* $D = (P, \mathcal{B}, I)$, $|P| = v$, *nazivamo* t-(v, k, λ) ***dizajnom*** *ako vrijedi:*

i) za svaki blok B *je* $|\Gamma(B)| = k < v$,

ii) za svakih t *različitih točkaka* $p_1, p_2, ..., p_t \in P$ *je*

$$|\Gamma(p_1) \cap \Gamma(p_2) \cap ... \cap \Gamma(p_t)| = \lambda.$$

Nadalje ćemo broj blokova t-(v, k, λ) dizajna $D = (P, \mathcal{B}, I)$ označavati s b ($|\mathcal{B}| = b$). Dizajn ćemo nazivati **trivijalnim** ako je broj blokova u pojednostavnjenju tog dizajna jednak $\binom{v}{k}$. Inače ga nazivamo **netrivijalnim**.

Propozicija 3.2 *Ako je* $D = (P, \mathcal{B}, I)$ t-(v, k, λ) *dizajn, onda je* D *(t-1)-*(v, k, λ^*) *dizajn pri čemu je* $\lambda^* = \lambda \frac{v-t+1}{k-t+1}$.

U daljnjem radu bavit ćemo se isključivo 2-(v,k,λ) dizajnima.

Propozicija 3.3 *Neka je $D=(P,\mathcal{B},I)$ 2-(v,k,λ) dizajn. Tada vrijedi:*

i) Postoji $r=\frac{\lambda(v-1)}{(k-1)}\in\mathbb{N}$ takav da za svaku točku $p\in P$ vrijedi $|\Gamma(p)|=r$;

ii) $bk=rv$.

Propozicija 3.4 (Fisherova nejednakost) *Neka je $D=(P,\mathcal{B},I)$ 2-(v,k,λ) dizajn. Tada je $v\le b$.*

Definicija 3.5 *2-(v,k,λ) dizajn u kojem je broj točaka jednak broju blokova, tj. $v=b$, nazivamo (v,k,λ) **simetričnim dizajnom**.*

Propozicija 3.6 *Neka je G grupa i $D=(P,\mathcal{B},I)$ 2-(v,k,λ) dizajn G-tranzitivan po blokovima i $B\in\mathcal{B}$. Tada $\left|G_{D(B)}\right|$ dijeli $\lambda\,|G_B|$ i D^S je jednostavni 2-$(v,k,\frac{\lambda|G_B|}{\left|G_{D(B)}\right|})$ dizajn G-tranzitivan po blokovima.*

Dokaz. Po Propoziciji 2.12 (iii) vrijedi da je D^S jednostavna incidencijska struktura G-tranzitivna po blokovima. Također, po Propoziciji 2.12 (ii) za svaki $B\in\mathcal{B}$ broj $\frac{\left|G_{D(B)}\right|}{|G_B|}=|\{B'\in B: D(B)=D(B')\}|$ je konstanta. Kako za svake dvije različite točke $p,q\in P$ vrijedi $\left|D^S(p)\cap D^S(q)\right|=|D(p)\cap D(q)|\,\frac{|G_B|}{\left|G_{D(B)}\right|}=\lambda\frac{|G_B|}{\left|G_{D(B)}\right|}$, slijedi $\left|G_{D(B)}\right|\mid\lambda\,|G_B|$ i D^S je 2-$(v,k,\lambda\frac{|G_B|}{\left|G_{D(B)}\right|})$ dizajn. ■

Korolar 3.7 *Neka je G grupa i $D=(P,\mathcal{B},I)$ 2-(v,k,λ) dizajn G-tranzitivan po incidencijama. Tada je dizajn D^S G-tranzitivan po incidencijama.*

Dokaz. Tvrdnja slijedi direktno iz Propozicija 2.13 i 3.6. ■

Propozicija 3.8 *Neka je $D=(P,\mathcal{B},I)$ 2-(v,k,λ) dizajn i $n\in\mathbb{N}$. Incidencijska struktura $D_n=\{P,\mathcal{B}\times\{1,..,n\},I_n\}$, pri čemu je $I_n=\{(p,(B,i)):(p,B)\in I, i\in\{1,..,n\}\}$, je 2-$(v,k,n\lambda)$ dizajn.*

Propozicija 3.9 (Zieschang, [22]) *Neka je* $\Gamma = (P, \mathcal{B}, I)$ *incidencijska struktura* G*-tranzitivna po incidencijama,* $|P| = v$*,* $p \in P$*,* $B \in \mathcal{B}$*,* $(p, B) \in I$ *i* $|\Gamma(B)| = k$*. Tada je* Γ *2-dizajn ako i samo ako vrijedi*

$$|\Gamma(B) \cap Q| = \frac{(k-1)\,|Q|}{v-1}, \text{ za svaku orbitu } Q \text{ od } G_p \text{ u } P\backslash\{p\}.$$

Dokaz. Neka je Q orbita od G_p u $P\backslash\{p\}$ i $q \in Q$. Djelovanjem s G_p dobivamo da je $|\Gamma(p) \cap \Gamma(q)| = |\Gamma(p) \cap \Gamma(q')|$ za sve $q' \in Q$. Zbog tranzitivnosti po incidencijama vrijedi $|\Gamma(B) \cap Q| = |\Gamma(B') \cap Q|$ za svaki $B' \in \Gamma(p)$ (jer je G_p tranzitivna na $\Gamma(p)$ po Propoziciji 2.1). Sada prebrojavanjem skupa $\{(q', B') \in I : q' \in Q,\, B' \in \Gamma(p)\}$ na dva načina dobijemo

$$|Q|\,|\Gamma(p) \cap \Gamma(q)| = |\Gamma(p)|\,|\Gamma(B) \cap Q|\,.$$

Ako je Γ 2-dizajn, onda je $|\Gamma(B) \cap Q| = \frac{|Q||\Gamma(p)\cap\Gamma(q)|}{|\Gamma(p)|} = \frac{\lambda|Q|}{r} = \frac{(k-1)|Q|}{v-1}$, za svaku orbitu Q od G_p u $P\backslash\{p\}$.

Ako vrijedi $|\Gamma(B) \cap Q| = \frac{(k-1)|Q|}{v-1}$, onda je $|\Gamma(p) \cap \Gamma(q)| = \frac{|\Gamma(p)||\Gamma(B)\cap Q|}{|Q|} = \frac{|\Gamma(p)|(k-1)}{v-1}$. Kako $|\Gamma(p)|$ ne ovisi o izboru p zbog tranzitivnosti po incidencijama, to je broj blokova koji je incidentan dvjema različitim točkama neovisan o izboru tih točaka. Također, $|\Gamma(B)|$ iz istog razloga ne ovisi o izboru B pa je Γ 2-dizajn. ■

Propozicija 3.10 *Neka je* $D = (P, \mathcal{B}, I)$ *2-*(v, k, λ) *dizajn* G*-tranzitivan po incidencijama i* G*-imprimitivan po točkama te* Σ *sustav imprimitivnosti na skupu točaka. Tada postoji* $\mu \in \mathbb{N}$ *takav da je* $|D(B) \cap \Delta| \in \{0, \mu\}$ *za sve* $B \in \mathcal{B}$ *i sve* $\Delta \in \Sigma$*.*

Dokaz. Pokažimo da su svi neprazni presjeci točaka incidentnih nekom bloku iz $\mathcal{B}$ i nekog bloka imprimitivnosti iz Σ ekvipotentni. Neka je $D(B_1) \cap \Delta_1 \neq \emptyset$ i $D(B_2) \cap \Delta_2 \neq \emptyset$. Neka su $(p_1, B_1), (p_2, B_2) \in I$ za neke dvije točke $p_1 \in \Delta_1$ i

$p_2 \in \Delta_2$. Kako je dizajn D G-tranzitivan po incidencijama, postoji neki $g \in G$ takav da je $g(p_1, B_1) = (p_2, B_2)$. Pokažimo da je $g(D(B_1) \cap \Delta_1) \subseteq D(B_2) \cap \Delta_2$. Neka je $a \in D(B_1) \cap \Delta_1$. Tada je $a \in D(B_1)$ pa je $ga \in gD(B_1) = D(gB_1) = D(B_2)$. Također, kako za $p_1 \in \Delta_1$ vrijedi $gp_1 = p_2 \in \Delta_2$, a zbog toga što je Σ sustav imprimitivnosti na skupu točaka, mora biti $g\Delta_1 = \Delta_2$ pa je $ga \in \Delta_2$. Dakle,

$$|D(B_1) \cap \Delta_1| = |g(D(B_1) \cap \Delta_1)| \leq |D(B_2) \cap \Delta_2|\,.$$

Analogno odabirom $g^{-1} \in G$ pokažemo da je $|D(B_2) \cap \Delta_2| \leq |D(B_1) \cap \Delta_1|$ pa je konačno

$$|D(B_1) \cap \Delta_1| = |D(B_2) \cap \Delta_2|\,.$$

■

Nadalje ćemo za svaki blok $B \in \mathcal{B}$ i svaki blok imprimitivnosti $\Delta \in \Sigma$, takav da je $D(B) \cap \Delta \neq \emptyset$, kardinalnost skupa $D(B) \cap \Delta$ označavati s μ. Također ćemo, za svaki blok $B \in \mathcal{B}$, broj blokova imprimitivnosti $\Delta \in \Sigma$ takvih da je $D(B) \cap \Delta \neq \emptyset$, označavati s δ. Dakle,

$$\delta = |\{\Delta \in \Sigma \mid D(B) \cap \Delta \neq \emptyset\}|\,.$$

Lako se vidi da je tada $k = \mu\delta$. No kako ni k ni μ ne ovise o izboru bloka $B \in \mathcal{B}$, to ni δ nije ovisan o takvom izboru.

Propozicija 3.11 *Neka je $D = (P, \mathcal{B}, I)$ 2-(v, k, λ) dizajn G-tranzitivan po incidencijama i G-imprimitivan po točkama, Σ sustav imprimitivnosti na skupu točaka koji se sastoji od d blokova imprimitivnosti kardinalnosti c i $\Delta \in \Sigma$. Tada je D_Δ 2-(c, μ, λ) dizajn G_Δ-tranzitivan po incidencijama. Također vrijedi*

$$\frac{v-1}{k-1} = \frac{c-1}{\mu-1}.$$

Dokaz. Ako su $p, q \in \Delta$ dvije različite točke, onda je

$$\begin{aligned} |D_\Delta(p) \cap D_\Delta(q)| &= |\{B \in \mathcal{B}_\Delta \mid (p, B), (q, B) \in I\}| \\ &= |\{B \in \mathcal{B} \mid (p, B), (q, B) \in I\}| \\ &= |D(p) \cap D(q)| \\ &= \lambda. \end{aligned}$$

Po prethodnoj propoziciji vrijedi da su svaka dva neprazna presjeka bloka dizajna s blokom imprimitivnosti ekvipotentna pa su svi blokovi dizajna D_Δ ekvipotentni.

Jer su D i D_Δ 2-dizajni vrijedi $\lambda(v-1) = r(k-1)$ i $\lambda(c-1) = r(\mu-1)$. Ako bi bilo $\mu = 1$, onda iz $\lambda(c-1) = 0$ slijedi $c = 1$ što je u kontradikciji s činjenicom da je Σ sustav imprimitivnosti. Stoga imamo $\frac{r}{\lambda} = \frac{v-1}{k-1} = \frac{c-1}{\mu-1}$. ■

Dizajn D_Δ nazivamo **poddizajnom dizajna** D **s obzirom na blok imprimitivnosti** Δ.

Propozicija 3.12 *Za dani 2-(v, k, λ) dizajn $D = (P, \mathcal{B}, I)$ G-tranzitivan po incidencijama i G-imprimitivan po točkama, broj blokova b_Δ njegovog poddizajna D_Δ jednak je $\frac{cr}{\mu}$.*

Dokaz. Prebrojimo na dva načina sve incidencije dizajna D_Δ. On ima c točaka od kojih je svaka incidentna s r blokova. S druge strane, svaki od njegovih b_Δ blokova je stupnja μ. Dakle $cr = b_\Delta \mu$, tj. $b_\Delta = \frac{cr}{\mu}$. ■

Propozicija 3.13 *Neka je $D = (P, \mathcal{B}, I)$ 2-(v, k, λ) dizajn G-tranzitivan po incidencijama i G-imprimitivan po točkama, Σ sustav imprimitivnosti na skupu točaka koji se sastoji od d blokova imprimitivnosti kardinalnosti c. Tada je D/Σ 2-$(d, \delta, \frac{c^2\lambda}{\mu^2})$ dizajn G-tranzitivan po incidencijama.*

Dokaz. Neka su Δ_1 i Δ_2 dva različita bloka imprimitivnosti. Tada je

$$D/\Sigma(\Delta_1) \cap D/\Sigma(\Delta_2) = \{B \in \mathcal{B} \mid \Delta_i \cap D(B) \neq \emptyset, i = 1, 2\}.$$

Skup $\Pi = \{(p_1, p_2, B) \mid B \in \mathcal{B}, p_i \in \Delta_i \cap D(B), i = 1, 2\}$ je kardinalnosti $c^2\lambda$. Za funkciju $\pi : \Pi \to D/\Sigma(\Delta_1) \cap D/\Sigma(\Delta_2)$ definiranu s

$$\pi(p_1, p_2, B) = B, \text{ za svaki } (p_1, p_2, B) \in \Pi,$$

vrijedi da je $\pi^{-1}(B)$ ekvipotentan skupu $(\Delta_1 \cap D(B)) \times (\Delta_2 \cap D(B))$, a on je kardinalnosti μ^2 za svaki B, pa je $D/\Sigma(\Delta_1) \cap D/\Sigma(\Delta_2)$ kardinalnosti $\frac{c^2\lambda}{\mu^2}$. Također, označimo s δ broj blokova imprimitivnosti s kojima proizvoljni blok $B \in \mathcal{B}$ ima neprazan presjek u D tj. $\delta = D/\Sigma(B)$. Tada za svaki blok $B \in \mathcal{B}$ vrijedi $|B| = \delta\mu$, tj. $\delta = \frac{k}{\mu}$, pa je D/Σ 2-$(d, \delta, \frac{c^2\lambda}{\mu^2})$ dizajn. ∎

Dizajn D/Σ nazivamo **kvocijentnim dizajnom dizajna D s obzirom na sustav imprimitivnosti Σ**.

Nadalje ćemo za dani sustav imprimitivnosti Σ koristiti oznake

$$\begin{aligned} c &= |\Delta| \text{ za svaki } \Delta \in \Sigma; \\ d &= |\Sigma|. \end{aligned}$$

Konstrukcije poddizajna i kvocijentnog dizajna s obzirom na dani sustav imprimitivnosti opisane su u [8, 22].

Dizajni D_Δ i D/Σ općenito neće biti jednostavni dizajni pa ćemo nadalje za njihove multiplicitete koristiti oznake θ_1 i θ_2 redom.

3.2 Neki primjeri dizajna tranzitivnih po incidencijama

Navedimo nekoliko primjera dizajna tranzitivnih po incidencijama.

Primjer 3.14 *(Afina geometrija, [2]) Neka je V n-dimenzionalni vektorski prostor nad poljem F_q i d prirodni broj strogo manji od n. Afina geometrija $AG_d(n,q)$ je incidencijska struktura kojoj su točke svi vektori iz V, a blokovi svi translati d-dimenzionalnih potprostora tj. $x+W$, pri čemu je $x \in V$, a W je d-dimenzionalni potprostor od V. Incidencija je dana relacijom "biti element".*

Afina geometrija $AG_d(n,q)$ je 2-(v,k,λ) dizajn pri čemu je $v=q^n$, $k=q^d$, $\lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$, $r = \begin{bmatrix} n \\ d \end{bmatrix}_q$ i $b = q^{n-d}\begin{bmatrix} n \\ d \end{bmatrix}_q$. Pritom je $\begin{bmatrix} n \\ i \end{bmatrix}_q$ broj svih i-dimenzionalnih potprostora n-dimenzionalnog vektorskog prostora nad F_q poznat kao Gaussov koeficijent i vrijedi

$$\begin{bmatrix} n \\ i \end{bmatrix}_q = \frac{(q^n-1)\,(q^{n-1}-1)\ldots(q^{n-i+1}-1)}{(q^i-1)\,(q^{i-1}-1)\ldots(q-1)}.$$

Grupa automorfizama tog dizajna je $AGL(n,q)$. Pokažimo da je afina geometrija tranzitivna po incidencijama. Neka su $(x, y+W)$ i $(x', y'+W')$ incidencije u $AG_d(n,q)$. Kako je $x \in y+W$, to je $x+W=y+W$ i analogno $x'+W'=y'+W'$. Sada odaberemo $A \in GL(n,q)$ koji bazu vektorskog prostora W prevodi u bazu prostora W'. Konačno imamo $(x'-Ax, A) \in AGL(n,q)$ za koji vrijedi:

$$\begin{aligned}
(x'-Ax,A)(x,y+W) &= ((x'-Ax,A)x, (x'-Ax,A)(x+W)) \\
&= (x'-Ax+Ax, x'-Ax+Ax+AW) \\
&= (x', x'+W') \\
&= (x', y'+W')\,.
\end{aligned}$$

Primjer 3.15 *(Projektivna geometrija, [2]) Neka je V $(n+1)$-dimenzionalni vektorski prostor nad poljem F_q pri čemu je n prirodni broj strogo veći od 1. Projektivna geometrija $PG_d(n,q)$ je incidencijska struktura kojoj su točke svi jednodimenzionalni potprostori od V, a blokovi svi $(d+1)$-dimenzionalni* *potprostori od* V*, za* $d \in \{1, ..., n-1\}$*. Incidencija je dana relacijom "biti potprostor".*

Projektivna geometrija $PG_d(n,q)$ *je 2-*(v,k,λ) *dizajn pri čemu je* $v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$, $k = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q$, $\lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$, $r = \begin{bmatrix} n \\ d \end{bmatrix}_q$ *i* $b = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q$*. Primijetimo da za* $d = n-1$ *imamo* $b = \begin{bmatrix} n+1 \\ n \end{bmatrix}_q = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = v$ *tj. projektivna geometrija* $PG_n(n,q)$ *je simetričan dizajn.*

Puna grupa automorfizama projektivne geometrije je $P\Gamma L(n+1,q) = PGL(n+1,q) \rtimes Aut(F_q)$*. Pokažimo da je ona tranzitivna po incidencijama. Neka su* $(\langle x_1 \rangle, W)$ *i* $(\langle x_1' \rangle, W')$ *incidencije u* $PG_d(n,q)$*. Odaberimo baze* $\{x_1, x_2, ...x_d\}$ *i* $\{x_1', x_2', ...x_d'\}$ *prostora* W *i* W' *redom. Sada odaberimo* $A \in PGL(n+1,q)$ *takav da vrijedi* $A\langle x_i \rangle = \langle x_i' \rangle$*. Konačno imamo:*

$$\begin{aligned} A(\langle x_1 \rangle, W) &= (A\langle x_1 \rangle, AW)) \\ &= (\langle x_1' \rangle, W'). \end{aligned}$$

Primjer 3.16 *(Cameron-Praeger, [7, 9]) Neka su* c, d, μ, δ *prirodni brojevi za koje vrijedi* $1 < \mu < c$ *i* $1 < \delta < d$*. Neka je* $P = \{1, ..., c\} \times \{1, ..., d\}$ *i* $\Delta_j = \{1, ..., c\} \times \{j\}$*, za svaki* $j \in \{1, ..., d\}$*. Također, neka je* $\mathcal{B}$ *skup svih* $B \subset P$ *takvih da je* $|B \cap \Delta_j| \in \{0, \mu\}$ *za svaki* $j \in \{1, ..., d\}$ *i* $|\{j \in \{1, ..., d\} \mid B \cap \Delta_j \neq \emptyset\}| = \delta$*.* $D = (P, \mathcal{B})$ *je 2-*(v,k,λ) *dizajn pri čemu je* $v = cd$*,* $k = \mu\delta$*,* $b = \binom{d}{\delta}\binom{c}{\mu}^d$*,* $\lambda = \frac{\binom{k}{2}}{\binom{v}{2}} b$*.*

Puna grupa automorfizama ovog dizajna je wreath produkt grupa S_c *i* S_d *tj.* $G = S_c \text{ wr } S_d$*. Elementi grupe* G *su funkcije na* P *oblika* (π, σ)*, pri čemu je* $\pi = (\pi_1, ..., \pi_d) \in S_c^d$*, i* $\sigma \in S_d$ *definirane s* $(\pi, \sigma)(i,j) = \left(\pi_{\sigma(j)}(i), \sigma(j)\right)$*. Skupovi* Δ_j *su blokovi imprimitivnosti grupe* G *po točkama i* D *je po točkama imprimitivni dizajn tranzitivan po incidencijama.*

U radu [7] Cameron i Praeger opisuju konstrukciju općenitijih blokovno tranzitivnih dizajna, ali mi navodimo samo primjer kad su takvi dizajni tranzitivni po incidencijama.

Primjer 3.17 *(Paley, [9]) Neka je F_q polje za koje je $q \equiv 3 (\bmod 4)$ i $F_q^{(2)} = \left\{x^2 \mid x \in F_q^*\right\}$. Definiramo jednostavnu incidencijsku strukturu P_q kojoj su točke F_q, a blokovi svi $x + F_q^{(2)}$ za svaki $x \in F_q$. Incidencijska struktura P_q je simetrični $(q, \frac{q-1}{2}, \frac{q-3}{4})$ dizajn.*

Neka je G grupa svih $f_{a,b} : F_q \to F_q$ bijekcija danih sa $f_{a,b}(x) = ax + b$ za svaki $a \in F_q^{(2)}$ i svaki $b \in F_q$. Grupa G je grupa automorfizama dizajna P_q. Pokažimo da djeluje tranzitivno po incidencijama. Neka je $\left(a, b + F_q^{(2)}\right)$ proizovljna incidencija. Tada je $f_{1,-b}\left(a, b + F_q^{(2)}\right) = \left(a - b, F_q^{(2)}\right)$, a kako je $a - b \in F_q^{(2)}$, to postoji $(a-b)^{-1} \in F_q^{(2)}$ te vrijedi $f_{(a-b)^{-1},0}\left(a - b, F_q^{(2)}\right) = \left(1, F_q^{(2)}\right)$ čime je dokazana tranzitivnost po incidencijama.

Puna grupa automorfizama dizajna P_q, za $q \geq 19$, je skup svih $f_{a,b,\sigma} : F_q \to F_q$ bijekcija danih s $f_{a,b,\sigma}(x) = a\sigma(x) + b$ za svaki $a \in F_q^{(2)}$ i svaki $b \in F_q$ i svaki $\sigma \in Aut(F_q)$. (vidi [13])

Primjer 3.18 *(Sferna geometrija, [9]) Neka je q potencija prostog broja i $\Omega = F_{q^n} \cup \{\infty\}$. Neka je $G = PGL(2, q^n)$ grupa koja se sastoji od svih bijekcija $f : \Omega \to \Omega$ koje su za sve $a, b, c, d \in F_{q^n}$, za koje je $ad - bc \neq 0$ dane pravilom*

$$\begin{aligned} f(x) &= \frac{ax+b}{cx+d}, \text{ za } x \neq \infty \text{ i } cx + d \neq 0, \\ f(\infty) &= \infty, \text{ za } c = 0, \\ f(\infty) &= \frac{a}{c}, \text{ za } c \neq 0, \\ f(-\frac{d}{c}) &= \infty, \text{ za } c \neq 0. \end{aligned}$$

Incidencijsku strukturu kojoj je skup točaka Ω, a skup blokova $G(F_q \cup \{\infty\})$ nazivamo sfernom geometrijom $SG(n, q)$. Ona je jednostavni 2-$(q^n + 1, q + 1, \frac{q^n - 1}{q - 1})$ dizajn tranzitivan po incidencijama.

Poglavlje 4

Primitivni dizajni tranzitivni po incidencijama

Često nam se prilikom potrage za imprimitivnim dizajnima javlja potreba za konstrukcijom određenog primitivnog dizajna ili dokazivanjem nepostojanja primitivnog dizajna s određenim parametrima. U ovom poglavlju opisat ćemo algoritam traženja dizajna s danim parametrima čija grupa automorfizama djeluje primitivno uz pomoć računala, konkretno računalnog programa MAGMA. Svi algoritmi mogu se pronaći u Dodatku.

Prvo ćemo konstruirati algoritam za provjeravanje tranzitivnosti po incidencijama nekog jednostavnog dizajna. Pritom ćemo koristiti uvjet dan u Propoziciji 3.9. Točnije, za dani dizajn odabrat ćemo proizvoljnu točku $p \in P$ nekog bloka $B \in \mathcal{B}$ te provjeriti je li omjer $\frac{|O \cap B|}{|O|}$ jednak $\frac{k-1}{v-1}$ za svaku netrivijalnu orbitu O stabilizatora točke p.

Blokovno tranzitivni dizajn $D = (P, \mathcal{B})$ je jednoznačno određen uređenim parom (G, B) gdje je G tranzitivna podgrupa od $Sym\,(P)$, a B proizvoljan element iz $\mathcal{B}$. Skup svih blokova $\mathcal{B}$ jednostavno možemo dobiti kao G-orbitu bloka B. Sada možemo za unešeni par (G, B) odrediti je li $D = (P, GB)$

dizajn tranzitivan po incidencijama. Algoritam 6.1 radi upravo to.

Sada opišimo algoritam za traženje netrivijalnih dizajna tranzitivnih po incidencijama s nekom primitivnom grupom automorfizama G. Prvo korištenjem Propozicije 3.9 odredimo moguće parametre k takvog dizajna. To radimo tako što za stabilizator proizvoljne točke p odredimo netrivijalne orbite $\{O_1, ..., O_n\}$ te za sve njih brojeve k za koje vrijedi da je $\frac{k-1}{v-1}|O_i| \in \mathbb{N}$ za svaki $i \in \{1, ..., n\}$. Za tako određene k potražimo sve moguće parametre b. Pritom koristimo sljedeće uvjete: $b \mid |G|$, $r = \frac{bk}{v} \in \mathbb{N}$, $\lambda = \frac{bk(k-1)}{v(v-1)} \in \mathbb{N}$ i $b < \binom{v}{k}$. Za sve uređene parove (k, b) odredimo sve podgrupe od G indeksa b jer su one kandidati za grupu G_B, a zatim odredimo njihove orbite kardinalnosti k. Ako takve postoje, onda su one kandidati za neki blok B. Sada koristeći Algoritam 6.1 provjerimo je li par (G, B) generira dizajn tranzitivan po incidencijama. MAGMA sadrži biblioteku svih primitvnih grupa danog stupnja $v \leq 4095$. Algoritam 6.3 za dani v računa, do na izomorfizam, sve moguće primitivne dizajne tranzitivne po incidencijama kojima je broj točaka kardinalnosti v .

Koristeći algoritam 6.3 konstruirali smo sve primitivne dizajne tranzitivne po incidencijama stupnja $v \leq 30$. Popis takvih dizajna nalazi se u dodatku u Tablici 10.

Sljedeći rezultat daje nam dovoljne uvjete za primitivnost po točkama dizajna tranzitivnog po incidencijama. Ovaj teorem ćemo posebno koristiti za dokazivanje primitivnosti po točkama Steinerovih 2-dizajna ($\lambda = 1$) tranzitivnih po incidencijama.

Teorem 4.1 (Kantor, [14]) *Grupa automorfizama G dizajna D tranzitivnog po incidencijama djeluje primitivno po točkama ako vrijedi nešto od sljedećeg:*

i) $r > \lambda(k-3)$;

ii) $\lambda > M(r, \lambda)(M(r, \lambda) - 1)$;

iii) $M(r, \lambda) = 1$;

iv) $M(r, \lambda) = 2$ *i* $\lambda \neq 2$;

v) $M(r, \lambda) = 2$ *i* $r \neq 2(k - 3)$;

vi) $M(r - \lambda, k) = 1$;

vii) $M(v, k) = 1$, $r = k + \lambda$ *i* k *nije kvadrat.*

Poglavlje 5

Simetrični imprimitivni dizajni tranzitivni po incidencijama

Teorem 4.1 nam daje naslutiti da je većina dizajna tranzitivnih po incidencijama primitivna po točkama. Naravno, simetričnost nam daje dodatnu restrikciju pa možemo pretpostaviti da ima jako malo simetričnih po točkama imprimitivnih dizajna tranzitivnih po incidencijama. U daljnjem radu bavit ćemo se isključivo takvim dizajnima, a primjeri simetričnih po točkama primitivnih dizajna mogu se pronaći u [4].

U ovom poglavlju pokušat ćemo pronaći sve simetrične imprimitivne dizajne tranzitivne po incidencijama kojima je parametar $\lambda \leq 10$. Pri filtriranju mogućih parametara pomoći će nam i sljedeći teorem iz [9].

Teorem 5.1 *Neka je D (v, k, λ) simetrični dizajn i neka je $g \in Aut(D)$. Tada automorfizam g ima jednak broj fiksnih točaka i fiksnih blokova.*

Korištenjem Propozicije 1.25 i Teorema 5.1 lako dobijemo sljedeći rezultat.

Teorem 5.2 *Neka je $D = (P, \mathcal{B}, I)$ (v, k, λ) simetrični dizajn i neka je G grupa automorfizama dizajna D. Tada je broj G-orbita na skupovima P i $\mathcal{B}$ jednak.*

Važnu ulogu u filtraciji dopustivih parametara potencijalnih dizajna ima i sljedeći teorem.

Teorem 5.3 (Bruck-Ryser-Chowla, [9]) *U (v, k, λ) simetričnom dizajnu vrijedi:*

i) ako je v paran, onda je $k - \lambda$ kvadrat prirodnog broja;

ii) ako je v neparan, onda postoji uređena trojka $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$ takva da je

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

Ključan teorem u potrazi za simetričnim imprimitivnim dizajnima tranzitivnim po incidencijama s "malim" λ dali su Praeger i Zhou. Teorem 5.4 daje nužne uvjete koje takvi potencijalni dizajni trebaju ispunjavati.

Teorem 5.4 (Praeger, Zhou, [18]) *Neka je G grupa, $D = (P, \mathcal{B})$ netrivijalni (v, k, λ) simetrični dizajn G-tranzitivan po incidencijama, Σ sustav imprimitivnosti za G na skupu točaka koji se sastoji od d blokova imprimitivnosti kardinalnosti c. Tada postoji $\mu \in \mathbb{N}$ takav da je $|B \cap \Delta| \in \{0, \mu\}$ za sve $B \in \mathcal{B}$ i $\Delta \in \Sigma$ i također vrijedi jedna od sljedećih tvrdnji:*

(a) $k \leq \frac{\lambda(\lambda-3)}{2}$;

(b) $(v, k, \lambda) = (\lambda^2(\lambda + 2), \lambda(\lambda + 1), \lambda)$ i $(c, \mu) \in \{(\lambda^2, \lambda), (\lambda + 2, 2)\}$;

(c) $(v, k, \lambda, c, \mu) = (\frac{(\lambda+2)(\lambda^2-2\lambda+2)}{4}, \frac{\lambda^2}{2}, \lambda, \frac{\lambda+2}{2}, 2)$ i vrijedi $\lambda \equiv 0 (\mathrm{mod}\, 4)$ ili $\lambda = 2u^2$, u neparan, $u \geq 3$ i $2(u^2 - 1)$ kvadrat prirodnog broja;

(d) $(v, k, \lambda, c, \mu) = (\frac{(\lambda+6)(\lambda^2+4\lambda-1)}{4}, \frac{\lambda(\lambda+5)}{2}, \lambda, \lambda+6, 3)$ i vrijedi $\lambda \equiv 1 (\mathrm{mod}\, 6)$ ili $\lambda \equiv 3 (\mathrm{mod}\, 6)$.

Propozicija 3.13 nam omogućava poboljšanje prethodnog rezultata.

Propozicija 5.5 *U Teoremu 5.4 u slučaju (b), za* $c = \lambda + 2$ *vrijedi da je* λ *paran, a u slučaju (d)* $\lambda \equiv 3 \pmod 6$.

Dokaz. Pretpostavimo da je $c = \lambda + 2$ i da je λ neparan. Tada je D/Σ 2-$(d, \delta, \frac{c^2\lambda}{\mu^2})$ dizajn što je kontradikcija jer $\frac{(\lambda+2)^2\lambda}{4} \notin \mathbb{N}$.

Nadalje, u slučaju (d) pretpostavimo da je $\lambda \equiv 1 \pmod 6$. Onda postoji $u \in \mathbb{N}_0$ takav da je $\lambda = 6u + 1$. Tada je D/Σ 2-$(d, \delta, \frac{c^2\lambda}{\mu^2})$ dizajn, što je kontradikcija jer $\frac{c^2\lambda}{\mu^2} = \frac{(6u+7)^2(6u+1)}{9} = 24u^3 + 60u^2 + 42u + \frac{49}{9} \notin \mathbb{N}$. ■

Sada ćemo korištenjem poboljšanog prethodnog teorema popisati sve moguće petorke parametara (v, k, λ, c, μ) simetričnih dizajna tranzitivnih po incidencijama i imprimitivnih po točkama za koje je $\lambda \leq 10$.

Teorem 5.6 *Neka je* G *grupa i* $\lambda \leq 10$, $D = (P, \mathcal{B})$ *netrivijalni* (v, k, λ) *simetrični dizajn* G*-tranzitivan po incidencijama,* Σ *netrivijalni sustav imprimitivnosti za* G *na skupu točaka, koji se sastoji od* d *blokova imprimitivnosti kardinalnosti* c *i neka je* $\mu \in \mathbb{N}$ *takav da je* $|B \cap \Delta| \in \{0, \mu\}$ *za sve* $B \in \mathcal{B}$ *i sve* $\Delta \in \Sigma$. *Tada takav dizajn ima jednu od petorki parametara danih* *u Tablici 1:*

Tablica 1

br. retka	v	k	λ	c	μ	*slučaj iz Teorema 5.4*
1	16	6	2	4	2	(b)
2	45	12	3	9	3	(b) i (d)
3	96	20	4	16	4	(b)
4	96	20	4	6	2	(b)
5	15	8	4	3	2	(c)
6	175	30	5	25	5	(b)
7	288	42	6	36	6	(b)
8	288	42	6	8	2	(b)
9	27	14	7	3	2	(a)
10	441	56	7	49	7	(b)
11	640	72	8	64	8	(b)
12	640	72	8	10	2	(b)
13	125	32	8	5	2	(c)
14	35	18	9	5	3	(a)
15	891	90	9	81	9	(b)
16	435	63	9	15	3	(d)
17	39	20	10	3	2	(a)
18	120	35	10	15	5	(a)
19	1200	110	10	100	10	(b)
20	1200	110	10	12	2	(b)

Dokaz. Prvo po Teoremu 4.1 imamo da za dizajn koji je tranzitivan po incidencijama iz $(r, \lambda) = 1$ slijedi da je primitivan po točkama, pa za $\lambda = 1$ nemamo simetričnih dizajna imprimitivnih po točkama. Sada potražimo moguće parametre za dizajne s $\lambda \in \{2, ..., 10\}$.

Slučaj b) Teorema 5.4 će nam za svaki $\lambda \in \{2, 4, 6, 8, 10\}$ dati po dvije moguće petorke parametara takvog potencijalnog dizajna, posebno će za $\lambda = 2$ te dvije petorke biti jednake, dok će za svaki $\lambda \in \{3, 5, 7, 9\}$ dati po jednu moguću petorku parametara. Tih trinaest slučajeva se nalaze u retcima 1, 2, 3, 4, 6, 7, 8, 10, 11, 12, 15, 19 i 20 Tablice 1.

Slučaj c) zbog uvjeta $\lambda \equiv 0 (\mathrm{mod}\, 4)$ ili $\lambda = 2u^2, u \geq 3$ daje parametre samo za $\lambda \in \{4, 8\}$, dok slučaj d) zbog uvjeta $\lambda \equiv 3 (\mathrm{mod}\, 6)$ daje parametre za $\lambda \in \{3, 9\}$. Pritom za $\lambda = 3$ dobijemo istu petorku parametara kao i u slučaju b) za $\lambda = 3$. Slučajevi c) i d) se nalaze u retcima 2, 5, 13 i 16 Tablice 1.

Analizirajmo još moguće petorke parametara koje proizlaze iz slučaja a) Teorema 5.4.

Za dani λ možemo odrediti gornju granicu za parametar k takvog potencijalnog dizajna. Za $\lambda = 2, 3$ vrijedi $k \leq 0$ što je nemoguće. U Tablici 2 navedimo gornje granice za parametar k za svaki $\lambda \in \{4, ..., 10\}$.

Tablica 2

λ	gornja granica parametra k $(\frac{\lambda(\lambda-3)}{2})$
4	2
5	5
6	9
7	14
8	20
9	27
10	35

Kako za sve dizajne vrijedi $\lambda(v-1) = r(k-1)$, a posebno za simetrične dizajne imamo $r = k$, to je $v = \frac{k(k-1)}{\lambda} + 1$. Kako broj točaka mora biti prirodan broj, to nam reducira broj mogućih kandidata za k. Također, zbog

$k < v$, vrijedi $r = k > \lambda$. U Tablici 3 navedimo kandidate za parametar k za svaki $\lambda \in \{4, ..., 10\}$ uzimajući u obzir gornje granice dane u Tablici 2.

Tablica 3

λ	kandidati za parametar k
4	nema
5	nema
6	7, 9
7	8, 14
8	9, 16, 17
9	10, 18, 19, 27
10	11, 15, 16, 20, 21, 25, 26, 30, 31, 35

U svakom imprimitivnom dizajnu vrijedi $\delta \neq 1$. Naime kad bi δ bio jednak 1 onda bi zbog $k = \mu\delta$ vrijedilo $k = \mu$ pa bi zbog $\frac{v-1}{k-1} = \frac{c-1}{\mu-1}$ vrijedilo $v = c$, a to je u kontradikciji s činjenicom da je dizajn imprimitivan. Kako smo već prije pokazali da je i $\mu \neq 1$, to znači da u imprimitivnom dizajnu k ne može biti prost broj. Izračunajmo sada pripadne parametre v za svaki od mogućih parova parametara (λ, k). Rezultati su dani u Tablici 4.

Tablica 4

(λ, k)	v	(λ, k)	v
(6,9)	13	(10,15)	22
(7,8)	9	(10,16)	25
(7,14)	27	(10,20)	39
(8,9)	10	(10,21)	43
(8,16)	31	(10,25)	61
(9,10)	11	(10,26)	66
(9,18)	35	(10,30)	88
(9,27)	79	(10,35)	120

Budući da u imprimitivnom dizajnu vrijedi $v = cd$ pri čemu su i c i d različiti od 1 to v ne može biti prost broj. Također, kako tražimo isključivo netrivijalne dizajne, mora vrijediti $k < v - 1$. Dakle, jedini moguće trojke parametara (v, k, λ) proizašlih iz slučaja a) su sljedeće: (27,14,7), (35,18,9), (22,15,10), (25,16,10), (39,20,10), (66,26,10), (88,30,10), (120,35,10).

Odmah vidimo da zbog slučaja i) Teorema 5.3 trojke parametara (22,15,10), (88,30,10) nisu dopustive.

Razmotrimo moguće parametre c i μ za preostalih 6 trojki parametara.

1. U slučaju $(v, k, \lambda) = (27, 14, 7)$ parametar c mora biti element skupa $\{3, 9\}$. Po Propoziciji 3.11 vrijedi $\frac{c-1}{\mu-1} = 2$ tj. za $c = 3$ imamo $\mu = 2$, a za $c = 9$ imamo $\mu = 5$, a kako $5 \nmid 14$, to mora biti $(v, k, \lambda, c, \mu) = (27, 14, 7, 3, 2)$.

2. U slučaju $(v, k, \lambda) = (35, 18, 9)$ parametar c mora biti element skupa $\{5, 7\}$. Sada iz $\frac{c-1}{\mu-1} = 2$ slijedi da za $c = 5$ imamo $\mu = 3$, a za $c = 7$ imamo $\mu = 4$, a kako $4 \nmid 18$, to mora biti $(v, k, \lambda, c, \mu) = (35, 18, 9, 5, 3)$.

3. U slučaju $(v, k, \lambda) = (25, 16, 10)$ parametar c mora biti 5, ali onda bi po Propoziciji 3.11 μ morao biti $\frac{7}{2}$ što je nemoguće pa je time ovaj slučaj eliminiran.

4. U slučaju $(v, k, \lambda) = (39, 20, 10)$ parametar c mora biti element skupa $\{3, 13\}$. Sada iz $\frac{c-1}{\mu-1} = 2$ slijedi da za $c = 3$ imamo $\mu = 2$, a za $c = 13$ imamo $\mu = 7$, a kako $7 \nmid 20$, to mora biti $(v, k, \lambda, c, \mu) = (39, 20, 10, 3, 2)$.

5. U slučaju $(v, k, \lambda) = (66, 26, 10)$ parametar μ mora biti element skupa $\{2, 13\}$. Sada iz $\frac{c-1}{\mu-1} = \frac{13}{5}$ slijedi da za $\mu = 2$ imamo $c = \frac{18}{5}$, a za $\mu = 13$ imamo $c = \frac{161}{5}$. Kako nijedan od ova dva c nije prirodan broj, ovaj je slučaj eliminiran.

6. U slučaju $(v, k, \lambda) = (120, 35, 10)$ parametar μ mora biti element skupa $\{5, 7\}$. Sada iz $\frac{c-1}{\mu-1} = \frac{7}{2}$ slijedi da za $\mu = 5$ imamo $c = 15$, a za $\mu = 7$ imamo $c = 22$. Kako $22 \nmid 120$, to mora biti $(v, k, \lambda, c, \mu) = (120, 35, 10, 15, 5)$.

Četiri dopustive petorke parametara iz slučaja a) nalaze se u retcima 9, 14, 17 i 18 Tablice 1.

Time smo ispitali sve mogućnosti za parametre (v, k, λ, c, μ) potencijalnog dizajna iz teorema. ■

Sada ćemo potražiti dizajne s danim petorkama parametara iz Tablice 1 ili pokušati dokazati njihovu neegzistenciju.

Prvo ćemo navesti poznate rezultate za slučajeve iz prvih pet redaka Tablice 1.

Q.M. Husein je u [12] dokazao sljedeći rezultat:

Teorem 5.7 *Postoje točno tri do na izomorfizam različita simetrična (16,6,2) dizajna.*

Napomena 5.8 *Regueiro je u [19] pokazala da su točno dva od tri simetrična (16,6,2)-dizajna tranzitivni po incidencijama i imprimitivni po točkama.*

Napomena 5.9 *Praeger je u [17] opisala konstrukciju i dokazala da postoji samo jedan simetrični imprimitivni po točkama (45,12,3)-dizajn tranzitivan po incidencijama.*

Napomena 5.10 *Law, Praeger i Reichard su u [16] dokazali da postoje četiri do na izomorfizam simetrična imprimitivna po točkama (96,20,4)-dizajna tranzitivna po incidencijama.*

Napomena 5.11 *Praeger i Zhou su u [18] dokazali da postoji točno jedan simetrični imprimitivni po točkama (15,8,4)-dizajn tranzitivan po incidencijama.*

Primjer 5.12 *Neka je* $D = (P, \mathcal{B}, I)$ $2-(v, k, \lambda)$ *dizajn. Incidencijska struktura* $D^c = (P, \mathcal{B}, I^c)$*, pri čemu je* $I^c = (P \times \mathcal{B}) \setminus I$*, je* $2-(v, v-k, b-2r+\lambda)$

dizajn. Nazivamo ga ***komplementom dizajna*** *D. Općenito vrijedi* $AutD = AutD^c$. *Tranzitivnost po incidencijama dizajna D ne povlači nužno i tranzitivnost po incidencijama dizajna* D^c. *U napomeni 5.11 (15,8,4)-dizajn je izomorfan komplementu projektivne geometrije* $PG_3\left(3,2\right)$. *Puna grupa automorfizama dizajna* $PG_3\left(3,2\right)$ *i* $PG_3\left(3,2\right)^c$ *djeluje tranzitivno po incidencijama i primitivno po točkama na oba dizajna. Međutim, dizajn* $PG_3\left(3,2\right)^c$ *ima grupu automorfizama koja djeluje tranzitivno po incidencijama i imprimitivno po točkama, dok dizajn* $PG_3\left(3,2\right)$ *nema takvu grupu.*

Propozicija 5.13 *Ne postoje* (v,k,λ) *simetrični dizajni tranzitivni po incidencijama i imprimitivni po točkama s parametrima iz redaka 13 i 16 Tablice 1.*

Dokaz. (Slučaj 13) Pretpostavimo da postoji (v,k,λ) simetrični dizajn tranzitivan po incidencijama i imprimitivan po točkama s danim parametrima. Kako je $v = 125$ neparan broj, to po Teoremu 5.3 postoji uređena trojka $(x,y,z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$ takva da je $x^2 = 24y^2 + 8z^2$. Ako trojka (x,y,z) zadovoljava jednadžbu $x^2 = 24y^2 + 8z^2$, onda ju zadovoljava i trojka (px,py,pz) i obratno za svaki $p \in \mathbb{Z}$ pa možemo odabrati trojku (x,y,z), koja zadovoljava danu jednadžbu, takvu da je $M(x,y,z) = 1$. Sada je $x^2 \equiv 2z^2 (\bmod 3)$. Pretpostavimo da je $z \not\equiv 0 (\bmod 3)$. Tada je $\left(\frac{x}{z}\right)^2 \equiv 2 (\bmod 3)$, što je nemoguće, pa je $z \equiv 0 (\bmod 3)$ tj. $z = 3z_0$ za neki $z_0 \in \mathbb{N}_0$. Sada je $x^2 = 24y^2 + 72z_0^2$ pa iz $3 \mid x^2$ slijedi i $3 \mid x$ pa je $x = 3x_0$ za neki $x_0 \in \mathbb{N}_0$. Slijedi $3x_0^2 = 8y^2 + 24z_0^2$ pa iz $3 \mid y^2$ slijedi i $3 \mid y$ te je $y = 3y_0$ za neki $y_0 \in \mathbb{N}_0$. Sada je $M(x,y,z) = M(3x_0, 3y_0, 3z_0) \neq 1$ što je kontradikcija s odabirom trojke (x,y,z).

(Slučaj 16) Pretpostavimo da postoji (v,k,λ) simetrični dizajn tranzitivan po incidencijama i imprimitivan po točkama s danim parametrima.

Kako je $v = 435$ neparan broj, to po Teoremu 5.3 postoji uređena trojka $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$ takva da je $x^2 = 54y^2 - 9z^2$. Opet možemo odabrati trojku (x, y, z), koja zadovoljava danu jednadžbu, takvu da je $M(x, y, z) = 1$. Sada je $x^2 \equiv 0 (\mathrm{mod}\, 3)$ pa iz $3 \mid x^2$ slijedi i $3 \mid x$ pa je $x = 3x_0$ za neki $x_0 \in \mathbb{N}_0$. Sada je $x_0^2 = 6y^2 - z^2$. Sada je $x_0^2 \equiv 2z^2 (\mathrm{mod}\, 3)$. Pretpostavimo da je $z \not\equiv 0 (\mathrm{mod}\, 3)$. Tada je $\left(\frac{x_0}{z}\right)^2 \equiv 2 (\mathrm{mod}\, 3)$ što je nemoguće pa je $z \equiv 0 (\mathrm{mod}\, 3)$ tj. $z = 3z_0$ za neki $z_0 \in \mathbb{N}_0$.Tada slijedi da je $x_0^2 = 6y^2 - 9z_0^2$. tj. $3 \mid x_0$ pa imamo i $3 \mid y^2$, a onda slijedi i $3 \mid y$ pa je $y = 3y_0$ za neki $y_0 \in \mathbb{N}_0$. Sada je $M(x, y, z) = M(3x_0, 3y_0, 3z_0) \neq 1$ što je kontradikcija s odabirom trojke (x, y, z). ■

Propozicija 5.14 *Ne postoje (v, k, λ) simetrični dizajni tranzitivni po incidencijama i imprimitivni po točkama s parametrima iz redaka 9 i 17 Tablice 1.*

Dokaz. Pretpostavimo da postoje simetrični dizajni tranzitivni po incidencijama i imprimitivni po točkama kojima je petorka parametara (v, k, λ, c, μ) jednaka $(27, 14, 7, 3, 2)$ ili $(39, 20, 10, 3, 2)$. No tada je po Propoziciji 3.13 parametar $\lambda_{D/\Sigma}$ njihovog kvocijentnog dizajna jednak $\frac{c^2\lambda}{\mu^2}$, odnosno redom $\frac{63}{4}$ ili $\frac{45}{2}$, što je nemoguće. ■

5.1 Eliminacije uz pomoć MAGME

Za daljnje eliminacije bit će nam potrebno definirati još neke pojmove.

Definicija 5.15 *Neka su $\Sigma = \{\Delta_i \subseteq \Omega \mid i \in \{1, .., d\}\}$ i $\Sigma' = \{\Delta'_i \subseteq \Omega \mid i \in \{1, .., d'\}\}$ sustavi imprimitivnosti djelovanja grupe G na skup Ω. Kažemo da je sustav imprimitivnosti Σ* ***podsustav od*** *Σ' i pišemo $\Sigma \leq \Sigma'$ ako za svaki $\Delta_i \in \Sigma$ postoji $j \in \{1, .., d'\}$ takav da je $\Delta_i \subseteq \Delta'_j$.*

Definicija 5.16 *Neka je Σ sustav imprimitivnosti djelovanja grupe G na skup Ω. Kažemo da je Σ* ***minimalni sustav imprimitivnosti*** *tog djelovanja ako za svaki sustav imprimitivnosti Σ' tog djelovanja iz $\Sigma' \leq \Sigma$ slijedi $\Sigma' = \Sigma$.*

Definicija 5.17 *Neka je Σ sustav imprimitivnosti djelovanja grupe G na skup Ω. Kažemo da je Σ* ***maksimalni sustav imprimitivnosti*** *tog djelovanja ako za svaki sustav imprimitivnosti Σ' tog djelovanja iz $\Sigma \leq \Sigma'$ slijedi $\Sigma' = \Sigma$.*

Propozicija 5.18 *Neka su Σ i Σ' sustavi imprimitivnosti djelovanja grupe G na skup Ω. Ako je $\Sigma \leq \Sigma'$, onda $|\Delta| \mid |\Delta'|$ za sve $\Delta \in \Sigma$ i sve $\Delta' \in \Sigma'$.*

Dokaz. Kako je svaki $\Delta \in \Sigma$ sadržan u nekom $\Delta' \in \Sigma'$, to je svaki Δ' unija nekih $\Delta \in \Sigma$ koji su međusobno ekvipotentni pa postoji $n \in \mathbb{N}$ takav da je $|\Delta'| = n \cdot |\Delta|$ tj. $|\Delta| \mid |\Delta'|$. ∎

Neka je $\Sigma = \{\Delta_i \subseteq P \mid i \in \{1,..,d\}\}$ sustav imprimitivnosti grupe G automorfizama dizajna $D = (P, \mathcal{B}, I)$ G-tranzitivnog po incidencijama i G-imprimitivnog po točkama. Definirajmo djelovanje grupe G na skup Σ.

$$g\Delta_i = \Delta_j \Leftrightarrow (\exists x \in \Delta_i)(\exists y \in \Delta_j)\ gx = y.$$

Neka je $\varphi_\Sigma : G \to Sym(\Sigma)$ permutacijska reprezentacija grupe G na skupu Σ. Označimo s $K = G_{(\Sigma)}$ jezgru i s G^Σ sliku tog homomorfizma. Tada je po Teoremu 1.1 $G/K \cong G^\Sigma$. Jasno, ako je Σ maksimalni sustav imprimitivnosti, onda je G^Σ primitivna na Σ.

Neka je $\varphi_\Delta : G_\Delta \to Sym(\Delta)$ permutacijska reprezentacija grupe G_Δ na proizvoljnom skupu $\Delta \in \Sigma$. Jezgra tog homomorfizma je $G_{(\Delta)}$, a sliku označimo s $(G_\Delta)^\Delta$. Jasno, ako je Σ minimalni sustav imprimitivnosti, onda je $(G_\Delta)^\Delta$ primitivna na Δ.

Sada pogledajmo dosad neeliminirane slučajeve prikazane u Tablici 5:

Tablica 5

	v	k	λ	c	μ
6	175	30	5	25	5
7	288	42	6	36	6
8	288	42	6	8	2
10	441	56	7	49	7
11	640	72	8	64	8
12	640	72	8	10	2
14	35	18	9	5	3
15	891	90	9	81	9
18	120	35	10	15	5
19	1200	110	10	100	10
20	1200	110	10	12	2

Primijetimo da je po Propoziciji 5.18 u svim preostalim slučajevima sustav imprimitivnosti Σ istovremeno i minimalan i maksimalan. Samim time u svim preostalim slučajevima su grupe G^{Σ} i $(G_{\Delta})^{\Delta}$ primitivne.

Daljnju teorijsku analizu provodimo isključivo za slučaj kad su G^{Σ} i $(G_{\Delta})^{\Delta}$ primitivne.

Sljedeću eliminaciju provest ćemo uz pomoć programskog paketa MAGMA:

Propozicija 5.19 *Ne postoje (v, k, λ) simetrični dizajni tranzitivni po incidencijama i imprimitivni po točkama s parametrima iz redaka 18, 19 i 20 Tablice 1.*

Dokaz. (Slučaj 18). Pretpostavimo da postoji takav dizajn. Tada za broj blokova b_1 njegovog poddizajna vrijedi $b_1 = \frac{c\delta}{\theta_1} = \frac{105}{\theta_1}$. Sada iz $\theta_1|\lambda$ i $b_1 \geq c$ slijedi $b_1 \in \{21, 105\}$. Kako su parametri poddizajna $(15, 5, 10)$, to su parametri pojednostavnjenja tog dizajna $(15, 5, \frac{10}{\theta_1})$, a lako se vidi da takav primitivan dizajn tranzitivan po incidencijama s traženim brojem blokova ne postoji (vidi Algoritam 6.4).

(Slučaj 19). Analognim zaključivanjem dobijemo $b_1 \in \{110, 220, 550, 1100\}$, a 2-$(100, 10, \frac{10}{\theta_1})$ primitivan dizajn tranzitivan po incidencijama s takvim brojem blokova ne postoji (vidi Algoritam 6.4).

(Slučaj 20). Pretpostavimo da postoji takav dizajn. Tada za broj blokova b_2 njegovog kvocijentnog dizajna vrijedi $b_2 = \frac{v}{\theta_2} = \frac{1200}{\theta_2}$. Sada iz $b_2 \geq d$ slijedi $b_2 \in \{100, 120, 200, 240, 300, 400, 600, 1200\}$, a 2-$(100, 55, \frac{360}{\theta_2})$ primitivan dizajn tranzitivan po incidencijama s takvim brojem blokova ne postoji (vidi Algoritam 6.4). ■

Za daljnje eliminacije promotrimo dva bitno različita slučaja u ovisnosti o K, tj. kada je K trivijalna i kada nije.

Ako je K trivijalna, onda je G izomorfna primitivnoj grupi stupnja d ($G \cong G/K \cong G^{\Sigma}$). Kako G djeluje tranzitivno na skup incidencija kojih ima bk (u simetričnim dizajnima isto što i vk), to kardinalnost skupa incidencija mora dijeliti red grupe G koja je podgrupa od S_d. Dakle, mora biti ispunjen uvjet

$$vk \mid d!.$$

Dani uvjet nije ispunjen u slučajevima iz redaka 6, 7, 10, 11 i 15 pa znamo da sigurno ne postoje dizajni tranzitivni po incidencijama s tim parametrima kojima bi K bila trivijalna. Eventualne dizajne tranzitivne po incidencijama iz slučajeva 8, 12, i 14 potražimo uz pomoć MAGME.

U ovim slučajevima prvo uzmemo sve primitivne grupe stupnja d koje su kandidati za grupu G^{Σ} i u svakoj od njih odredimo stabilizator proizvoljne točke. On je kandidat za grupu G_{Δ}. U takvoj grupi potražimo sve maksimalne podgrupe indeksa c koje su kandidati za stabilizator točke G_p. Tražimo isključivo maksimalne podgrupe jer su sustavi imprimitivnosti traženih dizajna minimalni. Konstruiramo permutacijsku grupu G stupnja $v = cd$ koja je izomorfna grupi G^{Σ} kojoj je stabilizator točke G_p. Kako tražimo simetrične dizajne, imamo $v = b$ pa potražimo podgrupe grupe G indeksa v koje su kandidati za grupu G_B, a zatim u takvim grupama potražimo orbite kardinalnosti k koje su kandidati za blokove B traženog dizajna. Konačno, provjerimo da li je $D = (P, GB)$ dizajn tranzitivan po incidencijama. U slučajevima 8, 12 i 14 nema takvog dizajna za $K = 1$. (vidi: Algoritam 6.5).

Razmotrimo sada slučaj kada je K netrivijalna. Tada vrijede sljedeći rezultati.

Napomena 5.20 *U svim sljedećim teoremima pretpostavljamo da je $D = (P, \mathcal{B}, I)$ (v, k, λ) simetrični dizajn G-tranzitivan po incidencijama i G-imprimitivan po točkama pri čemu G djeluje vjerno i čuva particiju Σ na d blokova imprimitivnosti kardinalnosti c. Također, pretpostavljamo da je kardinalnost svakog nepraznog presjeka nekog bloka i bloka imprimitivnosti jednaka μ kao i da je za svaki $B \in \mathcal{B}$ broj blokova imprimitivnosti s kojima blok B ima neprazni presjek jednak δ.*

Promotrimo djelovanje grupe K na proizvoljni blok imprimitivnosti Δ tj. homomorfizam $f : K \to Sym(\Delta)$. Označimo s K^{Δ} sliku tog homomorfizma.

Lema 5.21 *Neka je $K \neq 1$. Tada je $K^{\Delta} \neq 1$ za svaki $\Delta \in \Sigma$.*

Dokaz. Pretpostavimo suprotno, tj. da postoji $\Delta \in \Sigma$ takav da je $K^{\Delta} = 1$. Promotrimo djelovanje K na skup točaka P. Neka je $k \in K$ proizvoljan i $p \in P$ proizvoljna točka. Označimo s Δ' blok imprimitivnosti u kojem se nalazi p. Neka je $g \in G$ takav da je $g\Delta = \Delta'$. Kako je $p \in \Delta'$, to je $g^{-1}p \in \Delta$. Sada je $gkg^{-1}p = gg^{-1}p = p$. Pa vidimo da za svaki $k \in K$, gkg^{-1} djeluje trivijalno na svaku točku $p' \in \Delta'$ tj. gKg^{-1} djeluje trivijalno na Δ', a kako je $K \trianglelefteq G$, to je $gKg^{-1} = K$. Sada imamo da K djeluje trivijalno na Δ', a kako je p' odabran proizvoljno, to K djeluje trivijalno na svaki blok imprimitivnosti, tj. $K = 1$ što je u kontradikciji s početnom pretpostavkom. ■

Lema 5.22 *Neka je $K \neq 1$. Tada K^{Δ} djeluje tranzitivno na Δ.*

Dokaz. Prvo uočimo da je K^{Δ} netrivijalna normalna podgrupa grupe $(G_{\Delta})^{\Delta}$. Sada tvrdnja slijedi direktno iz Propozicije 1.34. ■

Za proizvoljni blok $B \in \mathcal{B}$ promotrimo restrikciju homomorfizma $f : K \to Sym\,(\Delta)$ na stabilizator bloka K_B. Označimo s K_B^{Δ} sliku tog homomorfizma.

Lema 5.23 *Neka je $K \neq 1$. Za svaki $B \in \mathcal{B}$ vrijedi $[K : K_B] = c$.*

Dokaz. Kako K^{Δ} djeluje tranzitivno na Δ, to i K djeluje tranzitivno na Δ i to vrijedi za svaki $\Delta \in \Sigma$. Dakle, K pri djelovanju na P ima d orbita duljine c. Po Teoremu 5.2 K pri djelovanju na $\mathcal{B}$ također ima d orbita koje su, zbog $K \trianglelefteq G$, jednake duljine, a kako zbog simetričnog dizajna imamo $|\mathcal{B}| = |P|$, to one moraju biti duljine c. Sada po Propoziciji 1.23 vrijedi $[K : K_B] = c$ za svaki $B \in \mathcal{B}$. ■

Propozicija 5.24 *Neka je $K \neq 1$. Tada je $\theta_2 = c$.*

Dokaz. Prvo uočimo da je $S = \{B' \in \mathcal{B} \mid D/\Sigma(B') = D/\Sigma(B)\}$ K-skup za svaki $B \in \mathcal{B}$. Za proizvoljni $k \in K$ vrijedi $D/\Sigma(kB') = k(D/\Sigma(B'))$, a kako je $k \in K = G_{(\Sigma)}$, on djeluje trivijalno na svaku točku kvocijentnog dizajna pa je $k(D/\Sigma(B')) = D/\Sigma(B')$ tj. $kB' \in S$. Sada je S unija orbita od K, a kako je $|S| = \theta_2$ i sve orbite od K po blokovima su duljine c, to postoji $n \in \mathbb{N}$ takav da je $\theta_2 = nc$. Sada koristeći Fisherovu nejednakost na pojednostavnjenju kvocijentnog dizajna dobijemo:

$$d \leq \frac{b}{\theta_2} = \frac{v}{\theta_2} = \frac{cd}{\theta_2},$$

tj. $\theta_2 \leq c$. Konačno, mora biti $n = 1$ tj. $\theta_2 = c$. ■

Propozicija 5.25 *Neka je $K \neq 1$. Tada je D/Σ^S simetrični dizajn.*

Dokaz. Kako je $\theta_2 = c$, to je broj blokova dizajna D/Σ^S jednak $\frac{b}{\theta_2} = \frac{v}{c} = \frac{cd}{c} = d$, što je jednako broju točaka tog dizajna. ■

Propozicija 5.26 *Neka je $K \neq 1$. Indeks grupe K^Δ po podgrupi K_B^Δ dijeli c.*

Dokaz. Vrijedi $[K : K_B] = \frac{|K|}{|K_B|} = \frac{|K^\Delta||K_{(\Delta)}|}{|K_B^\Delta||K_{B,(\Delta)}|} = \left[K^\Delta : K_B^\Delta\right]\left[K_{(\Delta)} : K_{B,(\Delta)}\right]$. Kako je $[K : K_B] = c$, to $\left[K^\Delta : K_B^\Delta\right] \mid c$. ■

Propozicija 5.27 *Neka je $K \neq 1$. Postoje orbite od K_B^Δ čija je unija kardinalnosti μ.*

Dokaz. Skup $B \cap \Delta$ je K_B^Δ-skup i kardinalnosti je μ. ■

Propozicija 5.28 *Ne postoje (v, k, λ) simetrični dizajni tranzitivni po incidencijama i imprimitivni po točkama s parametrima iz redaka 7, 12 i 14 Tablice 1.*

Dokaz. (Slučaj 7.) Prvo izračunajmo broj blokova pojednostavnjenja poddizajna D_Δ^S. On je jednak $\frac{c\delta}{\theta_1}$, a kako je $\theta_1 \mid \lambda$, to je $b \in \{42, 84, 126, 252\}$. Sada uz pomoć MAGME potražimo moguće kandidate za grupu $(G_\Delta)^\Delta$. Takva grupa za $b \in \{42, 126\}$ ne postoji. Za $b \in \{84, 252\}$ jedini kandidati za te grupe su $PSL(2, 8)$ i $P\Gamma L(2, 8)$. Sada potražimo kandidate za grupu K^Δ. Jedina normalna netrivijalna podgrupa grupe $PSL(2, 8)$ je ona sama, dok je u $P\Gamma L(2, 8)$ osim nje same normalna i grupa $PSL(2, 8)$. Koristeći Propoziciju 5.26 potražimo kandidate za K_B^Δ tj. grupama $PSL(2, 8)$ i $P\Gamma L(2, 8)$

potražimo sve podgrupe takve da indeks tih podgrupa dijeli c. Svi kandidati na skupu od 36 točaka imaju jednu od sljedeće četiri orbitne strukture: $\{1^1, 14^1, 21^1\}$, $\{1^1, 7^3, 14^1\}$, $\{8^1, 28^1\}$ i $\{36^1\}$ (orbitne strukture zapisujemo kao multiskupove). Kako po Propoziciji 5.27 u traženom dizajnu mora postojati unija orbita grupe K_B^Δ kardinalnosti 6, vidimo da takav dizajn ne postoji.

(Slučaj 12.) Računajući kao i u slučaju 7 broj blokova pojednostavnjenja poddizajna D_Δ^S mora biti iz skupa $\{45, 90, 180, 360\}$, no kako je $c = 10$ i $\mu = 2$, to je maksimalan broj blokova jednostavnog dizajna $\binom{10}{2}$ pa mora biti $b = 45$.

Dalje postupak ponavljamo kao u dokazu slučaja 7. Svi kandidati za grupu K_B^Δ imaju jednu od sljedeće dvije orbitne strukture: $\{1^1, 9^1\}$ i $\{10^1\}$. Kako po Propoziciji 5.27 u traženom dizajnu mora postojati unija orbita grupe K_B^Δ kardinalnosti 2, vidimo da takav dizajn ne postoji.

(Slučaj 14.) Broj blokova pojednostavnjenja poddizajna D_Δ^S mora biti iz skupa $\{10, 30\}$, no kako je $c = 5$ i $\mu = 3$, to je maksimalan broj blokova jednostavnog dizajna $\binom{5}{3}$ pa mora biti $b = 10$. Orbitne strukture potencijalnih grupa K_B^Δ su $\{1^1, 4^1\}$ i $\{5^1\}$ pa vidimo da ne postoji unija orbita kardinalnosti 3, a samim time ni traženi dizajn. $\blacksquare$

Lema 5.29 *Za svaki $\Delta \in \Sigma$ grupa K^Δ je izomorfna grupi $KG_{(\Delta)}/G_{(\Delta)}$.*

Dokaz. Po Teoremu 1.1 je $K^\Delta \cong K/K_{(\Delta)}$. Kako se u $K_{(\Delta)}$ nalaze svi elementi iz K koji fiksiraju cijeli Δ, očito je $K_{(\Delta)} = K \cap G_{(\Delta)}$. Sada imamo $K/K_{(\Delta)} = K/(K \cap G_{(\Delta)})$, a kako je $G_{(\Delta)} \trianglelefteq G$ po Teoremu 1.2 vrijedi $K/(K \cap G_{(\Delta)}) \cong KG_{(\Delta)}/G_{(\Delta)}$. Konačno imamo $K^\Delta \cong KG_{(\Delta)}/G_{(\Delta)}$. $\blacksquare$

Propozicija 5.30 *Postoji normalna podgrupa N grupe $\left(G^\Sigma\right)_\Delta$ izomorfna grupi $G_{(\Delta)}/K_{(\Delta)}$ takva da je $\left(G^\Sigma\right)_\Delta/N \cong (G_\Delta)^\Delta/K^\Delta$.*

Dokaz. Neka je $N = KG_{(\Delta)}/K$. Prvo pokažimo da je $N \cong G_{(\Delta)}/K_{(\Delta)}$. Dakle, po Teoremu 1.2 $KG_{(\Delta)}/K \cong G_{(\Delta)}/(G_{(\Delta)} \cap K) = G_{(\Delta)}/K_{(\Delta)}$ pa je prva tvrdnja dokazana. Sada dokažimo da je $\left(G^{\Sigma}\right)_{\Delta}/N \cong (G_{\Delta})^{\Delta}/K^{\Delta}$. Prvo uočimo da je po Teoremu 1.1 $\left(G^{\Sigma}\right)_{\Delta} \cong G_{\Delta}/K$. Sada je $\left(G^{\Sigma}\right)_{\Delta}/N \cong (G_{\Delta}/K)/(KG_{(\Delta)}/K)$, a ta grupa je po Teoremu 1.3 izomorfna grupi $G_{\Delta}/KG_{(\Delta)}$. S druge strane grupa $(G_{\Delta})^{\Delta}/K^{\Delta}$ je po Teoremu 1.1 i Lemi 5.29 izomorfna grupi $\left(G_{\Delta}/G_{(\Delta)}\right)/\left(KG_{(\Delta)}/G_{(\Delta)}\right)$ koja je po Teoremu 1.3 također izomorfna $G_{\Delta}/KG_{(\Delta)}$ čime je propozicija dokazana. ■

Primjenom Propozicija 5.26, 5.27 i 5.30 možemo ograničiti izbor mogućih kandidata za grupe $(G_{\Delta})^{\Delta}$, K^{Δ} i G^{Σ}, a u nekim slučajevima ih čak i u potpunosti eliminirati. U slučaju iz retka 11 ne postoji kombinacija tih grupa koja bi zadovoljila sve tri propozicije.

Propozicija 5.31 *Ne postoje (v, k, λ) simetrični dizajni tranzitivni po incidencijama i imprimitivni po točkama s parametrima iz retka 11 Tablice 1.*

Dokaz. Prvo uz pomoć MAGME odredimo sve moguće kandidate za grupu $\left(G^{\Sigma}\right)_{\Delta}$, a zatim odredimo sve njihove normalne podgrupe i njihove indekse. U ovom slučaju indeks takve normalne podgrupe mora biti u skupu {1, 2, 4, 8, 16, 36, 72, 144, 181440, 362880}. Sada potražimo kandidate za grupu $(G_{\Delta})^{\Delta}$ i njihove normalne podgrupe K^{Δ} čiji je indeks iz prethodno navedenog skupa. U svim K^{Δ} potražimo kandidate za K_B^{Δ} . Orbitne strukture takvih potencijalnih grupa K_B^{Δ} su sljedeće: $\{1^1, 3^{21}, 21^1\}$, $\{1^1, 9^7\}$, $\{1^1, 9^4, 27^1\}$, $\{1^1, 9^1, 27^2\}$, $\{1^1, 18^2, 27^1\}$, $\{1^1, 27^1, 36^1\}$, $\{1^1, 63^1\}$, $\{4^1, 12^5\}$, $\{16^1, 48^1\}$, $\{28^1, 36^1\}$, $\{64^1\}$ pa vidimo da ne postoji unija orbita kardinalnosti 8, a samim time ni traženi dizajn. ■

Pogledajmo koje kombinacije grupa $(G_{\Delta})^{\Delta}$, K^{Δ} i G^{Σ} zadovoljavaju Propozicije 5.26, 5.27 i 5.30 u preostala četiri slučaja (Tablice 6-9)

Napomena 5.32 *U prikazima grupa koristimo notaciju iz programskog paketa MAGMA. Oznaka pr(X, Y) označava primitivnu grupu koja se u MAGMINOJ biblioteci primitivnih grupa stupnja X nalazi pod identifikacijom Y. Oznaka (X, Y) označava grupu iz MAGMINE biblioteke grupa reda X pod identifikacijom Y.*

Tablica 6

Slučaj 6: $(v,k,\lambda,c,\mu) = (175,30,5,25,5)$			
Grupa	$(G_\Delta)^\Delta$	K^Δ	G^Σ
	$pr(25,13)$	$(100,11)$	$pr(7,4)$
	$pr(25,14)$	$(100,11)$	$pr(7,5)$
	$pr(25,19)$	$(100,11)$	$pr(7,5)$

Tablica 7

Slučaj 8: $(v,k,\lambda,c,\mu) = (288,42,6,8,2)$			
Grupa	$(G_\Delta)^\Delta$	K^Δ	G^Σ
	$pr(8,3)$	$(8,5)$	$pr(36,14)$

Tablica 8

Slučaj 10: $(v,k,\lambda,c,\mu) = (441,56,7,49,7)$			
Grupa	$(G_\Delta)^\Delta$	K^Δ	G^Σ
	$pr(49,9)$	$(98,4)$	$pr(9,5)$
	$pr(49,10)$	$(98,4)$	$pr(9,2)$
	$pr(49,22)$	$(98,4)$	$pr(9,7)$
	$pr(49,23)$	$(294,13)$	$pr(9,5)$
	$pr(49,24)$	$(294,13)$	$pr(9,2)$
	$pr(49,29)$	$(294,13)$	$pr(9,7)$

Tablica 9

Slučaj 15: $(v,k,\lambda,c,\mu)=(891,90,9,81,9)$			
Grupa	$(G_\Delta)^\Delta$	K^Δ	G^Σ
	$pr(81,45)$	$(648,711)$	$pr(11,4)$
	$pr(81,110)$	$(162,54)$	$pr(11,5)$
	$pr(81,115)$	$(324,164)$	$pr(11,5)$
	$pr(81,120)$	$(648,711)$	$pr(11,5)$
	$pr(81,133)$	$(324,164)$	$pr(11,6)$
	$pr(81,138)$	$(648,711)$	$pr(11,6)$

U svim mogućim slučajevima kandidati za grupu $(G_\Delta)^\Delta$ i K^Δ su grupe afinog tipa.

Nadalje pretpostavljamo da je $(G_\Delta)^\Delta$ primitivna grupa afinog tipa stupnja $c=p^\alpha$. Primijetimo da K^Δ ne mora nužno biti primitivna.

Sada za grupu X, s $[X]_p$ označimo skup $\{N\trianglelefteq X \mid |N|=p^a \text{ za neki } a\in\mathbb{N}_0\}$. Označimo s $O_p(X)$ maksimalnu grupu u skupu $[X]_p$. Kako iz $N_1,N_2\in[X]_p$ slijedi $N_1N_2\in[X]_p$, vidimo da je $O_p(X)$ dobro definirana, tj. postoji jedinstvena takva grupa u $[X]_p$.

Podgrupu translacija od $(G_\Delta)^\Delta$ označit ćemo s $T(\Delta)$. Može se pokazati da je $O_p((G_\Delta)^\Delta)=T(\Delta)$ (vidi [16]).

Često ćemo točke iz skupa Δ poistovjetiti s elementima iz $T(\Delta)$ budući da $T(\Delta)$ djeluje regularno na Δ. Također, skup Ω poistovjećujemo s $\bigcup_{i=1}^{d}T(\Delta_i)$, a K će biti podgrupa skupa $\left(\prod_{i=1}^{d}T(\Delta_i)\right)\rtimes GL(n,p)^d$ koja djeluje na $\bigcup_{i=1}^{d}T(\Delta_i)$ s

$$(x,A)v=x_i+A_iv,$$

$$\text{za sve } (x,A)\in\left(\prod_{i=1}^{d}T(\Delta_i)\right)\rtimes GL(n,p)^d,\ v\in T(\Delta_i).$$

Propozicija 5.33 *Ako je $N \trianglelefteq G$, onda je $gN_{(\Delta)}g^{-1} = N_{(g\Delta)}$ za sve $\Delta \in \Sigma$ i sve $g \in G$. Također, tada su svi $N_{(\Delta)} = 1$ ili su svi $N_{(\Delta)}$ međusobno različiti.*

Dokaz. Neka su $\Delta \in \Sigma$ i $g \in G$ proizvoljni.

Neka je $x \in gN_{(\Delta)}g^{-1}$. Tada postoji $h \in N_{(\Delta)}$ takav da je $x = ghg^{-1}$. Neka je $g\delta \in g\Delta$ proizvoljan. Sada je

$$xg\delta = ghg^{-1}g\delta = gh\delta = g\delta,$$

pa je $x \in G_{(g\Delta)}$. Kako je $N \trianglelefteq G$, to je $ghg^{-1} \in N$ pa je konačno $x \in N_{(g\Delta)}$. Dakle, $gN_{(\Delta)}g^{-1} \subseteq N_{(g\Delta)}$.

Obratno, neka je $x \in N_{(g\Delta)}$. Neka je $\delta \in \Delta$ proizvoljan. Tada je $g\delta \in g\Delta$ za svaki $g \in G$ pa je $xg\delta = g\delta$ tj. $g^{-1}xg\delta = \delta$. Sada je $g^{-1}xg \in G_{(\Delta)}$. Također, zbog normalnosti od N je $g^{-1}xg \in N$ pa je $g^{-1}xg \in N_{(\Delta)}$ tj. $x \in gN_{(\Delta)}g^{-1}$.

Pokažimo sada drugu tvrdnju. Na skupu Σ definirajmo relaciju ekvivalencije sa $\Delta \sim \Delta'$ ako i samo ako $N_{(\Delta)} = N_{(\Delta')}$. Kako iz $\Delta \sim \Delta'$ za svaki $g \in G$ slijedi $N_{(g\Delta)} = gN_{(\Delta)}g^{-1} = gN_{(\Delta')}g^{-1} = N_{(g\Delta')}$ tj. $g\Delta \sim g\Delta'$, vidimo da je ovo G-relacija, odnosno G čuva particiju induciranu ovom relacijom pa ta particija tvori blokovni sustav s obzirom na G. No kako K djeluje trivijalno na ovaj blokovni sustav, to je ova particija blokovni sustav s obzirom na G^{Σ}. Sada, kako je G^{Σ} primitivna grupa, slijedi da ili imamo d blokova imprimitivnosti kardinalnosti 1 ili jedan blok imprimitivnosti kardinalnosti d. U prvom slučaju za svaka dva različita $\Delta, \Delta' \in \Sigma$ vrijedi $\Delta \not\sim \Delta'$ tj. $N_{(\Delta)} \neq N_{(\Delta')}$. U drugom slučaju imamo da su svi $N_{(\Delta)}$ jednaki no onda iz $\bigcap_{\Delta\in\Sigma} G_{(\Delta)} = 1$ slijedi $\bigcap_{\Delta\in\Sigma} N_{(\Delta)} = 1$, a zbog jednakosti svih $N_{(\Delta)}$ imamo $N_{(\Delta)} = 1$. ■

Propozicija 5.34 *Za svaki $\Delta \in \Sigma$ vrijedi da je $O_p(K)^{\Delta} \cong F_p^{\alpha}$ i postoji $\beta \geq \alpha$ takav da je $O_p(K) \cong F_p^{\beta}$. Također, $O_p(K) \trianglelefteq G$ i $C_G(O_p(K)) \cap K = O_p(K)$.*

Dokaz. Iz $O_p(K)$ *char* $K \trianglelefteq G$ slijedi da je $O_p(K) \trianglelefteq G$ i $O_p(K)^\Delta \trianglelefteq (G_\Delta)^\Delta$ pa je $O_p(K)^\Delta \leq O_p((G_\Delta)^\Delta) = T(\Delta)$ za svaki $\Delta \in \Sigma$ i $O_p(K)^\Delta = T(\Delta) \cong F_p^\alpha$ (vidi [16]). Budući da je $O_p(K) \leq \prod_{\Delta \in \Sigma} T(\Delta)$, a iz definicije od $O_p(K)$ slijedi $O_p(K) = G \cap \prod_{\Delta \in \Sigma} T(\Delta)$ i $O_p(K)$ je elementarna abelova p-grupa dakle postoji $\beta \geq \alpha$ takav da je $O_p(K) \cong F_p^\beta$.

Budući da je $O_p(K)$ abelova grupa vrijedi da je $O_p(K) \leq C_G(O_p(K)) \cap K$. Neka je sada $x \in C_G(O_p(K)) \cap K$. Tada je $xs = sx$ za svaki $s \in O_p(K)$. Sada je $\varphi_\Delta(x)\varphi_\Delta(s) = \varphi_\Delta(s)\varphi_\Delta(x)$ pa je $\varphi_\Delta(x) \in C_{(G_\Delta)^\Delta}(O_p(K)^\Delta) = O_p(K)^\Delta$ pa je $x \in O_p(K)$ (u teoriji primitivnih grupa se pokaže da je $C_{(G_\Delta)^\Delta}(T(\Delta)) = T(\Delta)$, vidi [10]). ■

Propozicija 5.35 *Ako je $O_p(K)_{(\Delta)} \neq 1$ za neki $\Delta \in \Sigma$, onda je $C_G(O_p(K)) = O_p(K)$.*

Dokaz. Pretpostavimo da je $C_G(O_p(K)) \neq O_p(K)$. Onda po Propoziciji 5.34 postoji element x iz $C_G(O_p(K))$ koji nije u K. Kako je centralizator normalne podgrupe normalna podgrupa, to je $C_G(O_p(K))K/K$ netrivijalna normalna podgrupa od G^Σ pa djeluje tranzitivno na Σ. Onda i $C_G(O_p(K))$ djeluje tranzitivno na Σ. To znači da za Δ i Δ' iz Σ postoji $g \in C_G(O_p(K))$ takav da je $g\Delta = \Delta'$. Po Propoziciji 5.33 vrijedi $O_p(K)_{(\Delta)} = gO_p(K)_{(\Delta)}g^{-1} = O_p(K)_{(g\Delta)} = O_p(K)_{(\Delta')}$ pa su svi $O_p(K)_{(\Delta)} = 1$, što je u kontradikciji s početnom pretpostavkom. Dakle, $C_G(O_p(K)) = O_p(K)$. ■

Za dokazivanje Propozicije 5.37 koristit ćemo sljedeći poznat rezultat iz teorije simetričnih dizajna dan u [9]:

Teorem 5.36 *Ako je f broj fiksnih točaka netrivijalnog automorfizma simetričnog (v, k, λ) dizajna, onda je $f \leq k + \sqrt{k - \lambda}$.*

Propozicija 5.37 *Ako je* $k+\sqrt{k-\lambda}<2c$, *onda je* $K_{(\Delta)}\cap K_{(\Delta')}=1$ *za sve različite blokove imprimitivnosti* $\Delta,\Delta'\in\Sigma$ *te* $|K|\leq\left|K^{\Delta}\right|^2$ *i* $|O_p(K)|\leq c^2$.

Dokaz. Neka su Δ i Δ' različiti elementi iz Σ. Ako je $K_{(\Delta)}\cap K_{(\Delta')}$ netrivijalan, onda postoji nejedinični element u G koji ima barem $2c$ fiksnih točaka što je u kontradikciji s brojem fiksnih točaka netrivijalnog automorfizma simetričnog dizajna pa mora biti $K_{(\Delta)}\cap K_{(\Delta')}=1$. Kako je $K_{(\Delta)}K_{(\Delta')}\subseteq K$, a iz Propozicije 5.33 vrijedi da $\left|K_{(\Delta)}\right|$ ne ovisi o izboru Δ, to imamo

$$|K|\geq\left|K_{(\Delta)}K_{(\Delta')}\right|=\left|K_{(\Delta)}\right|\left|K_{(\Delta')}\right|=\left|K_{(\Delta)}\right|^2=\frac{|K|^2}{\left|K^{\Delta}\right|^2},$$

tj. $|K|\leq\left|K^{\Delta}\right|^2$. Analogno dobijemo i $|O_p(K)|\leq\left|O_p(K)^{\Delta}\right|^2$, a kako je $\left|O_p(K)^{\Delta}\right|=|T(\Delta)|=\left|F_p^{\alpha}\right|=p^{\alpha}=c$, imamo traženi rezultat. ■

Napomena 5.38 *Primijetimo da je uvjet* $k+\sqrt{k-\lambda}<2c$ *ispunjen u tri od preostala četiri slučaja: 6, 10 i 15. Za te slučajeve nam Propozicija 5.37 pri konstrukciji potencijalnog dizajna daje ogradu za redove grupa* K *i* $O_p(K)$.

Propozicija 5.39 *Neka je* $\Delta\in\Sigma$, $Y_1\leq F_p^*$ *i* $K^{\Delta}=T(\Delta)\rtimes Y$, *pri čemu je* $Y=\{yI\mid y\in Y_1\}\cong Y_1$. *Tada vrijedi:*

i) Grupa K *je izomorfna podgrupi od* $\left(\prod_{i=1}^{d}T(\Delta_i)\right)\rtimes Y^d$, *i* $O_p(K)$ *je izomorfna podgrupi od* $\prod_{i=1}^{d}T(\Delta_i)$.

ii) Postoji $K_0\leq K$ *takva da je* $K=O_p(K)\rtimes K_0$, *i* K_0 *je izomorfna podgrupi od* Y^d.

iii) Ako je $O_p(K)_{(\Delta_i)}\cap O_p(K)_{(\Delta_j)}$ *trivijalna grupa za sve različite* $\Delta_i,\Delta_j\in\Sigma$ *i* $|Y|<d$, *onda je* $K_0\cong Y$.

Dokaz. i) Budući da je $K\trianglelefteq G$ djelovanja od K na svim $\Delta\in\Sigma$ su izomorfna pa slijedi prvi dio tvrdnje. Kako je $O_p(K)=G\cap\prod_{i=1}^{d}T(\Delta)\leq\prod_{i=1}^{d}T(\Delta_i)$, slijedi druga tvrdnja.

ii) Neka je $N = \left(\prod_{i=1}^{d} T(\Delta_i)\right) \rtimes Y^d$. Budući da je $\prod_{i=1}^{d} T(\Delta_i) \trianglelefteq N$ rješiva i $N / \prod_{i=1}^{d} T(\Delta_i) \cong Y^d$ rješiva slijedi da je N rješiva grupa. K je podgrupa rješive grupe pa je i sama rješiva. Kako je $Y_1 \leq F_p^*$ i $\left|F_p^*\right| = p-1$, slijedi da $p \nmid |Y|^d$ pa je $\prod_{i=1}^{d} T(\Delta_i)$ p-Sylowljeva podgrupa grupe N. Budući da je $O_p(K) \leq \prod_{i=1}^{d} T(\Delta_i)$ slijedi da je $O_p(K)$ p-Sylowljeva podgrupa grupe K. Kako je K rješiva podgrupa, po Propoziciji 1.13 postoji p'-Hallova podgrupa K_0 te vrijedi $K = O_p(K) \rtimes K_0$.

iii) Neka je $s \in O_p(K)_{(\Delta_i)}$. To znači da je $s_i = 0$ pa iz trivijalnosti od $O_p(K)_{(\Delta_i)} \cap O_p(K)_{(\Delta_j)}$ slijedi da za svaki $s \in O_p(K)$ za koje je $s_i = s_j = 0$, za neke $i \neq j$, vrijedi da su svi $s_i = 0$. Iz $|Y| < d$ slijedi da za svaki $A = (a_1 I, ..., a_d I) \in K_0$, pri čemu su $a_i \in Y_1$, postoje različiti i, j takvi da je $a_i = a_j$. Sada uočimo da za svaki $s \in O_p(K)$ vrijedi:

$$\begin{aligned}(0,A)(s,I)(0,A)^{-1}(s,I)^{-a_i} &= (As,A)(0,A^{-1})(-a_i s, I)\\ &= (As,I)(-a_i s,I)\\ &= (As - a_i s, I).\end{aligned}$$

Kako je $s \in O_p(K) \trianglelefteq K$, to je $As - a_i s$ element iz $O_p(K)$ kojemu su i-ta i j-ta koordinata jednake 0 pa su mu sve koordinate jednake 0, tj. $As = a_i s$. Sada je $a_1 = a_2 = ... = a_d$ pa je svaki $A \in K_0$ oblika $(a_1 I, ..., a_1 I)$ tj. $K_0 \cong Y$.

■

Propozicija 5.40 *Ne postoje (v,k,λ) simetrični dizajni tranzitivni po incidencijama imprimitivni po točkama s parametrima iz retka 6 Tablice 1.*

Dokaz. Prvo navedimo sve moguće kombinacije grupa $(G_\Delta)^\Delta$, K^Δ i G^Σ za slučaj 6.

$(G_\Delta)^\Delta$	K^Δ	G^Σ
$pr(25,13)$	$(100,11)$	$pr(7,4)$
$pr(25,14)$	$(100,11)$	$pr(7,5)$
$pr(25,19)$	$(100,11)$	$pr(7,5)$

Kako je G tranzitivna po incidencijama, mora vrijediti $vk \mid |G|$. Kako je $vk = 2 \cdot 3 \cdot 5^3 \cdot 7$ i $|G| = \left|G^\Sigma\right| |K|$, mora vrijediti $5^3 \mid \left|G^\Sigma\right| |K|$. S obzirom da su jedine moguće grupe G^Σ pr(7,4) i pr(7,5) redova 42 i 168 redom, vidimo da $5 \nmid \left|G^\Sigma\right|$ pa mora vrijediti $5^3 \mid |K|$.

Pokazuje se (u MAGMI) da je $K^\Delta = T(\Delta) \rtimes \langle 2I \rangle$ pa iz Propozicije 5.39 slijedi $K = O_5(K) \rtimes \langle 2I \rangle$.

U grupi G postoji element x reda 7 koji nije element iz $O_5(K)$. Neka je grupa $H = O_5(K)\langle x \rangle$. Grupa $\langle x \rangle$ je 7-Sylowljeva podgrupa od H. Broj 7-Sylovljevih podgrupa syl_7 dijeli red od $O_5(K)$ te je $syl_7 \equiv 1 (\mathrm{mod}\, 7)$. Kako je zbog Propozicije 5.37 $|O_5(K)| \leq 25^2$, slijedi da je $syl_7 = 1$. Sve Sylowljeve podgrupe od H su normalne pa element x komutira s $O_5(K)$ po elementima. Sada je $x \in C_G(O_5(K)) \neq O_5(K)$ pa po Propoziciji 5.35 vrijedi da je $O_5(K)_{(\Delta)} = 1$, odnosno $O_5(K)^\Delta \cong O_5(K) / O_5(K)_{(\Delta)} \cong O_5(K)$. Sada je $|O_5(K)| = 25$ pa vidimo da $|K| = |O_5(K)| |\langle 2I \rangle| = 100$ što je u kontradikciji s $5^3 \mid |K|$. ■

Propozicija 5.41 *Ne postoje (v,k,λ) simetrični dizajni tranzitivni po incidencijama i imprimitivni po točkama s parametrima iz retka 10 Tablice 1.*

Dokaz. Prvo navedimo sve moguće kombinacije grupa $(G_\Delta)^\Delta$, K^Δ i G^Σ za slučaj 10.

$(G_\Delta)^\Delta$	K^Δ	G^Σ
$pr(49,9)$	$(98,4)$	$pr(9,5)$
$pr(49,10)$	$(98,4)$	$pr(9,2)$
$pr(49,22)$	$(98,4)$	$pr(9,7)$
$pr(49,23)$	$(294,13)$	$pr(9,5)$
$pr(49,24)$	$(294,13)$	$pr(9,2)$
$pr(49,29)$	$(294,13)$	$pr(9,7)$

Kako je G tranzitivna po incidencijama, mora vrijediti $vk \mid |G|$. Kako je $vk = 2^3 \cdot 3^2 \cdot 7^3$ i $|G| = \left|G^\Sigma\right| |K|$, mora vrijediti $7^3 \mid \left|G^\Sigma\right| |K|$. S obzirom da su jedine moguće grupe G^Σ pr(9,2), pr(9,5) i pr(9,7) redova 72, 144 i 432 redom, vidimo da $7 \nmid \left|G^\Sigma\right|$ pa mora vrijediti $7^3 \mid |K|$.

Pokazuje se (u MAGMI) da je za $K^\Delta = (98,4) = T(\Delta) \rtimes \langle 6I \rangle$, a za $K^\Delta = (294,13) = T(\Delta) \rtimes \langle 3I \rangle$ pa iz Propozicije 5.39 slijedi $K = O_7(K) \rtimes \langle aI \rangle$ pri čemu je $a \in \{3,6\}$ tj. K_0 je ciklička grupa reda 6 ili 2.

Kako je zbog Propozicije 5.37 $|O_7(K)| \leq 49^2$, slijedi da je $|O_7(K)| = 7^\beta$, pri čemu je $\beta \in \{3,4\}$. Također, jer je $|O_7(K)| \neq 49 = \left|O_7(K)^\Delta\right|$, onda je $O_7(K)_{(\Delta)} \neq 1$ pa vrijedi $C_G(O_7(K)) = O_7(K)$.

Po Propoziciji 5.39 ii) vrijedi $K_0 \cong K/O_p(K)$, a kako imamo

$$(G/O_p(K))/(K/O_p(K)) \cong G/K \cong G^\Sigma,$$

to je $G/O_p(K)$ proširenje $K_0.G^\Sigma$.

Sada u MAGMI potražimo proširenja $K_0.G^\Sigma$ za slučaj $K_0 = C_2$ i $G^\Sigma = pr(9,2)$. Za ta proširenja se pokaže da je presjek svih jezgri ireducibilnih linearnih reprezentacija stupnja manjeg ili jednakog $\beta = 4$ kardinalnosti 9. Pritom primijetimo da je $C_2 \leq C_6$ i $pr(9,2) \leq pr(9,5) \leq pr(9,7)$ pa su proširenja $C_2.pr(9,2)$ podgrupe proširenja $K_0.G^\Sigma$ za sve izbore K_0 i G^Σ pa je i njihov presjek svih jezgri ireducibilnih linearnih reprezentacija stupnja manjeg ili jednakog $\beta = 4$ kardinalnosti djeljive sa 9. To znači da u svakom slučaju prema Napomeni 1.45 mora vrijediti $9 \mid |C_G(O_7(K))| = |O_7(K)|$, što je kontradikcija jer je $O_7(K)$ 7-grupa. ■

Sva prethodna analiza iz ovog poglavlja dovodi nas do sljedećeg glavnog rezultata:

Teorem 5.42 *Neka je* $\lambda \leq 10$. *Postoji točno osam do na izomorfizam netrivijalnih simetričnih* (v, k, λ) - *dizajna* D *za koje je* (v, k, λ) *različit od* $(288, 42, 6)$ *i* $(891, 90, 9)$ *te za koje postoji grupa automorfizama* G *takva da je dizajn* D G*-tranzitivan po incidencijama i* G*-imprimitivan po točkama. Posebno, postoje takva*

dva (16,6,2) dizajna,

jedan (45,12,3) dizajn,

jedan (15,8,4) dizajn i

četiri (96,20,4) dizajna.

Dokaz. Teorem 5.6 nam daje moguće petorke parametara (v, k, λ, c, μ) takvih dizajna. Eliminacijske Propozicije 5.13, 5.14, 5.19, 5.28, 5.31, 5.40 i 5.41 i uvjet teorema $(v, k, \lambda) \notin \{(288, 42, 6), (891, 90, 9)\}$ nam eliminiraju sve osim prvih pet petorki parametara. Napomene 5.8, 5.9, 5.10 i 5.11 opisuju broj dizajna s parametrima iz prvih pet redaka. ■

Poglavlje 6

Dodatak

6.1 Algoritmi

U ovom dijelu dat ćemo neke algoritme koje smo koristili pri konstrukciji dizajna odnosno pokazivanju njihove neegzistencije. Kako su glavni fokus ovog rada dizajni tranzitivni po incidencijama, prvi od njih je algoritam koji za dani G i B provjerava je li incidencijska struktura $D = (P, \mathcal{B})$ dizajn tranzitivan po incidencijama, pri čemu je $G \leq Sym(P)$, a $\mathcal{B} = GB$.

Algoritam 6.1 *FTD:=function(G,B);*

p:=Representative(B);

orb:={Set(x):x in Orbits(Stabiliser(G,p))};

orb:={x:x in orb|x ne {p}};

k:=#B; v:=Degree(G);

ftd:=false;

if (#Orbit(Stabiliser(G,B),p) eq k) and (forall(u) {x:x in orb|#(B meet x) eq ((k-1)#x)/(v-1)}) then ftd:=true;*

end if;

return ftd;

end function;

Sljedeće ćemo dati pomoćni algoritam koji će nam listu dizajna filtrirati na način da ukloni dizajne koji su međusobno izomorfni.

Algoritam 6.2 *IZO:=function(lista_ dizajna);*

```
dizajni:=[];
izo_ dizajni:=[];
for x in lista_ dizajna do
    if x notin izo_ dizajni then
    dizajni:=dizajni cat [x];
    izo_ dizajni:=izo_ dizajni cat [y:y in lista_ dizajna|IsIsomorphic(x,y)];
    end if;
end for;
return dizajni;
end function;
```

Sada ćemo dati algoritam koji smo koristili pri konstrukciji svih primitivnih dizajna s v točaka. Sama konstrukcija algoritma je detaljno opisana u 4. poglavlju. Primijetimo da brojač i broji do $n-2$ jer su zadnje dvije grupe u MAGMINOJ biblioteci uvijek A_v i S_v, a takve nam daju trivijalne dizajne.

Algoritam 6.3 *PFTD:=function(v);*

```
lista:=[];
n:=NumberOfPrimitiveGroups(v);
for i in {1..n-2} do
    G:=PrimitiveGroup(v,i);
```

```
        S:=Stabiliser(G,1);
        orb:=[#x:x in Orbits(S)|#x ne 1];
        kk:={k:k in [3..v-3]|forall(u){x:x in orb|IsIntegral((k-1)*x/(v-1))}};
        kk:=[x:x in kk|#G mod x eq 0];
        for k in kk do
            bb:={x:x in [2..#G-1]|#G mod x eq 0};
            bb:={x:x in bb|IsIntegral(k*x/v)};
            bb:={x:x in bb|IsIntegral(((k-1)*k*x)/((v-1)*v))};
            bb:=[x:x in bb|x lt Binomial(v,k)];
            redGB:=[Floor(#G/x):x in bb];
            for i in {1..#redGB} do
                GB:=[x`subgroup:x in Subgroups(G:OrderEqual:=redGB[i])];
                for s in GB do
                    orbs:=[Set(x):x in Orbits(s)|#x eq k];
                    orbs:=[x:x in orbs|FTD(G,x)];
                    for o in orbs do
                        lista:=lista cat [IncidenceStructure<v|Orbit(G,o)>];
                    end for;
                end for;
            end for;
        end for;
    end for;
    return IZO(lista);
    end function;
```

Algoritam 6.3 nije pogodan za $v > 30$ pa ćemo dati i algoritam koji također traži dizajne tranzitivne po incidencijama s v točaka, ali za točno određeni k i b. Ovo preciziranje parametara k i b nam daje mogućnost za traženje dizajna s nešto većim parametrima v. Također, kao i u Algoritmu 6.3 ne tražimo dizajne s grupom automorfizama A_v ili S_v jer za takve znamo da su trivijalni.

Algoritam 6.4 *PFTD:=function(v,k,b);*

```
lista:=[];
n:=NumberOfPrimitiveGroups(v);
for i in {1..n-2} do
    G:=PrimitiveGroup(v,i);
    if (#G mod b eq 0) then
        GB:=Subgroups(G:OrderEqual:=Floor(#G/b));
        GB:=[x‘subgroup:x in GB];
        for s in GB do
            orbs:=[Set(x):x in Orbits(s)|#x eq k];
            orbs:=[x:x in orbs|FTD(G,x)];
            for o in orbs do
                lista:=lista cat [IncidenceStructure<v|Orbit(G,o)>];
            end for;
        end for;
    end if;
end for;
return IZO(lista);
end function;
```

Sada navedimo algoritam za traženje simetričnih po točkama imprimitivnih dizajna tranzitivnih po incidencijama kojima je jezgra djelovanja na sustav imprimitivnosti trivijalna.

Algoritam 6.5 *SVFTD:=function(d,c,k);*

```
Gsigma:=[PrimitiveGroup(d,x):x in [1..NumberOfPrimitiveGroups(d)]];
lista:=[];
for G in Gsigma do
    Gdelta:=Stabilizer(G,1);
    MS:=[x`subgroup:x in MaximalSubgroups(Gdelta)|#Gdelta/#x eq c];
    for mms in MS do
        gg:=CosetImage(G,mms);
        GB:=[x`subgroup:x in Subgroups(gg:OrderEqual:=#mms)];
        for ba in [1..#GB] do
            orb:={Set(x): x in Orbits(GB[ba])|#x eq k};
            orb:=[x:x in orb|FTD(gg,x)];
            lista:=lista cat [IncidenceStructure< GSet(gg) |Orbit(gg,x)>:x in orb];
        end for;
    end for;
end for;
return IZO(D);
end function;
```

6.2 Primitivni dizajni tranzitivni po incidencijama za $v \leq 30$

Popis parametara svih 2-(v, k, λ) dizajna tranzitivnih po incidencijama i primitivnih po točkama za koje je $\lambda \leq 30$ dan je u Tablici 10. Uz parametre dizajna navedena je i njihova puna grupa automorfizama G.

Tablica 10

	(v,k,λ)	G		(v,k,λ)	G
$v=6$	$(6,3,2)$	$PSL(2,5)$		$(10,4,4)$	$P\Gamma L(2,9)$
$v=7$	$(7,3,1)$	$L(3,2)$		$(10,4,24)$	$P\Gamma L(2,9)$
	$(7,3,2)$	$AGL(1,7)$		$(10,5,8)$	$M(10)$
	$(7,3,4)$	$L(3,2)$		$(10,5,16)$	$P\Gamma L(2,9)$
	$(7,4,2)$	$L(3,2)$		$(10,6,5)$	$S(6)$
$v=8$	$(8,4,3)$	$ASL(3,2)$		$(10,6,10)$	$P\Gamma L(2,9)$
	$(8,4,6)$	$PGL(2,7)$	$v=11$	$(11,3,3)$	$L(2,11)$
	$(8,4,9)$	$PGL(2,7)$		$(11,3,6)$	$L(2,11)$
	$(8,4,12)$	$ASL(3,2)$		$(11,4,6)$	$L(2,11)$
$v=9$	$(9,3,1)$	$AGL(2,3)$		$(11,5,2)$	$L(2,11)$
	$(9,3,6)$	$AGL(2,3)$		$(11,5,4)$	$AGL(1,11)$
	$(9,4,3)$	$A\Gamma L(1,9)$		$(11,5,12)$	$L(2,11)$
	$(9,4,6)$	$A\Gamma L(1,9)$		$(11,5,12)$	$M(11)$
	$(9,4,9)$	$AGL(2,3)$		$(11,5,72)$	$M(11)$
	$(9,6,5)$	$AGL(2,3)$		$(11,6,3)$	$L(2,11)$
$v=10$	$(10,3,4)$	$S(6)$		$(11,6,15)$	$L(2,11)$
	$(10,4,2)$	$S(6)$		$(11,6,18)$	$M(11)$

	(v,k,λ)	G		(v,k,λ)	G
$v=12$	$(12,4,15)$	$PGL(2,11)$	$v=14$	$(14,3,6)$	$PSL(2,13)$
	$(12,4,15)$	$M(11)$		$(14,4,6)$	$PSL(2,13)$
	$(12,4,30)$	$PGL(2,11)$		$(14,4,12)$	$PGL(2,13)$
	$(12,4,30)$	$M(11)$		$(14,4,18)$	$PGL(2,13)$
	$(12,5,20)$	$PGL(2,11)$		$(14,4,36)$	$PGL(2,13)$
	$(12,5,20)$	$M(11)$		$(14,6,15)$	$PSL(2,13)$
	$(12,6,5)$	$M(11)$		$(14,6,15)$	$PGL(2,13)$
	$(12,6,25)$	$PSL(2,11)$		$(14,6,30)$	$PGL(2,13)$
	$(12,6,25)$	$PGL(2,11)$		$(14,7,18)$	$PSL(2,13)$
	$(12,6,25)$	$M(11)$		$(14,7,36)$	$PGL(2,13)$
	$(12,6,30)$	$M(12)$		$(14,8,28)$	$PGL(2,13)$
	$(12,6,50)$	$PGL(2,11)$	$v=15$	$(15,3,1)$	$PSL(4,2)$
	$(12,6,180)$	$M(12)$		$(15,3,12)$	$PSL(4,2)$
	$(12,8,70)$	$PGL(2,11)$		$(15,4,6)$	$PSL(4,2)$
	$(12,8,70)$	$M(11)$		$(15,4,12)$	$A(7)$
$v=13$	$(13,3,2)$	$AGL(1,13)$		$(15,4,36)$	$A(7)$
	$(13,3,2)$	$L(3,3)$		$(15,4,48)$	$PSL(4,2)$
	$(13,3,9)$	$L(3,3)$		$(15,5,4)$	$A(7)$
	$(13,4,1)$	$L(3,3)$		$(15,5,12)$	$A(7)$
	$(13,4,3)$	$AGL(1,13)$		$(15,5,16)$	$PSL(4,2)$
	$(13,4,18)$	$L(3,3)$		$(15,6,10)$	$A(7)$
	$(13,6,5)$	$AGL(1,13)$		$(15,6,15)$	$PSL(4,2)$
	$(13,6,15)$	$L(3,3)$		$(15,6,30)$	$A(7)$
	$(13,6,45)$	$L(3,3)$		$(15,6,40)$	$PSL(4,2)$
	$(13,8,42)$	$L(3,3)$		$(15,6,60)$	$PSL(4,2)$
	$(13,9,6)$	$L(3,3)$		$(15,7,3)$	$PSL(4,2)$

	(v,k,λ)	G		(v,k,λ)	G
	$(15,7,24)$	$PSL(4,2)$		$(16,5,16)$	$ASL(2,4):2$
	$(15,8,4)$	$PSL(4,2)$		$(16,5,24)$	$A\Gamma L(2,4)$
	$(15,9,24)$	$A(7)$		$(16,5,48)$	$2^4.A(6)$
	$(15,9,96)$	$PSL(4,2)$		$(16,5,56)$	$2^4.A(7)$
	$(15,10,18)$	$A(7)$		$(16,5,96)$	$2^4.S(6)$
	$(15,10,54)$	$A(7)$		$(16,5,168)$	$2^4.A(7)$
	$(15,10,72)$	$PSL(4,2)$		$(16,5,224)$	$2^4.PSL(4,2)$
	$(15,12,22)$	$PSL(4,2)$		$(16,6,2)$	$2^4.S(6)$
$v=16$	$(16,3,2)$	$A\Gamma L(2,4)$		$(16,6,4)$	$ASL(2,4):2$
	$(16,3,4)$	$ASL(2,4):2$		$(16,6,6)$	$A\Gamma L(2,4)$
	$(16,3,6)$	$2^4.S(6)$		$(16,6,10)$	$AGL(1,16):2$
	$(16,3,8)$	$2^4.S(6)$		$(16,6,10)$	$ASL(2,4):2$
	$(16,3,12)$	$A\Gamma L(2,4)$		$(16,6,12)$	$(S(4)xS(4)):2$
	$(16,4,1)$	$A\Gamma L(2,4)$		$(16,6,12)$	$2^4.A(6)$
	$(16,4,2)$	$ASL(2,4):2$		$(16,6,14)$	$2^4.A(7)$
	$(16,4,3)$	$2^4.S(6)$		$(16,6,15)$	$2^4.S(6)$
	$(16,4,3)$	$AGL(1,16):2$		$(16,6,20)$	$A\Gamma L(2,4)$
	$(16,4,4)$	$2^4.S(6)$		$(16,6,20)$	$ASL(2,4):2$
	$(16,4,6)$	$A\Gamma L(2,4)$		$(16,6,24)$	$2^4.S(6)$
	$(16,4,7)$	$2^4.PSL(4,2)$		$(16,6,30)$	$2^4.S(6)$
	$(16,4,12)$	$2^4.S(6)$		$(16,6,30)$	$A\Gamma L(2,4)$
	$(16,4,12)$	$A\Gamma L(1,16)$		$(16,6,42)$	$2^4.A(7)$
	$(16,4,36)$	$A\Gamma L(2,4)$		$(16,6,56)$	$2^4.PSL(4,2)$
	$(16,4,84)$	$2^4.PSL(4,2)$		$(16,6,60)$	$A\Gamma L(2,4)$
	$(16,5,4)$	$A\Gamma L(1,16)$		$(16,6,105)$	$2^4.PSL(4,2)$
	$(16,5,8)$	$2^4.S(6)$		$(16,7,42)$	$2^4.PSL(4,2)$

	(v,k,λ)	G		(v,k,λ)	G
	$(16,8,7)$	$2^4.PSL(4,2)$		$(17,5,5)$	$P\Gamma L(2,2^4)$
	$(16,8,28)$	$A\Gamma L(2,4)$		$(17,6,150)$	$P\Gamma L(2,2^4)$
	$(16,8,84)$	$2^4.S(6)$		$(17,6,75)$	$L(2,2^4):2$
	$(16,8,196)$	$2^4.PSL(4,2)$		$(17,8,7)$	$AGL(1,17)$
	$(16,9,48)$	$A\Gamma L(2,4)$		$(17,8,105)$	$P\Gamma L(2,2^4)$
	$(16,9,48)$	$2^4.S(6)$		$(17,8,420)$	$P\Gamma L(2,2^4)$
	$(16,9,336)$	$2^4.A(7)$		$(17,10,135)$	$P\Gamma L(2,2^4)$
	$(16,9,1344)$	$2^4.PSL(4,2)$		$(17,12,33)$	$P\Gamma L(2,2^4)$
	$(16,10,6)$	$2^4.S(6)$	$v=18$	$(18,3,8)$	$PSL(2,17)$
	$(16,10,12)$	$ASL(2,4):2$		$(18,4,12)$	$PSL(2,17)$
	$(16,10,18)$	$A\Gamma L(2,4)$		$(18,4,24)$	$PGL(2,17)$
	$(16,10,36)$	$2^4.A(6)$		$(18,4,48)$	$PGL(2,17)$
	$(16,10,42)$	$2^4.A(7)$		$(18,4,48)$	$PGL(2,17)$
	$(16,10,72)$	$2^4.S(6)$		$(18,6,10)$	$PSL(2,17)$
	$(16,10,126)$	$2^4.A(7)$		$(18,6,20)$	$PGL(2,17)$
	$(16,10,168)$	$2^4.PSL(4,2)$		$(18,6,40)$	$PGL(2,17)$
	$(16,12,11)$	$A\Gamma L(2,4)$		$(18,6,80)$	$PGL(2,17)$
	$(16,12,22)$	$ASL(2,4):2$		$(18,8,28)$	$PSL(2,17)$
	$(16,12,33)$	$2^4.S(6)$		$(18,8,56)$	$PGL(2,17)$
	$(16,12,44)$	$2^4.S(6)$		$(18,8,112)$	$PGL(2,17)$
	$(16,12,66)$	$A\Gamma L(2,4)$		$(18,9,32)$	$PSL(2,17)$
	$(16,12,77)$	$2^4.PSL(4,2)$		$(18,9,64)$	$PGL(2,17)$
$v=17$	$(17,4,3)$	$AGL(1,17)$		$(18,12,44)$	$PSL(2,17)$
	$(17,4,15)$	$P\Gamma L(2,2^4)$		$(18,12,88)$	$PGL(2,17)$
	$(17,4,45)$	$L(2,2^4):2$		$(18,12,176)$	$PGL(2,17)$
	$(17,4,90)$	$P\Gamma L(2,2^4)$	$v=19$	$(19,3,1)$	$19:9$

	(v,k,λ)	G		(v,k,λ)	G
	$(19,3,2)$	$AGL(1,19)$		$(21,4,48)$	$P\Sigma L(3,4)$
	$(19,6,5)$	$AGL(1,19)$		$(21,4,72)$	$P\Gamma L(3,4)$
	$(19,9,4)$	$19:9$		$(21,5,1)$	$P\Gamma L(3,4)$
	$(19,9,8)$	$AGL(1,19)$		$(21,5,12)$	$S(7)$
$v=20$	$(20,4,9)$	$PSL(2,19)$		$(21,5,16)$	$P\Sigma L(3,4)$
	$(20,4,18)$	$PGL(2,19)$		$(21,5,32)$	$P\Sigma L(3,4)$
	$(20,4,27)$	$PGL(2,19)$		$(21,5,48)$	$P\Gamma L(3,4)$
	$(20,4,54)$	$PGL(2,19)$		$(21,6,4)$	$P\Sigma L(3,4)$
	$(20,4,54)$	$PGL(2,19)$		$(21,6,8)$	$P\Sigma L(3,4)$
	$(20,5,36)$	$PGL(2,19)$		$(21,6,12)$	$P\Gamma L(3,4)$
	$(20,6,45)$	$PGL(2,19)$		$(21,6,60)$	$P\Sigma L(3,4)$
	$(20,6,45)$	$PSL(2,19)$		$(21,6,120)$	$P\Sigma L(3,4)$
	$(20,6,90)$	$PGL(2,19)$		$(21,6,180)$	$P\Gamma L(3,4)$
	$(20,6,90)$	$PGL(2,19)$		$(21,6,240)$	$P\Gamma L(3,4)$
	$(20,8,42)$	$PGL(2,19)$		$(21,7,12)$	$P\Sigma L(3,4)$
	$(20,8,126)$	$PGL(2,19)$		$(21,7,24)$	$P\Sigma L(3,4)$
	$(20,9,72)$	$PGL(2,19)$		$(21,7,36)$	$P\Gamma L(3,4)$
	$(20,10,81)$	$PGL(2,19)$		$(21,8,28)$	$P\Gamma L(3,4)$
	$(20,10,81)$	$PSL(2,19)$		$(21,8,336)$	$P\Gamma L(3,4)$
	$(20,10,162)$	$PGL(2,19)$		$(21,9,12)$	$S(7)$
	$(20,12,99)$	$PGL(2,19)$		$(21,9,48)$	$P\Gamma L(3,4)$
	$(20,12,198)$	$PGL(2,19)$		$(21,9,192)$	$P\Gamma L(3,4)$
$v=21$	$(21,3,3)$	$P\Gamma L(3,4)$		$(21,10,72)$	$P\Sigma L(3,4)$
	$(21,3,16)$	$P\Gamma L(3,4)$		$(21,10,144)$	$P\Sigma L(3,4)$
	$(21,4,3)$	$P\Gamma L(3,4)$		$(21,10,216)$	$P\Gamma L(3,4)$
	$(21,4,24)$	$P\Sigma L(3,4)$		$(21,12,66)$	$P\Gamma L(3,4)$

	(v,k,λ)	G		(v,k,λ)	G
	$(21,12,88)$	$P\Gamma L(3,4)$		$(22,9,960)$	$M(22):2$
	$(21,12,264)$	$P\Sigma L(3,4)$		$(22,10,120)$	$M(22):2$
	$(21,12,528)$	$P\Sigma L(3,4)$		$(22,10,1440)$	$M(22)$
	$(21,12,792)$	$P\Gamma L(3,4)$		$(22,10,2880)$	$M(22):2$
	$(21,14,52)$	$P\Sigma L(3,4)$		$(22,10,4320)$	$M(22):2$
	$(21,14,104)$	$P\Sigma L(3,4)$		$(22,11,160)$	$M(22)$
	$(21,14,156)$	$P\Gamma L(3,4)$		$(22,11,320)$	$M(22):2$
	$(21,15,28)$	$P\Sigma L(3,4)$		$(22,12,176)$	$M(22):2$
	$(21,15,56)$	$P\Sigma L(3,4)$		$(22,12,660)$	$M(22):2$
	$(21,15,84)$	$P\Gamma L(3,4)$		$(22,12,1760)$	$M(22):2$
	$(21,15,168)$	$P\Gamma L(3,4)$		$(22,14,130)$	$M(22):2$
	$(21,16,12)$	$P\Gamma L(3,4)$		$(22,14,1040)$	$M(22)$
$v=22$	$(22,4,30)$	$M(22):2$		$(22,14,2080)$	$M(22):2$
	$(22,4,160)$	$M(22):2$		$(22,15,80)$	$M(22)$
	$(22,5,20)$	$M(22):2$		$(22,15,160)$	$M(22):2$
	$(22,5,160)$	$M(22)$		$(22,15,560)$	$M(22):2$
	$(22,5,320)$	$M(22):2$		$(22,16,40)$	$M(22):2$
	$(22,6,5)$	$M(22):2$	$v=23$	$(23,5,210)$	$M(23)$
	$(22,6,80)$	$M(22)$		$(23,5,1120)$	$M(23)$
	$(22,6,160)$	$M(22):2$		$(23,6,105)$	$M(23)$
	$(22,6,600)$	$M(22):2$		$(23,6,840)$	$M(23)$
	$(22,7,16)$	$M(22)$		$(23,7,21)$	$M(23)$
	$(22,7,32)$	$M(22):2$		$(23,7,336)$	$M(23)$
	$(22,7,240)$	$M(22):2$		$(23,8,56)$	$M(23)$
	$(22,8,40)$	$M(22):2$		$(23,8,23520)$	$M(23)$
	$(22,8,3360)$	$M(22):2$		$(23,9,10080)$	$M(23)$

	(v,k,λ)	G		(v,k,λ)	G
	$(23,10,2520)$	$M(23)$		$(24,7,462)$	$M(24)$
	$(23,10,15120)$	$M(23)$		$(24,8,77)$	$PGL(2,23)$
	$(23,11,5)$	$23:11$		$(24,8,77)$	$M(24)$
	$(23,11,10)$	$AGL(1,23)$		$(24,8,154)$	$PGL(2,23)$
	$(23,11,280)$	$M(23)$		$(24,8,154)$	$PGL(2,23)$
	$(23,11,3360)$	$M(23)$		$(24,8,64680)$	$M(24)$
	$(23,12,336)$	$M(23)$		$(24,9,73920)$	$M(24)$
	$(23,12,4620)$	$M(23)$		$(24,10,27720)$	$M(24)$
	$(23,14,2730)$	$M(23)$		$(24,11,110)$	$PGL(2,23)$
	$(23,14,10920)$	$M(23)$		$(24,11,6160)$	$M(24)$
	$(23,15,210)$	$M(23)$		$(24,12,121)$	$PSL(2,23)$
	$(23,15,1680)$	$M(23)$		$(24,12,121)$	$PGL(2,23)$
	$(23,16,120)$	$M(23)$		$(24,12,121)$	$PSL(2,23)$
$v=24$	$(24,4,33)$	$PGL(2,23)$		$(24,12,242)$	$PGL(2,23)$
	$(24,4,33)$	$PSL(2,23)$		$(24,12,242)$	$PGL(2,23)$
	$(24,4,66)$	$PGL(2,23)$		$(24,12,616)$	$M(24)$
	$(24,4,66)$	$PGL(2,23)$		$(24,12,8470)$	$M(24)$
	$(24,4,66)$	$PGL(2,23)$		$(24,12,243936)$	$M(24)$
	$(24,6,55)$	$PGL(2,23)$		$(24,14,30030)$	$M(24)$
	$(24,6,55)$	$PSL(2,23)$		$(24,15,4620)$	$M(24)$
	$(24,6,55)$	$PSL(2,23)$		$(24,16,330)$	$PGL(2,23)$
	$(24,6,110)$	$PGL(2,23)$		$(24,16,330)$	$M(24)$
	$(24,6,110)$	$PGL(2,23)$		$(24,18,62832)$	$M(24)$
	$(24,6,110)$	$PGL(2,23)$	$v=25$	$(25,3,20)$	$AGL(2,5)$
	$(24,6,1155)$	$M(24)$		$(25,4,12)$	$(S(5)\times S(5)):2$
	$(24,6,6160)$	$M(24)$		$(25,4,18)$	$(S(5)\times S(5)):2$

	(v,k,λ)	G		(v,k,λ)	G
	$(25,4,30)$	$AGL(2,5)$		$(26,8,56)$	$P\Gamma L(2,25)$
	$(25,4,60)$	$AGL(2,5)$		$(26,8,84)$	$P\Gamma L(2,25)$
	$(25,6,50)$	$AGL(2,5)$		$(26,8,168)$	$P\Gamma L(2,25)$
	$(25,8,140)$	$AGL(2,5)$		$(26,8,336)$	$P\Gamma L(2,25)$
	$(25,10,90)$	$AGL(2,5)$		$(26,8,336)$	$P\Gamma L(2,25)$
	$(25,10,90)$	$AGL(2,5)$		$(26,10,108)$	$P\Sigma L(2,25)$
	$(25,12,55)$	$ASL(2,5):2$		$(26,10,216)$	$P\Gamma L(2,25)$
	$(25,12,110)$	$AGL(2,5)$		$(26,12,66)$	$P\Sigma L(2,25)$
	$(25,16,150)$	$AGL(2,5)$		$(26,12,66)$	$P\Sigma L(2,25)$
$v=26$	$(26,3,12)$	$P\Sigma L(2,25)$		$(26,12,132)$	$P\Gamma L(2,25)$
	$(26,4,12)$	$P\Sigma L(2,25)$		$(26,12,132)$	$P\Gamma L(2,25)$
	$(26,4,18)$	$P\Sigma L(2,25)$		$(26,12,264)$	$P\Gamma L(2,25)$
	$(26,4,24)$	$P\Gamma L(2,25)$		$(26,13,72)$	$P\Sigma L(2,25)$
	$(26,4,36)$	$P\Gamma L(2,25)$		$(26,13,144)$	$P\Gamma L(2,25)$
	$(26,4,72)$	$PGL(2,25)$		$(26,16,360)$	$P\Gamma L(2,25)$
	$(26,4,72)$	$P\Gamma L(2,25)$		$(26,20,38)$	$P\Sigma L(2,25)$
	$(26,4,144)$	$P\Gamma L(2,25)$		$(26,20,76)$	$P\Gamma L(2,25)$
	$(26,5,12)$	$P\Sigma L(2,25)$	$v=27$	$(27,3,1)$	$AGL(3,3)$
	$(26,5,24)$	$P\Gamma L(2,25)$		$(27,3,3)$	$3^3:13.3$
	$(26,6,3)$	$P\Sigma L(2,25)$		$(27,3,6)$	$A\Gamma L(1,27)$
	$(26,6,6)$	$P\Gamma L(2,25)$		$(27,3,24)$	$AGL(3,3)$
	$(26,6,60)$	$P\Sigma L(2,25)$		$(27,4,36)$	$AGL(3,3)$
	$(26,6,120)$	$PGL(2,25)$		$(27,4,216)$	$AGL(3,3)$
	$(26,6,120)$	$P\Gamma L(2,25)$		$(27,6,5)$	$AGL(1,27)$
	$(26,6,240)$	$P\Gamma L(2,25)$		$(27,6,5)$	$A\Gamma L(1,27)$
	$(26,8,28)$	$P\Sigma L(2,25)$		$(27,6,15)$	$A\Gamma L(1,27)$

	(v,k,λ)	G		(v,k,λ)	G
	$(27,6,15)$	$A\Gamma L(1,27)$		$(27,18,1836)$	$AGL(3,3)$
	$(27,6,15)$	$A\Gamma L(1,27)$		$(27,24,92)$	$AGL(3,3)$
	$(27,6,15)$	$A\Gamma L(1,27)$	$v=28$	$(28,3,2)$	$P\Gamma L(2,8)$
	$(27,6,20)$	$AGL(3,3)$		$(28,3,2)$	$P\Gamma L(2,8)$
	$(27,6,180)$	$AGL(3,3)$		$(28,3,2)$	$P\Gamma U(3,3)$
	$(27,6,270)$	$AGL(3,3)$		$(28,3,4)$	$P\Gamma L(2,8)$
	$(27,6,1080)$	$AGL(3,3)$		$(28,3,8)$	$P\Gamma U(3,3)$
	$(27,8,28)$	$AGL(3,3)$		$(28,3,10)$	$PSp(6,2)$
	$(27,8,504)$	$AGL(3,3)$		$(28,3,16)$	$PSp(6,2)$
	$(27,8,1512)$	$AGL(3,3)$		$(28,4,1)$	$P\Gamma L(2,8)$
	$(27,9,4)$	$AGL(3,3)$		$(28,4,1)$	$P\Gamma U(3,3)$
	$(27,9,12)$	$3^3:13.3$		$(28,4,4)$	$P\Gamma U(3,3)$
	$(27,9,24)$	$A\Gamma L(1,27)$		$(28,4,5)$	$PSp(6,2)$
	$(27,9,96)$	$AGL(3,3)$		$(28,4,13)$	$P\Gamma L(2,27)$
	$(27,9,216)$	$AGL(3,3)$		$(28,4,39)$	$PSL(2,27):3$
	$(27,9,432)$	$AGL(3,3)$		$(28,4,48)$	$P\Gamma U(3,3)$
	$(27,12,132)$	$AGL(3,3)$		$(28,4,78)$	$PGL(2,27)$
	$(27,12,792)$	$AGL(3,3)$		$(28,4,78)$	$P\Gamma L(2,27)$
	$(27,12,1188)$	$AGL(3,3)$		$(28,4,80)$	$PSp(6,2)$
	$(27,13,6)$	$3^3:13.3$		$(28,4,234)$	$P\Gamma L(2,27)$
	$(27,13,12)$	$A\Gamma L(1,27)$		$(28,5,160)$	$PSp(6,2)$
	$(27,13,864)$	$ASL(3,3)$		$(28,5,640)$	$PSp(6,2)$
	$(27,13,1728)$	$AGL(3,3)$		$(28,6,5)$	$P\Gamma L(2,8)$
	$(27,16,1080)$	$AGL(3,3)$		$(28,6,10)$	$P\Gamma L(2,8)$
	$(27,18,17)$	$AGL(3,3)$		$(28,6,10)$	$P\Gamma L(2,8)$
	$(27,18,918)$	$AGL(3,3)$		$(28,6,10)$	$P\Gamma L(2,8)$

	(v,k,λ)	G		(v,k,λ)	G
	$(28,6,10)$	$P\Gamma L(2,8)$		$(28,8,182)$	$PGL(2,27)$
	$(28,6,10)$	$P\Gamma L(2,8)$		$(28,8,546)$	$P\Gamma L(2,27)$
	$(28,6,20)$	$P\Gamma U(3,3)$		$(28,8,1680)$	$PSp(6,2)$
	$(28,6,40)$	$P\Gamma U(3,3)$		$(28,9,8)$	$P\Gamma L(2,8)$
	$(28,6,40)$	$PSp(6,2)$		$(28,9,8)$	$P\Gamma L(2,8)$
	$(28,6,40)$	$P\Gamma U(3,3)$		$(28,9,16)$	$P\Gamma L(2,8)$
	$(28,6,50)$	$PSp(6,2)$		$(28,9,32)$	$P\Gamma U(3,3)$
	$(28,6,80)$	$PSp(6,2)$		$(28,9,104)$	$P\Gamma L(2,27)$
	$(28,6,130)$	$PGL(2,27)$		$(28,9,312)$	$PSL(2,27):3$
	$(28,6,130)$	$P\Gamma L(2,27)$		$(28,9,320)$	$PSp(6,2)$
	$(28,6,195)$	$PSL(2,27):3$		$(28,9,624)$	$P\Gamma L(2,27)$
	$(28,6,200)$	$PSp(6,2)$		$(28,9,7680)$	$PSp(6,2)$
	$(28,6,390)$	$P\Gamma L(2,27)$		$(28,10,40)$	$PSp(6,2)$
	$(28,6,390)$	$P\Gamma L(2,27)$		$(28,10,45)$	$PSp(6,2)$
	$(28,6,390)$	$P\Gamma L(2,27)$		$(28,10,1440)$	$PSp(6,2)$
	$(28,6,480)$	$PSp(6,2)$		$(28,12,11)$	$PSp(6,2)$
	$(28,7,2)$	$P\Gamma L(2,8)$		$(28,12,11)$	$P\Gamma L(2,8)$
	$(28,7,6)$	$P\Gamma L(2,8)$		$(28,12,44)$	$P\Gamma U(3,3)$
	$(28,7,16)$	$PSp(6,2)$		$(28,12,88)$	$P\Gamma U(3,3)$
	$(28,7,48)$	$P\Gamma U(3,3)$		$(28,12,143)$	$PSL(2,27):3$
	$(28,7,78)$	$P\Gamma L(2,27)$		$(28,12,176)$	$P\Gamma U(3,3)$
	$(28,7,5760)$	$PSp(6,2)$		$(28,12,286)$	$P\Gamma L(2,27)$
	$(28,8,14)$	$P\Gamma U(3,3)$		$(28,12,660)$	$PSp(6,2)$
	$(28,8,56)$	$P\Gamma U(3,3)$		$(28,12,858)$	$P\Gamma L(2,27)$
	$(28,8,56)$	$P\Gamma U(3,3)$		$(28,12,858)$	$P\Gamma L(2,27)$
	$(28,8,70)$	$PSp(6,2)$		$(28,12,880)$	$PSp(6,2)$

	(v,k,λ)	G		(v,k,λ)	G
	$(28,12,2640)$	$PSp(6,2)$		$(30,5,28)$	$PSL(2,29)$
	$(28,13,156)$	$P\Gamma L(2,27)$		$(30,5,56)$	$PGL(2,29)$
	$(28,14,169)$	$P\Gamma L(2,27)$		$(30,6,35)$	$PGL(2,29)$
	$(28,14,169)$	$PSL(2,27):3$		$(30,6,70)$	$PSL(2,29)$
	$(28,14,338)$	$P\Gamma L(2,27)$		$(30,6,70)$	$PSL(2,29)$
	$(28,15,280)$	$PSp(6,2)$		$(30,6,70)$	$PGL(2,29)$
	$(28,15,560)$	$PSp(6,2)$		$(30,6,140)$	$PGL(2,29)$
	$(28,16,20)$	$PSp(6,2)$		$(30,6,140)$	$PGL(2,29)$
	$(28,18,34)$	$P\Gamma L(2,8)$		$(30,6,140)$	$PGL(2,29)$
	$(28,18,136)$	$PSp(6,2)$		$(30,7,42)$	$PSL(2,29)$
	$(28,18,442)$	$P\Gamma L(2,27)$		$(30,7,84)$	$PGL(2,29)$
	$(28,21,20)$	$P\Gamma L(2,8)$		$(30,8,196)$	$PGL(2,29)$
	$(28,21,160)$	$PSp(6,2)$		$(30,8,196)$	$PGL(2,29)$
	$(28,24,46)$	$P\Gamma U(3,3)$		$(30,8,196)$	$PGL(2,29)$
	$(28,24,230)$	$PSp(6,2)$		$(30,10,126)$	$PGL(2,29)$
	$(28,24,598)$	$P\Gamma L(2,27)$		$(30,10,126)$	$PSL(2,29)$
$v=29$	$(29,4,3)$	$AGL(1,29)$		$(30,10,252)$	$PGL(2,29)$
	$(29,7,6)$	$AGL(1,29)$		$(30,10,252)$	$PGL(2,29)$
	$(29,14,13)$	$AGL(1,29)$		$(30,12,154)$	$PSL(2,29)$
$v=30$	$(30,3,14)$	$PSL(2,29)$		$(30,12,308)$	$PGL(2,29)$
	$(30,4,42)$	$PSL(2,29)$		$(30,12,308)$	$PGL(2,29)$
	$(30,4,42)$	$PGL(2,29)$		$(30,12,308)$	$PGL(2,29)$
	$(30,4,84)$	$PGL(2,29)$		$(30,14,91)$	$PSL(2,29)$
	$(30,4,84)$	$PGL(2,29)$		$(30,14,182)$	$PGL(2,29)$
	$(30,4,84)$	$PGL(2,29)$		$(30,14,364)$	$PGL(2,29)$
	$(30,4,84)$	$PGL(2,29)$		$(30,15,98)$	$PSL(2,29)$

	(v,k,λ)	G		(v,k,λ)	G
	$(30,15,196)$	$PGL(2,29)$		$(30,24,644)$	$PGL(2,29)$
	$(30,20,532)$	$PGL(2,29)$			

Bibliografija

[1] Aschbacher, Michael. *Finite group theory.* Vol. 10. Cambridge University Press, 2000.

[2] Beth, Thomas, Dieter Jungnickel i Hanfried Lenz. *Design theory.* Vol. 69. Cambridge University Press, 1999.

[3] Bosma, Wieb, John Cannon i Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.

[4] Braić, Snježana, et al. "Primitive symmetric designs with up to 2500 points." *Journal of Combinatorial Designs* 19.6 (2011): 463-474.

[5] Cameron, Peter J. *Permutation groups.* Vol. 45. Cambridge University Press, 1999.

[6] Cameron, Peter J. i Jacobus Hendricus Van Lint. *Designs, graphs, codes, and their links.* Cambridge University Press, 1992.

[7] Cameron, Peter J. i Cheryl E. Praeger. "Block-transitive t-designs I: point-imprimitive designs." *Discrete mathematics* 118.1-3 (1993): 33-43.

[8] Camina, A. R. i P. H. Zieschang. "On the normal structure of flag transitive automorphism groups of 2-designs." *J. London Math. Soc.(2)* 41 (1990): 555-564.

[9] Colbourne, Charles i Jeffrey Dinitz, eds. *Handbook of combinatorial designs*. CRC press, 2007.

[10] Dixon, John D. i Brian Mortimer. *Permutation groups.* Vol. 163. Springer Science & Business Media, 1996.

[11] Hall, Marshall Jr. *The theory of groups.* New York (1959).

[12] Husain, Q. M. "On the Totality of the Solutions for the Symmetrial Incomplete Block Designs: λ= 2, k= 5 or 6." *Sankhyā: The Indian Journal of Statistics* (1945): 204-208.

[13] Kantor, William M. "2-transitive symmetric designs." *Transactions of the American Mathematical Society* 146 (1969): 1-28.

[14] Kantor, William M. "Automorphism groups of designs." *Mathematische Zeitschrift* 109.3 (1969): 246-252.

[15] Lander, Eric S. *Symmetric designs: an algebraic approach.* Vol. 74. Cambridge University Press, 1983.

[16] Law, Maska, Cheryl E. Praeger i Sven Reichard. "Flag-transitive symmetric 2-(96, 20, 4)-designs." *Journal of Combinatorial Theory, Series A* 116.5 (2009): 1009-1022.

[17] Praeger, Cheryl E. "The flag-transitive symmetric designs with 45 points, blocks of size 12, and 3 blocks on every point pair." *Designs, Codes and Cryptography* 44.1 (2007): 115-132.

[18] Praeger, Cheryl E. i Shenglin Zhou. "Imprimitive flag-transitive symmetric designs." *Journal of Combinatorial Theory, Series A* 113.7 (2006): 1381-1395.

[19] Regueiro, Eugenia O'Reilly. "On primitivity and reduction for flag-transitive symmetric designs." *Journal of Combinatorial Theory, Series A* 109.1 (2005): 135-148.

[20] Serre, Jean-Pierre. *Linear representations of finite groups.* Vol. 42. Springer Science & Business Media, 2012.

[21] Suzuki, Michio. *Group theory.* New York: Springer, 1986.

[22] Zieschang, Paul-Hermann. "Point regular normal subgroups of flag transitive automorphism groups of 2-designs." *Advances in mathematics* 121.1 (1996): 102-123.

Životopis

Aljoša Šubašić rođen je 10.11.1985. u Splitu gdje je 2004. godine završio Prirodoslovno - matematičku gimnaziju. Godine 2010. diplomirao je na Prirodoslovno - matematičkom fakultetu Sveučilišta u Splitu i stekao zvanje profesor matematike i informatike.

Od 2011./12. je doktorski student Sveučilišnog poslijediplomskog studija matematike Sveučilišta J.J. Strossmayera u Osijeku, Sveučilišta u Rijeci, Sveučilišta u Splitu i Sveučilišta u Zagrebu. Aktivan je član Seminara za diskretnu matematiku u Splitu. Od veljače 2011. zaposlen je kao asistent na Prirodoslovno - matematičkom fakultetu Sveučilišta u Splitu.

Kontakt

Aljoša Šubašić
Lovretska 2, 21000 Split
mobitel: 095/869-3135
mail: aljsub@pmfst.hr