UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

Načrti in Hadamardove matrike

(Designs and Hadamard Matrices)

Ime in priimek: Mateja Grižon
Študijski program: Matematika
Mentor: prof. dr. István Kovács
Somentor: doc. dr. Nino Bašić

Koper, september 2020

Ključna dokumentacijska informacija

Ime in PRIIMEK: Mateja GRIŽON

Naslov zaključne naloge: Načrti in Hadamardove matrike

Kraj: Koper

Leto: 2020

Število listov: 51 Število slik: 2 Število referenc: 14

Mentor: prof. dr. István Kovács

Somentor: doc. dr. Nino Bašić

Ključne besede: t-načrt, končna projektivna ravnina, Steinerjev sistem, incidenčna matrika, simetrični načrt, dual načrta, permutacijska grupa, avtomorfizem načrta, skrčitev načrta, razširitev načrta, Hadamardova matrika, Hadamardov načrt

Math. Subj. Class. (2020): 05B05, 51E05, 51E10, 05B20, 15B34, 20B05, 05E18

Izvleček:
Načrt s parametri t-(v, k, λ) je par $(X, \mathcal{B})$, tako da velja: X je množica moči v; $\mathcal{B}$ je družina k-podmnožic množice X; vsaka t-podmnožica množice X se pojavi v natanko λ elementih družine $\mathcal{B}$. Predstavimo potrebe pogoje za obstoj t-načrta in pokažemo, da so končne projektivne ravnine simetrični 2-načrti. Simetrični načrt ima enako število točk in blokov. Za simetrične načrte spoznamo dodatne potrebne pogoje za njihov obstoj. Pokažemo, da končne projektivne ravnine reda 6 ne obstajajo. Definiramo avtomorfizem načrta in dokažemo, da grupa avtomorfizmov načrta deluje zvesto na množici blokov $\mathcal{B}$. Pokažemo, da lahko s pomočjo t-tranzitivne grupe, kjer je $t \geq 2$, konstruiramo t-načrt. Hadamardove matrike so matrike s koeficienti iz $\{-1, 1\}$, katerih vrstice so ortogonalne. Normalizirana Hadamardova matrika ima v prvi vrstici in prvem stolpcu same enke. Pokažemo, da lahko iz normalizirane Hadamardove matrike reda $4\lambda+4$ dobimo simetrični načrt s parametri 2-$(4\lambda+3, 2\lambda+1, \lambda)$. Velja tudi obratno, iz vsakega takšnega načrta lahko dobimo normalizirano Hadamardovo matriko. Vse predstavljene koncepte ponazorimo s konkretnimi primeri.

Key document information

Name and SURNAME: Mateja GRIŽON

Title of final project paper: Designs and Hadamard matrices

Place: Koper

Year: 2020

Number of pages: 51 Number of figures: 2 Number of references: 14

Mentor: Prof. István Kovács, PhD

Co-Mentor: Assist. Prof. Nino Bašić, PhD

Keywords: t-design, finite projective plane, Steiner system, incidence matrix, symmetric design, dual design, permutation group, automorphism of a design, contraction of a design, extension of a design, Hadamard matrix, Hadamard design

Math. Subj. Class. (2020): 05B05, 51E05, 51E10, 05B20, 15B34, 20B05, 05E18

Abstract:
Design with parameters t-(v, k, λ) is a pair $(X, \mathcal{B})$, such that: X is a set of cardinality v; $\mathcal{B}$ is a family of k-subsets of X; each t-subset of X appears in exactly λ members of the family $\mathcal{B}$. We present required conditions for existence of a t-design and show that all finite projective planes are symmetric 2-designs. Symmetric designs have the same number of points and blocks. We present additional required conditions for existence of symmetric designs. We show that there are no finite projective planes of order 6. We define an automorphism of a design and prove that the automorphism group of a design acts faithfully on the set of blocks $\mathcal{B}$. We show that a t-transitive group, where $t \geq 2$, can be used to construct a t-design. Hadamard matrices are matrices with coefficients from $\{-1, 1\}$, such that their row vectors are othogonal. Normalised Hadamard matrix is the one that has only ones in the first row and in the first column. We show that a normalised Hadamard matrix of order $4\lambda + 4$ gives rise to a symmetric design with parameters 2-$(4\lambda + 3, 2\lambda + 1, \lambda)$. The converse also holds, each such design can be used to obtain a normalised Hadamard matrix. All of the above concepts are explained with concrete examples.

Zahvala

Zahvaljujem se mentorju prof. dr. Istvánu Kovácsu za pomoč pri izbiri teme, usmerjanje pri pisanju in razpoložljivost.

Zahvaljujem se somentorju doc. dr. Ninu Bašiću za vso podporo, pomoč, nasvete, potrpežljivost in vložen čas pri nastajanju zaključne naloge.

Brez vas mi ne bi uspelo zaključiti zaključne naloge. HVALA!

Prav tako se bi rada zahvalila vsem profesorjem fakultete, ki so prispevali, da sem pridobila nova znanja potrebna za zaključek študija.
Zahvalila se bi tudi vsem strokovnim delavce, ki so mi kakorkoli pomagali.

Zahvalila bi se rada vsem kolegom s fakultete, ki so mi kakorkoli pomagali in prijateljem, ki so me vedno spodbujali.

Posebna zahvala gre moji mami Ledi, tatiju Pavlu, sestri Martini, svaku Luku in seveda fantu Amletu, ki so verjeli vame in so me vse čas spodbujali in podpirali.

Zaključno nalogo bi rada posvetila staršem in nonotom (Edvinu, Neviji, Ani, Marjanu in Milanu).

Kazalo vsebine

Kazalo slik in grafikonov

Seznam kratic

tj. to je
npr. na primer
oz. oziroma
itd. in tako dalje

1 Uvod

V kombinatoriki pogosto proučujemo *incidenčne strukture*. Incidenčna struktura je par $(X, \mathcal{B})$, kjer je X končna množica, $\mathcal{B}$ pa družina podmnožic množice X. Elementom množice X običajno pravimo *točke*, elementom družine $\mathcal{B}$ pa *bloki*. Po navadi zahtevamo, da ima incidenčna struktura še neke dodatne lastnosti. Če npr. zahtevamo, da so vsi bloki moči 2, dobimo enostavne grafe. Blokom v tem primeru rečemo povezave. Če npr. zahtevamo, da je $|X| = |\mathcal{B}| = n$, da je vsak blok moči k in da je vsaka točka vsebovana v natanko k blokih, dobimo kombinatorične (n_k) konfiguracije.

V našem primeru zahtevamo, da so vsi bloki enake moči. Velikost bloka označimo s parametrom k. Poleg tega zahtevamo, da je naša struktura "regularna" v naslednjem smislu: vsaka t-podmnožica[1] množice X mora biti vsebovana v natanko λ blokih. Parameter v je moč množice X. Tako incidenčno strukturo $(X, \mathcal{B})$ imenujemo *načrt s parametri* t-(v, k, λ) oz. t-*načrt*.

Pri študiju t-načrtov (kot tudi pri študiju sorodnih kombinatoričnih struktur) se običajno ukvarjamo z naslednjimi vprašanji:

(1) Ali načrt s parametri t-(v, k, λ) sploh obstaja? Če načrt obstaja, ali ga znamo konstruirati?

(2) Če načrt s parametri t-(v, k, λ) obstaja, ali je edinstven? Torej, ali obstaja do izomorfizma natančno en sam tak načrt? Kaj sploh pomeni izomorfizem t-načrtov?

(3) Ali t-načrt lahko na nek način raširimo, tako da je dobljena struktura tudi t-načrt?

(4) Kaj lahko povemo o grupi avtomorfizmov načrta? Ali obstajajo načrti, ki imajo tranzitivno grupo avtomorfizmov?

Teh vprašanj je preveč, da bi se lahko vsem podrobno posvetili. V naslednjih nekaj odstavkih na kratko predstavimo, kaj bralca čaka v pričujočem delu. Naša glavna referenca je [1], v pomoč pa so nam tudi [3, 6, 7, 12].

V drugem poglavju se bomo srečali z definicijo načrta. Zapisali bomo izrek, ki govori o potrebnih pogojih za obstoj načrtov z določenimi parametri. Ogledamo si

[1] Množici moči n pravimo n-*množica*. Podobno, z izrazom n-*podmnožica* poimenujemo podmnožico moči n.

primer Steinerjevega načrta, tj. načrta s parametri t-(v, k, λ), kjer je $t \geq 2$ in $\lambda = 1$. Pokažemo, da so končne projektivne ravnine (kot je npr. Fanova ravnina) tudi načrti. Definiramo incidenčno matriko načrta, ki jo označimo z A, ter dokažemo nekatere njene lastnosti.

V tretjem poglavju definiramo simetrični t-(v, k, λ) načrt. Dokažemo, da je vsak simetrični načrt nujno 2-načrt. Pokažemo, da incidenčna matrika simetričnega načrta zadošča enačbi $A^TA = AA^T$. Predstavimo tudi dualni načrt $(X^*, \mathcal{B}^*)$ načrta $(X, \mathcal{B})$. Spoznamo naslednji izrek: Če simetrični 2-(v, k, λ) načrt, kjer je v sodo število, obstaja, potem je $k - \lambda$ popolni kvadrat. V primeru, ko je v liho število, velja naslednje: Če simetrični 2-(v, k, λ) načrt obstaja, potem imam enačba $x^2 = (k-\lambda)y^2 + (-1)^{\frac{1}{2}(v-1)}\lambda z^2$ celoštevilsko rešitev (x, y, z), pri čemer je vsaj ena spremenljivka neničelna. S pomočjo tega pokažemo, da končne projektivne ravnine reda 6 ne obstajajo.

V četrtem poglavju predstavimo pojme iz teorije permutacijskih grup, ki jih uporabljamo v petem poglavju.

Peto poglavje je namenjeno avtomorfizmom načrtov. Definiramo avtomorfizem načrta in dokažemo, da grupa avtomorfizmov načrta deluje zvesto na množici blokov $\mathcal{B}$. Pokažemo, da lahko s pomočjo t-tranzitivne grupe, kjer je $t \geq 2$, konstruiramo t-načrt.

V šestem poglavju poglavju predstavimo skrčitve in razširitve načrtov. Predstavimo potreben pogoj za obstoj razširitve D^+ nekega načrta D.

V sedmem poglavju definiramo Hadamardove matrike in si ogledamo nekaj lastnosti takih matrik. Pokažemo, kako lahko iz Hadamardove matrike dobimo incidenčno matriko simetričnega načrta. Za konec iz načrta s parametri 2-$(15, 7, 3)$ konstruiramo Hadamardovo matriko reda 16.

2 Načrti

V tem poglavju formalno definiramo t-načrte in si ogledamo nekaj primerov. Predstavimo potrebne pogoje za obstoj načrta z danimi parametri. Nato pokažemo, da so končne projektivne ravnine posebni primeri načrtov. Na koncu poglavja dokažemo nekatere lasnosti incidenčnih matrik načrtov, ki jih bomo potrebovali v nadaljevanju.

2.1 Definicija in osnovne lasnosti

Množici moči k pravimo k-množica. Podobno podmnožici moči k pravimo k-podmnožica.

Definicija 2.1. *Načrt s parametri* t-(v, k, λ) je par $(X, \mathcal{B})$, tako da velja:

1. X je množica moči v;
2. $\mathcal{B}$ je družina k-podmnožic množice X;
3. vsaka t-podmnožica množice X se pojavi v natanko λ elementih družine $\mathcal{B}$.

Elementom množice X pravimo točke. Elementom družine $\mathcal{B}$ pa bloki načrta. Parametri načrta so pozitivna cela števila in velja $v > k \geq t$. Ponavljajoči bloki niso dovoljeni.

Nekateri avtorji [11] v definiciji načrta dopuščajo $v \geq k$. Z našo definicijo ne izgubimo nič pomembnega. Edini načrt, pri katerem je $v = k$, je načrt z enim samim blokom, ki vsebuje vse točke. Tak k-$(k, k, 1)$ načrt je trivialen in za nas nezanimiv.

Primer 2.2. Naj bo $X = \{1, 2, 3, \ldots, 10, 11\}$ in naj bo

$$\begin{aligned}\mathcal{B} = \{&\{1,2,3,7,10\},\{1,2,6,9,11\},\{1,3,4,5,9\},\{1,4,6,7,8\},\\ &\{1,5,8,10,11\},\{2,3,4,8,11\},\{2,4,5,6,10\},\{2,5,7,8,9\},\\ &\{3,5,6,7,11\},\{3,6,8,9,10\},\{4,7,9,10,11\}\}.\end{aligned}$$

Opazimo, da je $v = 11$ in da vsak blok vsebuje pet točk, torej $k = 5$. Lahko se tudi prepričamo, da vsak par elementov množice X nastopa v natanko dveh blokih. Na primer par $\{5, 7\}$ nastopa v blokih $\{2, 5, 7, 8, 9\}$ in $\{3, 5, 6, 7, 11\}$. To pomeni, da je $(X, \mathcal{B})$ načrt s parametri 2-$(11, 5, 2)$ oz. 2-načrt.

Primer 2.3. Naj bo $X = \{1, 2, 3, \ldots, 8\}$ in naj bo

$$\mathcal{B} = \{\{1,2,3,4\},\{1,2,5,6\},\{1,2,7,8\},\{1,3,5,7\},\{1,3,6,8\},\{1,4,5,8\},\{1,4,6,7\},\\ \{2,3,5,8\},\{2,3,6,7\},\{2,4,5,7\},\{2,4,6,8\},\{3,4,5,6\},\{3,4,7,8\},\{5,6,7,8\}\}.$$

Podobno kot v prejšnjem primeru se lahko prepričamo, da je $(X, \mathcal{B})$ načrt s parametri 3-$(8, 4, 1)$.

Definicija 2.4. Naj bo X končna množica in $\binom{X}{t}$ družina vseh t-podmnožic množice X. Načrtu $(X, \binom{X}{t})$ pravimo *polni načrt*. Parametri tega načrta so t-$(v, t, 1)$.

Primer 2.5. Naj bo $X = \{1, 2, 3, 4, 5\}$ in $t = 3$. Potem je

$$\binom{X}{3} = \{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\},\\ \{1,4,5\},\{2,3,4\},\{2,3,5\},\{2,4,5\},\{3,4,5\}\}.$$

$(X, \binom{X}{3})$ je polni načrt s parametri 3-$(5, 3, 1)$.

Izrek 2.6. *Naj bo $(X, \mathcal{B})$ t-načrt s parametri t-(v, k, λ). Potem je $(X, \mathcal{B})$ tudi s-načrt za vse $s = 1, 2, \ldots, t$. Kot s-načrt ima parametre s-(v, k, λ_s), pri čemer velja*

$$\lambda_s = \lambda \cdot \frac{(v-s)(v-s-1)\ldots(v-t+1)}{(k-s)(k-s-1)\ldots(k-t+1)}. \tag{2.1}$$

Primer 2.7. Po izreku 2.6 sledi, da je 2-$(11, 5, 2)$ načrt iz primera 2.2 tudi 1-$(11, 5, 5)$ načrt. Vrednost $\lambda_s = 5$ smo izračunali po enačbi (2.1).

Dokaz izreka 2.6. Izrek bomo dokazali z matematično indukcijo po vrednosti s.

Baza indukcije: $s = t$. To očitno velja, saj je $(X, \mathcal{B})$ t-načrt po predpostavki izreka. Za $s = t$ sta števec in imenovalec ulomka v enačbi (2.1) 'prazna'. V tem primeru za vrednost ulomka vzamemo 1. Iz enačbe (2.1) sledi, da je $\lambda_s = \lambda$.

Indukcijski korak: Predpostavimo, da izrek velja za $s = i+1, \ldots, t-1, t$. Pokazati moramo, da izrek velja za $s = i$. Po indukcijski predpostavki je $(X, \mathcal{B})$ $(i+1)$-načrt. Iz definicije načrta sledi, da se vsaka $(i+1)$-podmnožica množice X pojavi v natanko λ_{i+1} blokih.

Naj bo I poljubna i-podmnožica množice X. Definirajmo množico $\mathcal{S}_I$:

$$\mathcal{S}_I = \{(x, B) \in X \times \mathcal{B} : x \notin I \text{ in } I \cup \{x\} \subseteq B\}, \tag{2.2}$$

kjer so x točke in B bloki načrta.

Elemente množice $\mathcal{S}_I$ bomo prešteli na dva načina:

1. način:

$$|\mathcal{S}_I| = \sum_{(x,B):x\notin I \text{ in } I\cup\{x\}\subseteq B} 1 = \sum_{B:I\subseteq B}\left(\sum_{x:x\notin I \text{ in } x\in B} 1\right)$$
$$= \sum_{B:I\subseteq B}(k-i) = (k-i)\sum_{B:I\subseteq B} 1 = (k-i)\cdot\lambda_i(I).$$

Vsoto, ki gre po vseh ustreznih parih (x, B), smo zapisali kot dvojno vsoto. Zunanja vsota gre po vseh ustreznih blokih B, notranja pa po ustreznih točkah x. Poljuben blok B ima k elementov. Bloki, po katerih teče zunanja vsota, vsebujejo množico I, za katero velja $|I| = i$. Notranja vsota teče po točkah, ki jih je natanko $|B \setminus I| = k - i$. Oznaka $\lambda_i(I)$ označuje število blokov, ki vsebujejo množico I.

2. način:

$$|\mathcal{S}_I| = \sum_{(x,B):x\notin I \text{ in } I\cup\{x\}\subseteq B} 1 = \sum_{x:x\notin I}\left(\sum_{B:\{x\}\cup I\subseteq B} 1\right)$$
$$= \sum_{x:x\notin I}\lambda_{i+1} = \lambda_{i+1}\sum_{x:x\notin I} 1 = \lambda_{i+1}\cdot(v-i).$$

V tem primeru teče zunanja vsota po vseh ustreznih točkah x, notranja pa po vseh ustreznih blokih B. Bloki, po katerih teče notranja vsota, ustrezajo pogoju $I\cup\{x\} \subseteq B$. Množica $I \cup \{x\}$ ima $i + 1$ elementov, saj $x \notin I$. Po indukcijski predpostavki je število blokov, po katerih teče notranja vsota, ravno λ_{i+1}. Zunanja vsota teče po točkah x, ki ustrezajo pogoju $x \notin I$. Takšnih točk je ravno $|X \setminus I| = v - i$.

Štetji enačimo in dobimo:

$$(k-i)\cdot\lambda_i(I) = (v-i)\cdot\lambda_{i+1}, \tag{2.3}$$

od koder sledi

$$\lambda_i(I) = \frac{(v-i)}{(k-i)}\cdot\lambda_{i+1}. \tag{2.4}$$

Iz enačbe (2.4) je razvidno, da je vrednost $\lambda_i(I)$ neodvisna od izbire množice I. Zato lahko pišemo $\lambda_i = \lambda_i(I)$. Vsaka i-podmnožica množice X je vsebovana v λ_i blokih načrta. To pa pomeni, da je $(X, \mathcal{B})$ i-načrt s parametri i-(v, k, λ_i). Po indukcijski predpostavki velja

$$\lambda_{i+1} = \lambda\cdot\frac{(v-(i+1))(v-(i+1)-1)\ldots(v-t+1)}{(k-(i+1))(k-(i+1)-1)\ldots(k-t+1)}. \tag{2.5}$$

Če λ_{i+1} v enačbi (2.4) nadomestimo z izrazom iz enačbe (2.5), dobimo enačbo (2.1). □

Število blokov, ki vsebujejo 1-podmnožico množice X po navadi označimo z r, tj. $r = \lambda_1$. Število vseh blokov označimo z b, tj. $b = |\mathcal{B}|$.

Posledica 2.8. *Naj bo $(X, \mathcal{B})$ t-načrt. Velja*

$$(v-i)\lambda_{i+1} = (k-i)\lambda_i \tag{2.6}$$

za vsak $0 \leq i \leq t-1$.

Dokaz. V dokazu izreka 2.6 smo že pokazali, da (2.6) velja za $1 \leq i \leq t-1$. V primeru, ko je $i = 0$, je I iz dokaza izreka 2.6 prazna množica. Oznaka λ_0 je število blokov, ki vsebujejo prazno množico, torej $\lambda_0 = b$. Indukcijski korak iz dokaza izreka 2.6 velja tudi za $i = 0$. □

Posledica 2.9. *Naj bo $(X, \mathcal{B})$ t-načrt. Velja*

$$vr = bk. \tag{2.7}$$

Dokaz. V enačbi (2.6) lahko postavimo $i = 0$ in upoštevamo, da je $\lambda_0 = b$ in $\lambda_1 = r$. □

Izrek 2.10. *Če obstaja načrt $(X, \mathcal{B})$ s parametri t-(v, k, λ), potem velja*

$$(k-i)(k-i-1)\dots(k-t+1) \mid \lambda(v-i)(v-i-1)\dots(v-t+1) \tag{2.8}$$

za vsak $0 \leq i \leq t-1$.

Dokaz. Enačbo (2.1) lahko zapišemo kot

$$\lambda_i = \frac{\lambda(v-i)(v-i-1)\dots(v-t+1)}{(k-i)(k-i-1)\dots(k-t+1)}. \tag{2.9}$$

Ker je λ_i celo število, mora biti tudi vrednost ulomka na desni strani (2.9) celo število. To se zgodi samo, ko je števec ulomka deljiv z imenovalcem. □

Primer 2.11. Ali obstaja načrt s parametri 3-$(11, 4, 1)$? To bomo ugotovili s pomočjo izreka 2.10. Vrednosti parametrov so $t = 3$, $v = 11$, $k = 4$ in $\lambda = 1$. Parametre bomo vstavili v enačbo (2.8) za $0 \leq i \leq 2$.

Za $i = 0$ dobimo pogoj $4 \cdot 3 \cdot 2 \mid 11 \cdot 10 \cdot 9$, kar lahko zapišemo kot $2^3 \cdot 3 \mid 2 \cdot 3^2 \cdot 5 \cdot 11$. Ta pogoj ni izpolnjen, zato načrt s parametri 3-$(11, 4, 1)$ ne obstaja. Pogojev za $i = 1$ in $i = 2$ ni potrebno preverjati.

Primer 2.12. Ali obstaja načrt s parametri 5-$(28, 7, 1)$? Kaj nam v tem primeru pove izreka 2.10? Vrednosti parametrov so $t = 5$, $v = 28$, $k = 7$ in $\lambda = 1$. Parametre vstavimo v enačbo (2.8) za $0 \leq i \leq 4$ in dobimo pogoje:

$$7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \mid 1 \cdot 28 \cdot 27 \cdot 26 \cdot 25 \cdot 24 \text{ oziroma } 2^3 \cdot 3^2 \cdot 5 \cdot 7 \mid 2^6 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 13$$
$$6 \cdot 5 \cdot 4 \cdot 3 \mid 1 \cdot 27 \cdot 26 \cdot 25 \cdot 24 \text{ oziroma } 2^3 \cdot 3^2 \cdot 5 \mid 2^4 \cdot 3^4 \cdot 5^2 \cdot 13$$
$$5 \cdot 4 \cdot 3 \mid 1 \cdot 26 \cdot 25 \cdot 24 \text{ oziroma } 2^2 \cdot 3 \cdot 5 \mid 2^4 \cdot 3 \cdot 5^2 \cdot 13$$
$$4 \cdot 3 \mid 1 \cdot 25 \cdot 24 \text{ oziroma } 2^2 \cdot 3 \mid 2^3 \cdot 3 \cdot 5^2$$
$$3 \mid 1 \cdot 24 \text{ oziroma } 3 \mid 2^3 \cdot 3$$

Vsi pogoji veljajo, toda to ne pomeni nujno, da načrt s temi parametri obstaja. Izrek tudi nič ne pove, kako konstruirati take načrte.

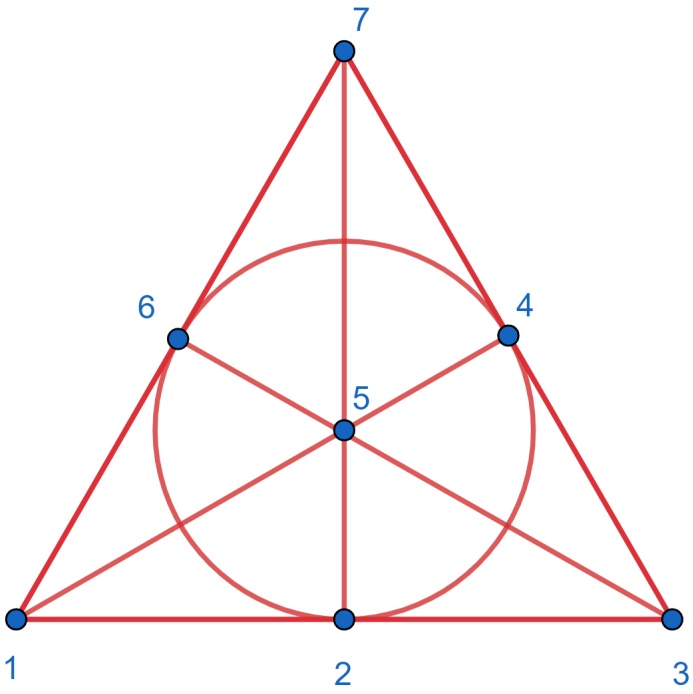
2.2 Steinerjevi sistemi

Definicija 2.13. Načrtu s parametri t-$(v, k, 1)$, kjer je $t \geq 2$, pravimo *Steinerjev sistem* in ga običajno označimo z $S(t, k, v)$. Steinerjevemu sistemu s parametri $S(2, 3, v)$ pravimo *Steinerjev trojček*.

Primer 2.14. Naj bo $X = \{1, 2, 3, \ldots, 7\}$ in

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

Vidimo, da je $v = 7$. Ker vsak blok vsebuje tri točke, je $k = 3$. Vidimo tudi, da vsak par točk nastopa v natanko enem bloku, zato je $\lambda = 1$ in $t = 2$. Par $(X, \mathcal{B})$ je načrt s parametri 2-$(7, 3, 1)$ oziroma Steinerjev trojček $S(2, 3, 7)$, ki je bolj znan po imenu Fanova ravnina (glej sliko 1).



Slika 1: Fanova ravnina.

2.3 Končne projektivne ravnine

Definicija 2.15. *Končna projektivna ravnina* je par $(X, \mathcal{L})$, kjer je X končna množica in $\mathcal{L}$ družina podmnožic množice X, ki zadošča naslednjim aksiomom:

(PR1) za vsak par $\{x, y\} \subseteq X$, $x \neq y$, obstaja natanko en element $l \in \mathcal{L}$, da je $\{x, y\} \subseteq l$;

(PR2) za vsak par $\{l, p\} \subseteq \mathcal{L}$, $l \neq p$, velja $|l \cap p| = 1$;

(PR3) obstajajo štiri različne točke $T = \{t_1, t_2, t_3, t_4\} \subseteq X$, tako da za vsak $l \in \mathcal{L}$ in vse $U \subseteq T$, kjer je $|U| = 3$, velja $U \nsubseteq l$.

Elementom množice X pravimo točke, elementom družine $\mathcal{L}$ pa pravimo premice.

Trditev 2.16. *Naj bosta $l_1 \in \mathcal{L}$ in $l_2 \in \mathcal{L}$ dve različni premici. Potem obstaja točka $x \in X$, ki ni vsebovana v nobeni od teh premic, tj. $x \notin l_1$ in $x \notin l_2$.*

Dokaz. Denimo, da trditev ne drži, tj. vsaka točka pripada eni od teh dveh premic. Po aksiomu (PR2) obstaja natanko ena točka $z \in l_1 \cap l_2$. Z $x_1, x_2, x_3, \ldots$ označimo točke, ki pripadajo l_1 (in ne pripadajo l_2). Podobno, z $y_1, y_2, y_3, \ldots$ označimo točke, ki priapadajo l_2 (in ne pripadajo l_1). Naj bo T množica štirih točk, ki nam jo zagotavlja aksiom (PR3). Vemo, da $z \notin T$, saj bi v tem primeru vsaj tri točke iz T ležale na skupni premici. Poleg tega vemo, da T vsebuje največ dve izmed točk $x_1, x_2, x_3, \ldots$ in največ dve izmed točk $y_1, y_2, y_3, \ldots$. Brez škode za splošnost je $T = \{x_1, x_2, y_1, y_2\}$. Naj bo p_1 premica, ki vsebuje x_1 in y_1, in naj bo p_2 premica, ki vsebuje x_2 in y_2. Premici p_1 in p_2 obstajata po aksiomu (PR1). Vemo, da je $p_1 \neq p_2$, sicer bi bili v protislovju z (PR3). Po aksiomu (PR2) se p_1 in p_2 sekata v natanko eni točki, ki jo označimo z w. Če je $w \in l_1$, potem je $l_1 = p_1$ po aksiomu (PR1), saj l_1 in p_1 vsebujeta točki y_1 in w. (Točki y_1 in w sta različni. Če bi veljalo $y_1 = w$, potem bi sledilo, da je $p_2 = l_1$, saj bi l_1 in p_2 vsebovali točki y_1 in y_2. To pa bi pomenilo, da je $x_2 \in l_1$, protislovje.) Iz $l_1 = p_1$ sledi $x_1 \in l_1$, protislovje. Torej $w \notin l_1$. Podobno pokažemo, da $w \notin l_2$. Torej $w \in l_1 \cup l_2$. To pa je v protislovju z začetno predpostavko. □

Lema 2.17. *Naj bo $(X, \mathcal{L})$ končna projektivna ravnina. Vse premice vsebujejo enako število točk, tj. $|l| = |p|$ za vse $l, p \in \mathcal{L}$.*

Dokaz. Naj bosta l_1 in l_2 poljubni premici in naj bo $z \in l_1 \cap l_2$. Po trditvi 2.16 obstaja točka $s \in l_1 \cup l_2$. Definiramo preslikavo $\varphi\colon l_1 \setminus \{z\} \to l_2 \setminus \{z\}$. Naj bo $x \in l_1$, $x \neq z$. Po aksiomu (PR1) obstaja natanko ena premica p, ki vsebuje x in s. Po aksiomu (PR2) imata premici p in l_2 natanko eno skupno točko, ki jo označimo z y. Definiramo $\varphi(x) = y$. Preslikava φ je dobro definirana, ker je premica p enolično določena, prav tako pa je enolično določeno presečišče premic l_2 in p. Pokazali bomo, da je φ bijektivna preslikava.

Naj bosta $x_1, x_2 \in l_1 \setminus \{z\}$. Naj bo $\varphi(x_1) = \varphi(x_2)$. Naj bo p_1 premica, ki vsebuje točke x_1, s in $\varphi(x_1)$. Naj bo p_2 premica, ki vsebuje točkex_2, s in $\varphi(x_2)$. Po aksiomu (PR1) je $p_1 = p_2$ (saj obe premici vsebujeta točki s in $\varphi(x_1)$). Po aksiomu (PR2) se p_1 in $l_1$sekata v natanko eni točki, torej $x_1 = x_2$. Z drugimi besedami, φ je injektivna preslikava.

Naj bo $y \in l_2 \setminus \{z\}$ poljubna točka. Po aksiomu (PR1) obstaja natanko ena premica p, ki vsebuje y in s. Z x označimo presečišče premic p in l_1 (ki je po aksiomu (PR2)

enolično določeno). Prepričajmo se, da je $x \neq z$. Če bi veljalo $x = z$, bi iz aksioma (PR1) sledilo $l_2 = p$. To bi pomenilo, da je $s \in l_2$, kar pa ni mogoče. Vidimo, da je $y = \varphi(x)$. Z drugimi besedami, φ je surjektivna preslikava.

Ker je preslikava φ bijektivna, je $|l_2 \setminus \{z\}| = |l_1 \setminus \{z\}|$ oziroma $|l_1| = |l_2|$. □

Naj bo $n+1 = |l|$, kjer je $l \in \mathcal{L}$. Število n je *red* končne projektivne ravnine $(X, \mathcal{L})$.

Trditev 2.18. *Naj bo $x \in X$ poljubna točka. Obstaja premica l, ki ne vsebuje točke x, tj. $x \notin l$.*

Dokaz. Denimo, da trditev ne drži, tj. vse premice potekajo skozi točko x. Naj bodo $T = \{t_1, t_2, t_3, t_4\}$ točke, ki nam jih zagotovi aksiom (PR3). Lahko se zgodi, da je $x \in T$. V tem primeru naj bo $t_4 = x$. Kakor koli že, točke t_1, t_2 in t_3 ne ležijo na isti premici. Po aksiomu (PR1) obstaja natanko ena premica l_1, ki vsebuje x in t_1. Podobno, z l_2 označimo premico, ki vsebuje x in t_2, z l_3 pa premico, ki vsebuje x in t_3. Po aksiomu (PR1) obstaja premica $p_{1,2}$, ki vsebuje t_1 in t_2. Podobno, s $p_{1,3}$ označimo premico, ki vsebuje t_1 in t_3, s $p_{2,3}$ pa premico, ki vsebuje t_2 in t_3. Ker točka x leži na vseh premicah, velja $x \in p_{1,2}$, $x \in p_{1,3}$ in $x \in p_{2,3}$. Ker $\{x, t\} \subseteq p_{1,2}$ in $\{x, t\} \subseteq p_{1,3}$, iz aksioma (PR1) sledi $p_{1,2} = p_{1,3}$. Podobno lahko pokažemo še $p_{1,2} = p_{2,3}$, torej velja $p_{1,2} = p_{1,3} = p_{2,3}$. To pomeni, da so t_1, t_2 in t_3 na isti premici, protislovje. □

Lema 2.19. *Naj bo $(X, \mathcal{L})$ končna projektivna ravnina. Vse točke so vsebovane v enakem številu premic, tj. $|\{l \in \mathcal{L} : x \in l\}| = |\{l \in \mathcal{L} : y \in l\}|$ za vse $x, y \in X$.*

Dokaz. Naj bo $x \in X$ poljubna točka. Po trditvi 2.18 obstaja premica $l \in \mathcal{L}$, $x \notin l$. Definirajmo preslikavo $\psi \colon \{l' \in \mathcal{L} : x \in l'\} \to l$. Naj bo p poljubna premica, ki vsebuje točko x. Po aksiomu (PR2) obstaja natanko ena točka y, ki je skupna premicama l in p. Definiramo $\psi(p) = y$. Preslikava ψ je dobro definirana, ker je točka y enolično določena.

Naj bosta p_1 in p_2 poljubni premici, ki vsebujeta točko x. Naj bo $\psi(p_1) = \psi(p_2)$. Iz aksioma (PR1) sledi $p_1 = p_2$. Z drugimi besedami, ψ je injektivna.

Naj bo $u \in l$ poljubna točka. Po aksiomu (PR1) obstaja premica p, ki vsebuje točki x in u. Vidimo, da je $u = \psi(p)$, torej je preslikava ψ surjektivna.

Ker je ψ bijektivna, sledi $|\{l' \in \mathcal{L} : x \in l'\}| = |l|$. Lema 2.17 pa nam pove, da vsaka premica vsebuje isto število točk, kar smo označili z $n + 1$. Torej $|\{l' \in \mathcal{L} : x \in l'\}| = n + 1$. □

Izrek 2.20. *Naj bo $(X, \mathcal{L})$ končna projektivna ravnina reda n. Potem velja*

$$|X| = |\mathcal{L}| = n^2 + n + 1.$$

Dokaz. Naj bo $t \in X$ poljubna točka. Iz leme 2.19 vemo, da je točka t vsebovana v $n+1$ različnih premicah, ki jih označimo z $l_1, l_2, \ldots, l_{n+1}$. Iz aksioma (PR1)sledi, da ne obstaja točka, ki ne bi bila vsebovana v nobeni izmed premic $l_1, l_2, \ldots, l_{n+1}$. Iz aksioma (PR2) sledi $(l_i \setminus \{t\}) \cap (l_i \setminus \{t\}) = \emptyset$ za $i \neq j$. Lema 2.17 nam pove, da je $|l_i| = n+1$ za vse $1 \leq i \leq n+1$ oziroma $|l_j \setminus \{t\}| = n$. Torej:

$$X = \bigcup_{i=1}^{n+1} l_i = \left(\bigsqcup_{i=1}^{n+1} l_i \setminus \{t\} \right) \sqcup \{t\},$$

kjer simbol $\sqcup$ označuje disjunktno unijo množic. Od tod sledi:

$$\begin{aligned} |X| &= \left| \bigcup_{i=1}^{n+1} l_i \right| = \left(\sum_{i=1}^{n+1} |l_i \setminus \{t\}| \right) + |\{t\}| \\ &= \left(\sum_{i=1}^{n+1} n \right) + 1 = (n+1)n + 1 = n^2 + n + 1. \end{aligned}$$

Naj bo $l \in \mathcal{L}$ poljubna premica. Iz leme 2.17 vemo, da premica l vsebuje $n+1$ točk, ki jih označimo z $x_1, x_2, \ldots, x_{n+1}$. Definirajmo $L_i = \{p \in \mathcal{L} : x_i \in p\}$ za $1 \leq i \leq n+1$. Iz aksioma (PR2) sledi, da ne obstaja premica, ki ne bi bila vsebovana v nobeni od množic $L_1, L_2, \ldots, L_{n+1}$. Iz aksioma (PR1) sledi $L_i \cap L_j = \{l\}$ za $i \neq j$, torej $(L_i \setminus \{l\}) \cap (L_j \setminus \{l\}) = \emptyset$ za $i \neq j$. Lema 2.19 nam pove, da je $|L_i| = n+1$ za vse $1 \leq i \leq n+1$ oziroma $|L_i \setminus \{l\}| = n$. Torej:

$$\mathcal{L} = \bigcup_{i=1}^{n+1} L_i = \left(\bigsqcup_{i=1}^{n+1} L_i \setminus \{l\} \right) \sqcup \{l\}.$$

Od tod sledi:

$$\begin{aligned} |\mathcal{L}| &= \left| \bigcup_{i=1}^{n+1} L_i \right| = \left(\sum_{i=1}^{n+1} |L_i \setminus \{l\}| \right) + |\{l\}| \\ &= \left(\sum_{i=1}^{n+1} n \right) + 1 = (n+1)n + 1 = n^2 + n + 1. \end{aligned}$$

□

Primer 2.21. Naj bo $(X, \mathcal{L})$ končna projektivna ravnina reda n. Po lemi 2.17 vse premice vsebujejo $n+1$ točk. Po aksiomu (PR1) je par $\{x_i, x_j\} \subseteq X$, $i \neq j$, vsebovan v natanko eni premici. Po izreku 2.20 je $|X| = n^2+n+1$. Torej je $(X, \mathcal{L})$ 2-$(n^2+n+1, n+1, 1)$ načrt. Poleg tega vemo tudi, da je $b = n^2+n+1$ (to nam pove izrek 2.20) in $r = n+1$ (to nam pove lema 2.19).

2.4 Incidenčne matrike načrtov

Definicija 2.22. Naj bo $(X, \mathcal{B})$ načrt, kjer je $X = \{x_1, x_2, \ldots, x_v\}$ in $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_b\}$. *Incidenčna matrika* načrta $(X, \mathcal{B})$ je $v \times b$ matrika $A = (a_{ij})_{1 \le i \le v, 1 \le j \le b}$, kjer je

$$a_{ij} = \begin{cases} 1, & \text{če je } x_i \in \beta_j, \\ 0, & \text{sicer.} \end{cases} \tag{2.10}$$

Z $I_{n\times n}$ bomo označevali identično matriko velikosti $n \times n$, z $J_{n\times m}$ pa matriko samih enic velikosti $n \times m$.

Lema 2.23. *Za incidenčno matriko A poljubnega 2-(v, k, λ) načrta velja, da je*

$$AA^T = (r - \lambda)I_{v\times v} + \lambda J_{v\times v}. \tag{2.11}$$

Dokaz. Po definiciji produkta matrik dobimo

$$(AA^T)_{i,j} = a_{i,1}a_{j,1} + a_{i,2}a_{j,2} + a_{i,3}a_{j,3} + \cdots + a_{i,v}a_{j,v} = \sum_{\ell=1}^{v} a_{i,\ell}a_{j,\ell}. \tag{2.12}$$

V primeru, ko je $i = j$, dobimo $(AA^T)_{i,i} = \sum_{\ell=1}^{v} a_{i,\ell}^2 = \sum_{\ell=1}^{v} a_{i,\ell}$, to pa je ravno število blokov, ki vsebujejo točko x_i, kar je ravno r. V primeru, ko je $i \neq j$, je produkt $a_{i,\ell}a_{j,\ell}$ enak 1 samo, če sta obe točki x_i in x_j vsebovani v bloku β_l. Torej, $(AA^T)_{i,j}$ je ravno število blokov, ki vsebujejo par točk $\{x_i, x_j\}$. To pa je v primeru 2-načrta ravno λ. □

Lema 2.24. *Za incidenčno matriko A poljubnega 2-načrta velja*

$$\det(AA^T) = rk(r - \lambda)^{v-1}. \tag{2.13}$$

Dokaz. Iz leme 2.23 vemo, da je

$$AA^T = \begin{bmatrix} r & \lambda & \lambda & \ldots & \lambda \\ \lambda & r & \lambda & & \vdots \\ \lambda & \lambda & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \lambda \\ \lambda & \ldots & \ldots & \lambda & r \end{bmatrix}. \tag{2.14}$$

V matriki (2.14) od vseh stolpcev od drugega do zadnjega odštejemo prvi stolpec in dobimo:

$$\begin{bmatrix} r & (\lambda - r) & (\lambda - r) & \ldots & (\lambda - r) \\ \lambda & (r - \lambda) & & & \\ \lambda & & (r - \lambda) & & \\ \vdots & & & \ddots & \\ \lambda & & & & (r - \lambda) \end{bmatrix}. \tag{2.15}$$

Ta operacija (prištevanje večkratnika enega stolpca nekemu drugemu stolpcu) ohrani vrednost determinante. V matriki (2.15) vse vrstice od druge do zadnje prištejemo prvi vrstici in dobimo:

$$\begin{bmatrix} r+(v-1)\lambda & & & & & \\ \lambda & (r-\lambda) & & & & \\ \lambda & & (r-\lambda) & & & \\ \vdots & & & \ddots & & \\ \lambda & & & & (r-\lambda) \end{bmatrix}. \tag{2.16}$$

Ker je (2.16) spodnje trikotna matrika, je njena determinanta enaka produktu elementov na diagonali, torej je

$$\det(AA^T) = (r+(v-1)\lambda)(r-\lambda)^{v-1}. \tag{2.17}$$

Iz posledice 2.8 (za $i = 1$) sledi $(v-1)\lambda_2 = (k-1)\lambda_1$. Ker imamo opravka z 2-načrtom, je $\lambda = \lambda_2$. Torej je $(v-1)\lambda = (k-1)r$. V (2.17) upoštevamo $(v-1)\lambda = (k-1)r$ in dobimo $(r+(k-1)r)(r-\lambda)^{v-1}$, kar je ravno $kr(r-\lambda)^{v-1}$. □

Izrek 2.25. *Za poljuben 2-načrt velja $b \geq v$.*

Dokaz. Obravnavamo dva primere glede na vrednost $\det(AA^T)$:

i) $\det(AA^T) = 0$: Iz lemi 2.24 sledi $rk(r–\lambda)^{v-1} = 0$. To velja samo, če je $r - \lambda = 0$, iz česar sledi $r = \lambda$, torej $\lambda_1 = r = \lambda = \lambda_2$. Uporabimo posledico 2.8 (za $i = 1$):

$$\begin{aligned} (v-1)\lambda_2 &= (k-1)\lambda_1 \\ v-1 &= k-1 \\ v &= k \end{aligned}$$

Po definiciji načrta (definicija 2.1) to ni dovoljeno.

ii) $\det(AA^T) \neq 0$: Matrika AA^T je polnega ranga, torej $\text{rang}(AA^T) = v$. Iz linearne algebre vemo, da rang produkta matrik ni večji od rangov faktorjev, torej $\text{rang}(A) \geq \text{rang}(AA^T)$. Ker je A matrika velikosti $v \times b$, velja $\text{rang}(A) \leq b$. Torej

$$b \geq \text{rang}(A) \geq \text{rang}(AA^T) = v,$$

iz česar sledi $b \geq v$. □

3 Simetrični načrti

V tem poglavju obravnavamo načrte, ki imajo enako število točk in blokov. Takim načrtom pravimo simetrični načrti. (Da se izognemo trivialnim primerom, v definiciji izvzamemo polne načrte in 1-načrte.) Pokažemo, da je vsak simetrični načrt 2-načrt, obratno pa ne velja, kot bomo videli na primeru 3.13. Nato pokažemo, da imata vsaka dva bloka simetričnega načrta λ skupnih točk. Predstavimo duale načrtov. Dual načrta dobimo tako, da točke in bloki na nek način 'zamenjajo vloge'. Pokažemo, da so duali simetričnih 2-načrtov tudi 2-načrti. Na koncu poglavja predstavimo še dodatne potrebne pogoje za obstoj simetričnih načrtov (izrek 3.14 in izrek 3.15). Z uporabo teh pogojev pokažemo, da končne projektivne ravnine reda 6 ne obstajajo.

Definicija 3.1. Načrt s parametri t-(v, k, λ) je *simetričen*, če ni poln in je $v = b$ ter $t \geq 2$.

Bistven pogoj je to, da je $v = b$, tj. število točk je enako številu blokov.

Izrek 3.2. *Če je načrt s parametri t-(v, k, λ) simetričen, potem je $t = 2$.*

Dokaz. Naj bo $(X, \mathcal{B})$, kjer je $X = \{x_1, x_2, \ldots, x_v\}$ in $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_b\}$, simetričen načrt s parametri t-(v, k, λ). Denimo, da je $t \geq 3$. V primeru, da je $t > 3$, uporabimo izrek 2.6, ki nam pove, da je $(X, \mathcal{B})$ tudi 3-(v, k, λ_3) načrt (za ustrezno vrednost parametra λ_3). Zato se lahko brez škode za splošnost omejimo na $t = 3$.

Naj bo

$$\widetilde{X} = \{x_1, \ldots, x_{v-1}\} = X \setminus \{x_v\} \text{ in}$$
$$\widetilde{\mathcal{B}} = \{\beta \setminus \{x_v\} : \beta \in \mathcal{B}, x_v \in \beta\}.$$

Prepričajmo se, da je $(\widetilde{X}, \widetilde{\mathcal{B}})$ načrt s parametri 2-$(v-1, k-1, \lambda)$. Velja $|\widetilde{X}| = |X \setminus \{x_v\}| = v - 1$. Naj bo $\widetilde{\beta} \in \widetilde{\mathcal{B}}$ poljuben blok. Po definiciji je $\widetilde{\beta} = \beta \setminus \{x_v\}$, kjer je $\beta \in \mathcal{B}$. Torej velja $|\widetilde{\beta}| = |\beta \setminus \{x_v\}| = k - 1$. Ker je $(X, \mathcal{B})$ 3-načrt, se trojček $\{x_i, x_j, x_v\}$, $1 \leq i < j < v$, pojavi v λ blokih načrta $(X, \mathcal{B})$. Velja

$$\{x_i, x_j, x_v\} \subseteq \beta \in \mathcal{B} \Longleftrightarrow \{x_i, x_j\} \subseteq \beta \setminus \{x_v\} \in \widetilde{\mathcal{B}}.$$

To pomeni, da je par $\{x_i, x_j\}$ vsebovan v λ blokih načrta $(\widetilde{X}, \widetilde{\mathcal{B}})$. Parametri načrta $(\widetilde{X}, \widetilde{\mathcal{B}})$ so res 2-$(v-1, k-1, \lambda)$.

Naj bo r število blokov načrta $(X, \mathcal{B})$, ki vsebuje točko x_v. Ker je $|\widetilde{\mathcal{B}}| = |\{\beta \in \mathcal{B} : x_v \in \beta\}|$, sledi $|\widetilde{\mathcal{B}}| = r$. Iz izreka 2.25 sledi

$$r \geq v - 1. \tag{3.1}$$

Ker je $(X, \mathcal{B})$ simetričen načrt, velja $b = v$. Po posledici 2.9 velja tudi

$$r = k. \tag{3.2}$$

Iz (3.1) in (3.2) sledi

$$k \geq v - 1.$$

Spomnimo se, da mora biti $k < v$. Če je $k > v - 1$, sledi $v - 1 < k < v$. To pa ni mogoče, saj sta v in k celi števili. Edina možnost je $k = v - 1$. Iz $k = v - 1$ in iz $b = v$ sledi $\mathcal{B} = \{X \setminus \{x_i\} : x_i \in X\} = \binom{X}{v-1}$. To pomeni, da je $(X, \mathcal{B})$ poln načrt, kar pa je v protislovju z definicijo simetričnega načrta (definicija 3.1). □

Parametre simetričnega 2-(v, k, λ) načrta povezujejo naslednje enakosti:

$$b = v, \tag{3.3}$$

$$r = k, \tag{3.4}$$

$$k(k-1) = \lambda(v-1). \tag{3.5}$$

Enakost (3.3) je del definicije simetričnega načrta. Enakost (3.4) sledi iz (3.3) in posledice 2.9. Če v (2.6) vstavimo $i = 1$, dobimo $(v-1)\lambda_2 = (k-1)\lambda_1$, iz te enakosti pa dobimo (3.5), če upoštevamo $\lambda = \lambda_2$ (ker je $t = 2$) in $\lambda_1 = r = k$.

Spomnimo se leme 2.23, ki pravi, da za incidenčno matriko A poljubnega 2-načrta velja

$$AA^T = (r - \lambda)I_{v\times v} + \lambda J_{v\times v}.$$

Lema 3.3. *Za incidenčno matriko A simetričnega 2-(v, k, λ) načrta velja*

$$A^T A = (k - \lambda)I_{b\times b} + \lambda J_{b\times b}. \tag{3.6}$$

Dokaz. Ker je načrt simetričen ($v = b$), je A kvadratna matrika. Po definiciji produkta matrik dobimo

$$(AJ)_{i,j} = a_{i,1} + a_{i,2} + \cdots + a_{a,v} = \sum_{l=1}^{v} a_{i,l} = |\{\beta \in \mathcal{B} : x_i \in \beta\}| = r.$$

Z drugimi besedami, $AJ = rJ = kJ$. Podobno dobimo še

$$(JA)_{i,j} = a_{1,j} + a_{2,j} + \cdots + a_{v,j} = \sum_{l=1}^{v} a_{l,j} = |\{x \in X : x \in \beta_j\}| = k.$$

Z drugimi besedami, $JA = kJ$.

V dokazu izreka 2.25 smo že pokazali, da je $\det(AA^T) \neq 0$. Iz linearne algebre vemo, da je $\det(AA^T) = \det(A) \cdot \det(A^T)$. Torej $\det(A) \cdot \det(A^T) \neq 0$. Od tod sledi $\det(A) \neq 0$ in $\det(A^T) \neq 0$. Matrika A je obrnljiva (tj. A^{-1} obstaja).

Enačbo (2.11) z leve pomnožimo z A^{-1} in dobimo

$$A^{-1}AA^T = (k-\lambda)A^{-1}I + \lambda A^{-1}J,$$

od tod pa

$$A^T = (k-\lambda)A^{-1} + \lambda A^{-1}J.$$

Iz $AJ = kJ$ sledi $J = \frac{1}{k}AJ$ torej:

$$A^{-1}J = A^{-1}(\frac{1}{k}AJ) = \frac{1}{k}A^{-1}(AJ) = \frac{1}{k}(A^{-1}A)J = \frac{1}{k}J.$$

Zdaj pa lahko izračunamo:

$$\begin{aligned} A^TA &= ((k-\lambda)A^{-1} + \lambda A^{-1}J)A \\ &= (k-\lambda)A^{-1}A + \lambda(A^{-1}J)A \\ &= (k-\lambda)I + \lambda(\frac{1}{k}J)A \\ &= (k-\lambda)I + \lambda\frac{1}{k}(JA) \\ &= (k-\lambda)I + \lambda\frac{1}{k}(kJ) \\ &= (k-\lambda)I + \lambda J \end{aligned}$$

□

Posledica 3.4. *Za incidenčno matriko A simetričnega* 2-(v, k, λ) *načrta velja*

$$A^TA = AA^T. \tag{3.7}$$

Dokaz. Sledi iz leme 3.3 in leme 2.23 pri čemer upoštevamo (3.3) in (3.4). □

Izrek 3.5. *Če je* $(X, \mathcal{B})$ *simetrični* 2-(v, k, λ) *načrt, imata vsaka dva različna bloka natanko* λ *skupnih točk, tj.* $|\beta_i \cap \beta_j| = \lambda$ *za vse* $i \neq j$.

Dokaz. Pri dokazu bomo uporabili incidenčno matriko načrta. Po definiciji produkta matrik velja

$$(A^TA)_{i,j} = a_{1,i}a_{1,j} + a_{2,i}a_{2,j} + \cdots + a_{v,i}a_{v,j} = \sum_{\ell=1}^{v} a_{\ell,i}a_{\ell,j}.$$

Po definiciji incidenčne matrike velja, da $a_{\ell i} = 1$ samo, če je $x_\ell \in \beta_i$, in $a_{\ell j} = 1$ samo, če je $x_\ell \in \beta_j$. Produkt $a_{\ell i}a_{\ell j}$ je enak 1 natanko tedaj, ko je $x_\ell \in \beta_i \cap \beta_j$. Torej:

$$\sum_{\ell=1}^{v} a_{\ell,i}a_{\ell,j} = \begin{cases} |\{x \in X : x \in \beta_j\}|, & \text{če } i = j, \\ |\{x \in X : x \in \beta_i \cap \beta_j\}|, & \text{če } i \neq j. \end{cases}$$

Po lemi 3.3 je $(A^TA)_{i,j} = \lambda$, če je $i \neq j$. □

3.1 Duali načrtov

Definicija 3.6. Naj bo $(X, \mathcal{B})$ načrt in $x \in X$. *Zvezda* točke x, z oznako $\mathrm{st}(x)$, je množica blokov, ki vsebujejo točko x, tj. $\mathrm{st}(x) = \{\beta \in \mathcal{B} : x \in \beta\}$.

Primer 3.7. Naj bo $(X, \mathcal{B})$ Fanova ravnina, kot v primeru 2.14.
Zvezda točke $x = 1$ je

$$\mathrm{st}(1) = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}\}.$$

Zvezda točke $x = 4$ je

$$\mathrm{st}(4) = \{\{1, 4, 5\}, \{2, 4, 7\}, \{3, 4, 7\}\}.$$

Definicija 3.8. Naj bo $(X, \mathcal{B})$ načrt. *Dual* načrta $(X, \mathcal{B})$ je par $(X^*, \mathcal{B}^*)$, kjer je

$$X^* = \mathcal{B} \text{ in}$$
$$\mathcal{B}^* = \{\mathrm{st}(x) : x \in X\}.$$

Primer 3.9. Naj bo $(X, \mathcal{B})$ načrt kot v primeru 2.2. Bloke načrta označimo po vrsti takole: $\beta_1 = \{1, 2, 3, 7, 10\}$, $\beta_2 = \{1, 2, 6, 9, 11\}, \ldots$. Zato lahko pišemo $\mathcal{B} = \{\beta_1, \beta_2, \beta_3, \ldots, \beta_{11}\}$. Potem je

$$X^* = \mathcal{B} = \{\beta_1, \beta_2, \beta_3, \ldots, \beta_{11}\},$$

$$\begin{aligned} \mathcal{B}^* = \{\mathrm{st}(x) : x \in X\} = \{&\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\}, \{\beta_1, \beta_2, \beta_6, \beta_7, \beta_8\}, \{\beta_1, \beta_3, \beta_6, \beta_9, \beta_{10}\}, \\ &\{\beta_3, \beta_4, \beta_6, \beta_7, \beta_{11}\}, \{\beta_3, \beta_5, \beta_7, \beta_8, \beta_9\}, \{\beta_2, \beta_4, \beta_7, \beta_9, \beta_{10}\}, \\ &\{\beta_1, \beta_4, \beta_8, \beta_9, \beta_{11}\}, \{\beta_4, \beta_5, \beta_6, \beta_8, \beta_{10}\}, \{\beta_2, \beta_3, \beta_8, \beta_{10}, \beta_{11}\}, \\ &\{\beta_1, \beta_5, \beta_7, \beta_{10}, \beta_{11}\}, \{\beta_2, \beta_5, \beta_6, \beta_7, \beta_{10}\}\}. \end{aligned}$$

Par $(X^*, \mathcal{B}^*)$ je dual načrta $(X, \mathcal{B})$.

Trditev 3.10. *Naj bo $(X, \mathcal{B})$ poljuben t-(v, k, λ) načrt. Potem je $(X^*, \mathcal{B}^*)$ načrt s parametri* 1-(b, r, k).

Dokaz. Naj bo poljuben t-(v, k, λ) načrt. Podrobneje si oglejmo $(X^*, \mathcal{B}^*)$. Velja $|X^*| = |\mathcal{B}| = b$. Po definiciji 3.6 je $\mathrm{st}(x) = \{\beta \in \mathcal{B} : x \in \beta\}$, torej

$$|\,\mathrm{st}(x)| = |\{\beta \in \mathcal{B} : \{x\} \subseteq \beta\}| = \lambda_1 = r.$$

Pokažimo, da je vsaka točka vsebovana v enakem številu blokov. Naj bo $x^* = \beta \in \mathcal{B}$ poljubna točka duala. Ker so bloki načrta $(X^*, \mathcal{B}^*)$ zvezde točk v $(X, \mathcal{B})$, lahko namesto β^* pišemo $\mathrm{st}(x)$. Potem je

$$|\{\beta^* \in \mathcal{B}^* : x^* \in \beta^*\}| = |\{x \in X : \beta \in \mathrm{st}(x)\}| = k.$$

Utemeljimo, da velja zadnji enačaj v zgornji enakosti. Blok β je vsebovan v $\mathrm{st}(x)$ natanko tedaj, ko je $x \in \beta$. Torej je blok β vsebovan v zvezdi od vsake svoje točke. Par $(X^*, \mathcal{B}^*)$ je 1-(b, r, k) načrt. □

Primer 3.11. Poglejmo si par $(X^*, \mathcal{B}^*)$ iz primera 3.9. Po trditvi 3.10 je $(X^*, \mathcal{B}^*)$ 1-$(11, 5, 5)$ načrt. Preverimo lahko, da se vsak par $\{\beta_i, \beta_j\}, i \neq j$, pojavi v dveh blokih, zato je $(X^*, \mathcal{B}^*)$ tudi 2-$(11, 5, 2)$ načrt. Trojček $\{\beta_1, \beta_2, \beta_3\}$ se pojavi v enem bloku, trojček $\{\beta_1, \beta_2, \beta_9\}$ pa v nobenem, zato $(X^*, \mathcal{B}^*)$ ni 3-načrt.

V primeru 3.11 smo videli, da je dual simetričnega 2-načrta iz primera 3.9 tudi simetrični 2-načrt. To ni zgolj naključje, ker ima izrek 3.5 naslednjo posledico.

Posledica 3.12. *Naj bo $(X, \mathcal{B})$ simetrični 2-(v, k, λ) načrt. Potem je $(X^*, \mathcal{B}^*)$ načrt s parametri 2-(v, k, λ).*

Dokaz. Naj bosta $x_i^* = \beta_i$ in $x_j^* = \beta_j$ različni točki načrta $(X^*, \mathcal{B}^*)$. Potem je

$$|\{\beta^* \in \mathcal{B}^* : \{x_i^*, x_j^*\} \subseteq \beta^*\}| = |\{x \in X : \{\beta_i, \beta_j\} \subseteq \mathrm{st}(x)\}| = \lambda.$$

Zvezde, ki vsebuje bloka β_i in β_j, so ravno zvezde od njihovih skupnih točk, teh pa je po izreku 3.5 ravno λ. □

Primer 3.13. Naj bo $(X, \mathcal{B})$ načrt kot v primeru 2.3. Bloke načrta označimo po vrsti takole: $\beta_1 = \{1, 2, 3, 4\}$, $\beta_2 = \{1, 2, 5, 6\}, \ldots$. Zato lahko pišemo $\mathcal{B} = \{\beta_1, \beta_2, \beta_3, \ldots, \beta_{14}\}$. Potem je $X^* = \mathcal{B}$ in

$$\begin{aligned}\mathcal{B}^* = \{&\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7\}, \{\beta_1, \beta_2, \beta_3, \beta_8, \beta_9, \beta_{10}, \beta_{11}\},\\ &\{\beta_1, \beta_4, \beta_5, \beta_8, \beta_9, \beta_{12}, \beta_{13}\}, \{\beta_1, \beta_6, \beta_7, \beta_{10}, \beta_{11}, \beta_{12}, \beta_{13}\},\\ &\{\beta_2, \beta_4, \beta_6, \beta_8, \beta_{10}, \beta_{12}, \beta_{14}\}, \{\beta_2, \beta_5, \beta_7, \beta_9, \beta_{11}, \beta_{12}, \beta_{14}\},\\ &\{\beta_3, \beta_4, \beta_7, \beta_9, \beta_{10}, \beta_{13}, \beta_{14}\}, \{\beta_3, \beta_5, \beta_6, \beta_8, \beta_{11}, \beta_{13}, \beta_{14}\}\}.\end{aligned}$$

Lahko se prepričamo, da je par $(X^*, \mathcal{B}^*)$ 2-$(14, 7, 2)$ načrt, ki pa ni simetričen.

Izrek 3.14. *Naj bo v sodo število in naj obstaja simetrični 2-(v, k, λ) načrt. Potem je $k - \lambda$ popolni kvadrat.*

Dokaz. Naj bo A incidenčna matrika načrta. Iz linearne algebre vemo, da je $\det A^T = \det A$. Zato velja:

$$(\det A)^2 = (\det A) \cdot (\det A^T) = \det(AA^T) = rk(r-\lambda)^{v-1} = k^2(k-\lambda)^{v-1}. \tag{3.8}$$

V enačbi (3.8) predzadnji enačaj velja po lemi 2.24, zadnji enačaj pa zaradi (3.4). Iz enačbe (3.8) sledi

$$(k-\lambda)^{v-1} = \left(\frac{\det A}{k}\right)^2. \tag{3.9}$$

Ker je število na desni strani enačbe (3.9) popolni kvadrat, mora biti tudi $(k-\lambda)^{v-1}$ popolni kvadrat. Ker je $v-1$ liho število, mora biti $k-\lambda$ popolni kvadrat. □

Izrek 3.15. *Naj bo v liho število in naj obstaja simetrični 2-(v, k, λ) načrt. Potem ima enačba*

$$x^2 = (k-\lambda)y^2 + (-1)^{\frac{1}{2}(v-1)}\lambda z^2 \tag{3.10}$$

celoštevilsko rešitev (x, y, z), pri čemer je vsaj ena od spremenljivk x, y oziroma z neničelna.

Dokaz lahko bralec najde v [1].

Lema 3.16. *Število $x^2 + 1$ ni deljivo s 3 za noben $x \in \mathbb{Z}$.*

Dokaz. Število x je lahko oblike $3t, 3t+1$ ali $3t-1$.

- Če je $x = 3t$, potem $3 \mid (3t)^2 + 1 = 9t^2 + 1$, od tod pa sledi $3 \mid 1$, protislovje.
- Če je $x = 3t+1$, potem $3 \mid (3t+1)^2 + 1 = 9t^2 + 6t + 2$ od tod pa sledi $3 \mid 2$, protislovje.
- Če je $x = 3t-1$, potem $3 \mid (3t-1)^2 + 1 = 9t^2 - 6t + 2$ od tod pa sledi $3 \mid 2$, protislovje.

To pomeni, da $x^2 + 1$ ne more biti deljivo s 3. □

Izrek 3.17. *Končna projektivna ravnina reda 6 ne obstaja.*

Dokaz. Denimo, da obstaja končna projektivna ravnina $(X, \mathcal{L})$ reda $n = 6$. Spomnimo se (glej primer 2.21), da je končna projektivna ravnina reda n načrt s parametri 2-$(n^2+n+1, n+1, 1)$. V konkretnem, $(X, \mathcal{L})$ je 2-$(43, 7, 1)$ načrt. Izrek 2.20 nam pove, da je $(X, \mathcal{L})$ simetričen načrt. Ker je $v = 43$ liho število, lahko uporabimo izrek 3.15. Če parametre $k = 7$, $\lambda = 1$ in $v = 43$ vstavimo v enačbo (3.10) dobimo

$$x^2 = 6y^2 - z^2, \tag{3.11}$$

ki ima celoštevilsko rešitev. Brez škode za splošnost lahko predpostavimo, da je največji skupni delitelj števil x, y in z enak 1. (Sicer lahko izrazimo $x = \widetilde{x}d$, $y = \widetilde{y}d$ in $z = \widetilde{z}d$, kjer je d največji skupni delitelj števil x, y in z. Ni težko videti, da je tudi $(\widetilde{x}, \widetilde{y}, \widetilde{z})$ rešitev enačbe (3.11).)

Iz enačbe (3.11) sledi $x^2 + z^2 = 6y^2$. Vidimo, da $3 \mid x^2 + z^2$. Število z je lahko oblike $3k, 3k + 1$ ali $3k - 1$ za nek $k \in \mathbb{Z}$. Če je $z = 3k + 1$ potem je $x^2 + (3k + 1)^2 = x^2 + 9k^2 + 6k + 1$, od tod pa sledi $3 \mid x^2 + 1$, kar po lemi 3.16 ni mogoče. Podobno, če je $z = 3k - 1$, potem je $x^2 + (3k + 1)^2 = x^2 + 9k^2 - 6k + 1$, od tod pa sledi $3 \mid x^2 + 1$, kar po lemi 3.16 ni mogoče. Edina možnost je $z = 3k$, tj. $3 \mid z$. Potem iz enačbe (3.11) sledi $x^2 = 6y^2 - 9k^2$, kar pomeni, da $3 \mid x$, tj. $x = 3l$. Iz enačbe (3.11) sledi $6y^2 = x^2 + z^2 = 9l^2 + 9k^2$. Od tod dobimo $2y^2 = 3l^2 + 3k^2$. Vidimo, da $3 \mid y$. Število 3 je skupni delitelj števil x, y in z, protislovje. To pomeni, da (3.11) ni rešljiva, kar pomeni, da načrt s parametri 2-$(43, 7, 1)$ ne obstaja. □

4 Permutacijske grupe

V tem poglavju definiramo pojme iz teorije permutacijskih grup, ki jih uporabljamo v poglavju 5. Za več podrobnosti se lahko bralec obrne na [9, 10].

Definicija 4.1. Naj bo G neprazna množica (tj. $G \neq \emptyset$) in $\circ$ binarna operacija na množici G. Par $(G, \circ)$ je *grupa*, če velja:

- Za vse $a, b, c \in G$ velja:
$$(a \circ b) \circ c = a \circ (b \circ c).$$
(Pravimo, da je operacija $\circ$ asociativna.)
- Obstaja element $e \in G$, tako da za vsak $a \in G$ velja:
$$a \circ e = e \circ a = a.$$
(Element e je nevtralni element v G za operacijo $\circ$.)
- Za vsak $a \in G$ obstaja $a^{-1} \in G$, tako da velja:
$$a \circ a^{-1} = a^{-1} \circ a = e.$$
(Za vsak element a obstaja njegov nasprotni element a^{-1}.)

Primer 4.2. Naj bo $\mathbb{Z}_8 = \{0, 1, 2, \ldots, 7\}$. Operacija $+$ na elementih množice $\mathbb{Z}_8$ je definirana tako, da po vsakem seštevanju vzamemo ostanek pri deljenju z 8. $(\mathbb{Z}_8, +)$ je grupa. Nevtralni element grupe $(\mathbb{Z}_8, +)$ je število 0. Nasproti element k elementu 3 je 5, saj je $3 + 5 = 5 + 3 = 0$.

Kadar je operacija razvidna iz konteksta, bomo namesto $(G, \circ)$ pisali G in "grupa" rekli kar množici G.

Definicija 4.3. Naj bo G grupa. Podmnožica $H \subseteq G$ je *podgrupa* grupe G, če je zaprta za binarno operacijo grupe G in je sama zase tudi grupa za to isto binarno operacijo. Oznaka $H \leq G$ pomeni, da je H podgrupa grupe G.

Primer 4.4. Naj bo $(\mathbb{Z}_8, +)$ kot v primeru 4.2. Podmnožici $H_1 = \{0, 2, 4, 6\}$ in $H_2 = \{0, 4\}$ sta podgrupi grupe $\mathbb{Z}_8$ (za isto operacijo).

4.1 Simetrične grupe

Naj bo M neprazna množica. Bijektivni preslikavi $\pi\colon M \to M$ pravimo *permutacija* na M. Množica $\{\pi\colon M \to M \mid \pi \text{ je bijektivna}\}$ skupaj z operacijo kompozitum preslikav (tj. $(\pi \circ \rho)(m) = \pi(\rho(m))$, kjer je $m \in M$) je grupa, ki jo označimo z $\mathrm{Sym}(M)$ in ji pravimo *simetrična grupa na* M. Če je $\pi(m) = m$ za nek $m \in M$, pravimo, da π pribije element m oz. da je m fiksna točka permutacije π. Permutacija π je *r-cikel*, če obstajajo različne točke $m_1, \ldots, m_r$, tako da $\pi(m_i) = m_{i+1}$ za $1 \leq i < r$, $\pi(m_r) = m_1$, vse ostale elemente pa π pribije. Produkt permutacij π in ρ je definiran z $(\pi * \rho)(m) := \rho(\pi(m)) = (\rho \circ \pi)(m)$. Namesto $\pi * \rho$ bomo pogosto pisali kar $\pi\rho$. Poleg tega bomo za $\pi * \pi$ uporabljali krajši zapis π^2. Podobno bomo $\pi * \pi * \pi$ krajše pisali kot π^3 itd.

Grupo $\mathrm{Sym}(\{1, 2, \ldots, n\})$ na kratko označimo z S_n. Naj bo $\pi \in S_n$. Preslikavo π lahko zapišemo v obliki

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}.$$

Vsako permutacijo lahko zapišemo kot produkt disjunktnih ciklov.

Primer 4.5. Naj bo

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 9 & 4 & 3 & 1 & 10 & 8 & 2 & 6 \end{pmatrix}.$$

Potem je $\pi = (1\ 7\ 10\ 6) * (2\ 5\ 3\ 9) * (4) * (8)$. Cikle dolžine ena izpustimo in tudi simbola $*$ ne pišemo. Torej $\pi = (1\ 7\ 10\ 6)(2\ 5\ 3\ 9)$.

Definicija 4.6. Podgrupi grupe $\mathrm{Sym}(M)$ pravimo *permutacijska grupa* na množici M.

Definicija 4.7. Naj bodo $g_1, g_2, \ldots, g_k \in \mathrm{Sym}(M)$. Najmanjši podgrupi grupe $\mathrm{Sym}(M)$, ki vsebuje vse elemente $g_1, g_2, \ldots, g_k$, pravimo *podgrupa generirana z elementi* $g_1, g_2, \ldots, g_k$ in jo označimo z $\langle g_1, g_2, \ldots, g_k \rangle$. Elementom $g_1, g_2, \ldots, g_k$ pravimo *generatorji* grupe $\langle g_1, g_2, \ldots, g_k \rangle$.

Vsak element grupe $\langle g_1, g_2, \ldots, g_k \rangle$ lahko izrazimo kot produkt generatorjev in njihovih inverzov, npr. $g_1^3 (g_2^{-1})^2 g_1^2 g_3 g_2^2 (g_1^{-1})^3$.

Primer 4.8. Naj bo $g_1 = (1\ 5)(2\ 6)(3\ 7)(4\ 8)$ in naj bo $g_2 = (1\ 5\ 8\ 4)(2\ 6\ 7\ 3)$. Očitno

velja $g_1^2 = \mathrm{id}$ in $g_2^4 = \mathrm{id}$. Poiščimo še ostale elemente grupe $\langle g_1, g_2 \rangle$:

$$\begin{aligned} g_1 g_2 &= (1\ 8)(2\ 7), \\ g_2^2 &= (1\ 8)(2\ 7)(3\ 6)(4\ 5), \\ g_2 g_1 &= (3\ 6)(4\ 5), \\ g_2^3 &= (1\ 4\ 8\ 5)(2\ 3\ 7\ 6), \\ g_1 g_2^2 &= (1\ 4)(2\ 3)(5\ 8)(6\ 7). \end{aligned}$$

Bralec se lahko sam prepriča, da z množenjem generatorjev in njihovih inverzov ne moremo dobiti nobenih novih permutacij. Torej,

$$\langle g_1, g_2 \rangle = \{\mathrm{id}, g_1, g_2, g_1 g_2, g_2^2, g_2 g_1, g_2^3, g_1 g_2^2\} \leq S_8.$$

4.2 Delovanja grup

Definicija 4.9. Naj bo G grupa in M neprazna množica. *Delovanje* G na množici M je preslikava $\mu\colon M \times G \to M$, da velja:

- $\mu(x, \mathrm{id}_G) = x$ za vsak $x \in M$,
- $\mu(\mu(x, g), h) = \mu(x, gh)$ za vsaka $g, h \in G$ in vsak $x \in M$.

Identično preslikavo na množici M bomo pogosto označevali z id_M.

Primer 4.10. Naj bo $G = \mathbb{Z}_8 = \{0, 1, 2, \ldots, 7\}$ kot v primeru 4.2 in $M = \{0, 1, 2, 3\}$. Preverimo, da je preslikava $\mu(x, g) = (x + g) \bmod 4$ delovanje grupe G na množici M. Naj bo $x \in M$ poljuben. Velja $\mu(x, 0) = (x + 0) \bmod 4 = x \bmod 4 = x$.

Naj bodo $x \in M$ in $g, h \in G$ poljubni. Potem velja

$$\begin{aligned} \mu(\mu(x, g), h) &= \mu((x + g) \bmod 4, h) = ((x + g) \bmod 4 + h) \bmod 4 \\ &= ((x + g) + h) \bmod 4 = (x + (g + h)) \bmod 4 = \mu(x, g + h). \end{aligned}$$

Res, μ je delovanje grupe G na množici M. Pravimo tudi, da G deluje na množici M.

Namesto $\mu(x, g)$ bomo pogosto pisali kar $g(x)$.

Definicija 4.11. Delovanje grupe G na množici M je *zvesto*, če iz $\mu(x, g) = x$ za vsak $x \in M$ sledi $g = \mathrm{id}_G$.

Primer 4.12. Vzemimo delovanje iz primera 4.10. Ali je delovanje zvesto? Naj bo $x \in M$ poljuben. Potem je

$$\mu(x, 4) = (x + 4) \bmod 4 = x \bmod 4 = x.$$

To delovanje ni zvesto.

Definicija 4.13. Naj grupa G deluje na množici M. Naj bo $x \in M$ poljuben. Množici $\{g(x) : g \in G\}$ pravimo *orbita* elementa x pri delovanju G in jo označimo z x^G. Množici $\{g \in G : g(x) = x\}$ pravimo *stabilizator* elementa x v G in jo označimo z G_x.

Primer 4.14. Naj bo $G = \langle g_1, g_2 \rangle$ kot v primeru 4.8. Orbita elementa 1 je $1^G = \{1, 4, 5, 8\}$. Vidimo, da je $1^G = 4^G = 5^G = 8^G$. Orbita elementa 2 je $2^G = \{2, 3, 6, 7\}$. Podobno kot prej je $2^G = 3^G = 6^G = 7^G$. Delovanje ima dve orbiti.

Stabilizator elementa 1 je $G_1 = \{\mathrm{id}, g_2 g_1\}$.

Lema 4.15. *Naj grupa G deluje na množici M in naj bo $x \in M$ poljuben. Če je G končna grupa, velja:*

$$|G| = |G_x| \cdot |x^G|.$$

Dokaz lahko bralec najde v [9].

Definicija 4.16. Delovanje grupe G na množici M je *tranzitivno*, če za poljubna elementa $x, y \in M$ obstaja element $g \in G$, tako da je $g(x) = y$.

Lahko tudi rečemo, da je delovanje tranzitivno, ko ima eno samo orbito.

Primer 4.17. Delovanje grupe $\mathbb{Z}_8$ na množici $\{0, 1, 2, 3\}$ iz primera 4.8 je tranzitivno delovanje. Delovanje grupe $\langle g_1, g_2 \rangle$ na množici $\{1, 2, \ldots, 8\}$ ni tranzitivno, saj ima dve orbiti.

Primer 4.18. S pomočjo leme 4.15 bomo poiskali grupo simetrij kocke (geometrijsko telo). To lahko storimo tako, da označimo oglišča kocke s števili od 1 do 8, kot vidimo na sliki 2. Vsaka simetrija kocke mora oglišča preslikati v oglišča, zato lahko grupo simetrij kocke obravnavamo kot podgrupo grupe S_8. Naj $G \leq S_8$ označuje celotno grupo simetrij kocke. Najprej bomo poiskali red grupe G.

Vzemimo permutaciji $\varphi_1 = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$ in $\varphi_2 = (1\ 5\ 8\ 4)(2\ 6\ 7\ 3)$. Permutaciji φ_1 in φ_2 sta elementa grupe G. Vemo, da $\langle \varphi_1, \varphi_2 \rangle \leq G$. Podgrupa $\langle \varphi_1, \varphi_2 \rangle$ deluje tranzitivno na množici $\{1, 2, \ldots, 8\}$. Orbita točke 1 je $1^{\langle \varphi_1, \varphi_2 \rangle} = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Dolžina orbite je 8. Uporabimo lemo 4.15:

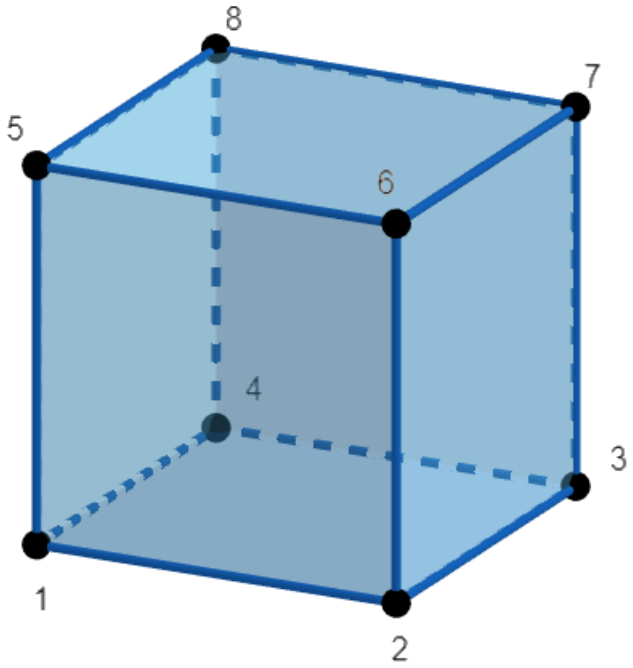
$$|G| = |G_1| \cdot |1^G| = |G_1| \cdot 8. \tag{4.1}$$

Zdaj pa si poglejmo stabilizator točke 1 v G. Ponovno uporabimo lemo 4.15 in dobimo

$$|G_1| = |(G_1)_2| \cdot |2^{G_1}|. \tag{4.2}$$

Podgrupa $(G_1)_2 = G_{(1,2)}$ stabilizira tako točko 1 kot tudi točko 2. Če enačbo (4.2) vstavimo v enačbo (4.1) dobimo

$$|G| = |G_{(1,2)}| \cdot |2^{G_1}| \cdot 8. \tag{4.3}$$



Slika 2: Kocka z označenimi oglišči.

Simetrije kocke robove slikajo v robove. Podgrupa G_1 lahko rob $(1,2)$ slika samo v $(1,2),(1,4)$ ali $(1,5)$. To pomeni, da $2^{G_1} \subseteq \{2,4,5\}$. Element $\varphi_3 = (2\ 5\ 4)(3\ 6\ 8) \in G_1$ pokaže, da $2^{G_1} = \{2,4,5\}$. Podgrupa $G_{(1,2)}$ fiksira rob $(1,2)$. Takšna simetrija je lahko rotacija okrog osi, ki vsebuje točki 1 in 2, ali pa zrcaljenje čez ravnino, ki vsebuje točki 1 in 2. Ni težko videti, da je stabilizator $G_{(1,2)} = \{\mathrm{id}, (4\ 5)(6\ 3)\}$. Iz tega sledi, da $|G| = |G_{(1,2)}| \cdot |2^{G_1}| \cdot 8 = 2 \cdot 3 \cdot 8 = 48$. Red grupe G je torej 48.

Izkaže se, da je $G = \langle (1\ 2\ 3\ 4)(5\ 6\ 7\ 8), (4\ 5)(6\ 3) \rangle$. To lahko preverimo s programskim paketom SageMath [14].

```
fi_1 = [(1, 2, 3, 4), (5, 6, 7, 8)]
fi_4 = [(4, 5), (6, 3)]
G = PermutationGroup([fi_1, fi_4])
print(G.order()) # 48
```

Definicija 4.19. Naj grupa G deluje na množici M in naj bo t naravno število. Delovanje je *t-tranzitivno*, če za poljubne paroma različne $x_1, x_2, \ldots, x_t \in M$ in poljubne paroma različne $y_1, y_2, \ldots, y_t \in M$ obstaja $g \in G$, da je $g(x_i) = y_i$ za vsak $1 \leq i \leq t$. Če za vsak $(x_1, x_2, \ldots, x_t)$ in vsak $(y_1, y_2, \ldots, y_t)$ obstaja natanko en tak g, gre za *strogo t-tranzitivno* delovanje.

Primer 4.20. Grupa simetrij kocke G iz primera 4.18 deluje na množici $\{1, 2, \ldots, 8\}$.

Videli smo že, da je delovanje 1-tranzitivno, ni pa 2-tranzitivno, saj noben element grupe G para $(1, 2)$ ne slika v $(1, 3)$.

5 Avtomorfizmi načrtov

To poglavje je posvečeno grupi avtomorfizmov načrta. Določimo red grupe avtomorfizmov Fanove ravnine in poiščemo generatorje te grupe. Nato pokažemo, da grupa avtomorfizmov načrta deluje zvesto na njegovih blokih. Na koncu poglavja predstavimo izrek, s katerim lahko iz t-tranzitivnega delovanja grupe na neki množici konstruiramo t-načrt.

Definicija 5.1. Naj bosta $(X, \mathcal{B})$ in $(X', \mathcal{B}')$ načrta. Preslikava $\varphi\colon X \to X'$ je *izomorfizem* načrtov, če je bijektivna in velja

$$\beta \in \mathcal{B} \iff \varphi(\beta) \in \mathcal{B}'.$$

Preslikavo φ razširimo na bloke načrta: če je $\beta = \{x_1, x_2, \ldots, x_k\}$, definiramo $\varphi(\beta) = \{\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_k)\}$.

Podobno, kot smo φ razširili na bloke, jo lahko raširimo tudi na množice blokov: če je $\{\beta_1, \beta_2, \ldots, \beta_m\}$ množica blokov, je $g(\{\beta_1, \beta_2, \ldots, \beta_m\}) = \{g(\beta_1), g(\beta_2), \ldots, g(\beta_m)\}$.

Primer 5.2. Vzemimo načrt iz primera 2.14 in načrt $(X', \mathcal{B}')$, kjer je $X' = \{A, B, C, D, E, F, G\}$ in

$$\mathcal{B}' = \{\{A, B, E\}, \{A, C, F\}, \{A, D, G\}, \{B, C, G\}, \{B, F, G\}, \{C, E, G\}, \{D, E, F\}\}.$$

Preslikava φ, ki je definirana s tabelo

x	1	2	3	4	5	6	7
$\varphi(x)$	A	B	E	C	F	G	D

je izomorfizem načrtov $(X, \mathcal{B})$ in $(X', \mathcal{B}')$. Res, $\varphi(\{1, 2, 3\}) = \{A, B, E\}$, $\varphi(\{1, 4, 5\}) = \{A, C, F\}, \varphi(\{1, 6, 7\}) = \{A, D, G\}, \ldots$.

Definicija 5.3. Naj bo φ preslikava kot v definiciji 5.1. Če je $(X, \mathcal{B}) = (X', \mathcal{B}')$, potem preslikavi φ pravimo *avtomorfizem* načrta $(X, \mathcal{B})$.

Avtomorfizem načrta $(X, \mathcal{B})$ je torej takšna permutacija π na množici X, za katero velja

$$\beta \in \mathcal{B} \iff \pi(\beta) \in \mathcal{B}. \tag{5.1}$$

Primer 5.4. Naj bo $(X, \mathcal{B})$ Fanova ravnina iz primera 2.14. Permutacije $\varphi_1 = \mathrm{id}_X, \varphi_2 = (4\ 5)(6\ 7)$ in $\varphi_3 = (1\ 5\ 6)(2\ 7\ 4)$ so avtomorfizmi načrta $(X, \mathcal{B})$. Naj bo $\varphi_4 = \varphi_2 * \varphi_3 = (1\ 5\ 2\ 7)(4\ 6)$ in $\varphi_5 = \varphi_3 * \varphi_2 = \varphi_2 \circ \varphi_3 = (1\ 4\ 2\ 6)(5\ 7)$. Lahko se prepričamo, da sta tudi φ_4 in φ_5 avtomorfizma načrta $(X, \mathcal{B})$.

Ni vsaka permutacija na X avtomorfizem načrta. Na primer, $\varphi_6 = (1\ 3\ 2\ 5)(4\ 6\ 7)$ ni avtomorfizem načrta $(X, \mathcal{B})$, saj $\varphi(\{1, 2, 3\}) = \{2, 3, 5\} \notin \mathcal{B}$.

Množico vseh avtomorfizmov načrta $(X, \mathcal{B})$ označimo z $\mathrm{Aut}(X, \mathcal{B})$. Očitno je $\mathrm{Aut}(X, \mathcal{B}) \subseteq \mathrm{Sym}(X)$.

Trditev 5.5. *Naj bo $(X, \mathcal{B})$ načrt. Potem je $\mathrm{Aut}(X, \mathcal{B})$ podgrupa grupe $\mathrm{Sym}(X)$.*

Dokaz. Očitno je $\mathrm{id}_X \in \mathrm{Aut}(X, \mathcal{B})$.

Pokažimo, da je $\mathrm{Aut}(X, \mathcal{B})$ zaprta za invertiranje. Naj bo $\beta \in \mathcal{B}$. Denimo, da $\varphi^{-1}(\beta) \notin \mathcal{B}$. Iz (5.1) sledi

$$\beta \notin \mathcal{B} \iff \pi(\beta) \notin \mathcal{B}. \tag{5.2}$$

Iz (5.2) sledi $\varphi(\varphi^{-1}(\beta)) = \beta \notin \mathcal{B}$, protislovje. Torej $\beta \in \mathcal{B} \Longrightarrow \varphi^{-1}(\beta) \in \mathcal{B}$.

Naj bo $\varphi^{-1}(\beta) \in \mathcal{B}$. Iz (5.1) sledi $\varphi(\varphi^{-1}(\beta)) = \beta \in \mathcal{B}$. Torej $\varphi^{-1}(\beta) \in \mathcal{B} \Longrightarrow \beta \in \mathcal{B}$. Res, inverzi avtomorfizmov so tudi avtomorfizmi.

Pokažimo zaprtost za množenje avtomorfizmov. Naj bosta φ in ψ avtomorfizma načrta $(X, \mathcal{B})$. Naj bo $\beta \in \mathcal{B}$. Iz (5.1) sledi $\varphi(\beta) \in \mathcal{B}$. Iz (5.1) sledi še $\psi(\varphi(\beta)) = (\varphi * \psi)(\beta) \in \mathcal{B}$. Naj bo $(\varphi * \psi)(\beta) \in \mathcal{B}$. Pokazali smo že, da so inverzi avtomorfizmov tudi avtomorfizmi. Potem je $\psi^{-1}(\psi(\varphi(\beta))) = \varphi(\beta) \in \mathcal{B}$. Potem je $\varphi^{-1}(\varphi(\beta)) = \beta \in \mathcal{B}$. □

Primer 5.6. Naj bo $(X, \mathcal{B})$ Fanova ravnina iz primera 2.14. Grupa avtomorfizmov Fanove ravnine $G = \mathrm{Aut}(X, \mathcal{B})$ deluje na množici $\{1, 2, 3, 4, 5, 6, 7\}$. Radi bi ugotovili red grupe G. Pomagali si bomo z lemo 4.15:

$$|G| = |G_1| \cdot |1^G|. \tag{5.3}$$

Permutaciji $\varphi_1 = (1\ 5\ 2\ 7)(4\ 6)$ in $\varphi_2 = (1\ 3\ 5\ 6)(2\ 7)$ sta avtomorfizma Fanove ravnine. Vidimo, da je $1^G = \{1, 2, 3, 4, 5, 6, 7\}$. Dolžina orbite je 7. Iz enačbe (5.3) sledi

$$|G| = |G_1| \cdot 7. \tag{5.4}$$

Ponovno uporabimo lemo 4.15 in dobimo

$$|G_1| = |G_{(1,2)}| \cdot |2^{G_1}|. \tag{5.5}$$

Če enačbo (5.5) vstavimo v enačbo (5.4) dobimo

$$|G| = |G_{(1,2)}| \cdot |2^{G_1}| \cdot 7. \tag{5.6}$$

Elementa $\varphi_3 = (2\ 4\ 6)(3\ 5\ 7) \in G_1$ in $\varphi_4 = (2\ 5\ 7)(3\ 4\ 6) \in G_1$ pokažeta, da $2^{G_1} = \{2, 3, 4, 5, 6, 7\}$. Torej, $|2^{G_1}| = 6$. Ni težko videti, da je $G_{(1,2)} = G_{(1,2,3)}$. Ponovno uporabimo 4.15:

$$|G_{(1,2)}| = |G_{(1,2,3)}| = |G_{(1,2,3,4)}| \cdot |4^{G_{(1,2,3)}}|. \tag{5.7}$$

Elementa $\varphi_5 = (4\ 6)(5\ 7) \in G_{(1,2,3)}$ in $\varphi_6 = (4\ 5)(6\ 7) \in G_{(1,2,3)}$ pokažeta, da $4^{G_{(1,2,3)}} = \{4, 5, 6, 7\}$. Torej, $|4^{G_{(1,2,3)}}| = 4$. Ni težko videti, da je grupa $G_{(1,2,3,4)}$ trivialna. Enačbo (5.7) vstavimo v enačbo (5.6) in dobimo:

$$|G| = |G_{(1,2,3,4)}| \cdot |4^{G_{(1,2,3)}}| \cdot |2^{G_1}| \cdot 7 = 1 \cdot 4 \cdot 6 \cdot 7 = 168. \tag{5.8}$$

Red grupe G je torej 168. Izkaže se, da je $G = \langle (1\ 5\ 2\ 7)(4\ 6), (1\ 3\ 5\ 6)(2\ 7) \rangle$. To lahko preverimo s programskim paketom SageMath [14].

```
fi_1 = [(1, 5, 2, 7), (4, 6)]
fi_2 = [(1, 3, 5, 6), (2, 7)]
G = PermutationGroup([fi_1, fi_2])
print(G.order()) # 168
```

Lema 5.7. *Naj bo $(X, \mathcal{B})$ t-načrt za $t \geq 2$. Tedaj grupa avtomorfizmov načrta $(X, \mathcal{B})$ deluje zvesto na $\mathcal{B}$.*

Dokaz. Naj bo $g \in \mathrm{Aut}(X, \mathcal{B})$ poljuben avtomorfizem, tako da $g(\beta) = \beta$ za vsak $\beta \in \mathcal{B}$.

Naj bo x poljubna točka. Označimo $\mathrm{st}(x) = \{\gamma_1, \gamma_2, \ldots, \gamma_{\lambda_1}\}$. Potem je

$$\begin{aligned} g(\mathrm{st}(x)) &= g(\{\gamma_1, \gamma_2, \ldots, \gamma_{\lambda_1}\}) = \{g(\gamma_1), g(\gamma_2), \ldots, g(\gamma_{\lambda_1})\} \\ &= \{\gamma_1, \gamma_2, \ldots, \gamma_{\lambda_1}\} = \mathrm{st}(x). \end{aligned}$$

Pokažimo še, da je $\mathrm{st}(g(x)) = g(\mathrm{st}(x))$. Če je $\beta \in \mathrm{st}(x)$, potem je oblike $\beta = \{x, y_2, \ldots, y_k\}$. Ker je g avtomorfizem, je $g(\beta) = \{g(x), g(y_2), \ldots, g(y_k)\} \in \mathcal{B}$. Ker $g(x) \in g(\beta)$, je $g(\beta) \in \mathrm{st}(g(x))$. Pokazali smo $g(\mathrm{st}(x)) \subseteq \mathrm{st}(g(x))$.

Če je $\beta \in \mathrm{st}(g(x))$, potem je oblike $\beta = \{g(x), z_2, \ldots, z_k\}$. Ker je g avtomorfizem, je $g^{-1}(\beta) = \{x, g^{-1}(z_2), \ldots, g^{-1}(z_k)\} \in \mathcal{B}$. Ker je $x \in g^{-1}(\beta)$ je $g^{-1}(\beta) \in \mathrm{st}(x)$. Torej $\beta = g(g^{-1}(\beta))$, kjer je $g^{-1}(\beta) \in \mathrm{st}(x)$. Pokazali smo $\mathrm{st}(g(x)) \subseteq g(\mathrm{st}(x))$.

Pokazali smo $\mathrm{st}(g(x)) = g(\mathrm{st}(x))$, že od prej vemo $g(\mathrm{st}(x)) = \mathrm{st}(x)$. Torej $\mathrm{st}(g(x)) = \mathrm{st}(x)$, tj. x in $g(x)$ imata enaki zvezdi.

Denimo, da $g(x) \neq x$. Vemo, da je $|\mathrm{st}(x)| = \lambda_1 = r$. Ker je $\mathrm{st}(x) = g(\mathrm{st}(x))$, so v $\mathrm{st}(x)$ natanko tisti bloki, ki vsebujejo x in $g(x)$, teh pa je ravno λ_2. Torej, $|\mathrm{st}(x)| = \lambda_1 = \lambda_2$. Uporabimo posledico 2.8 za $i = 1$ in dobimo:

$$\begin{aligned} (v-1)\lambda_2 &= (k-1)\lambda_1 \\ v - 1 &= k - 1 \\ v &= k \end{aligned}$$

Po definiciji načrta to ni dovoljeno, protislovje. To pomeni, da $g(x) = x$. Ker je x poljubna točka, je $g = \mathrm{id}_X$. □

Izrek 5.8. *Naj bo $t \geq 2$ in G permutacijska grupa, ki deluje t-tranzitivno na X. Naj bo $|X| = v$ in naj bo β podmnožica množice X, da je $|\beta| = k$ za $1 < k < v - 1$. Potem je $\mathcal{B} = \{g(\beta) : g \in G\}$ množica blokov t-načrta $(X, \mathcal{B})$, G je grupa avtomorfizmov, ki deluje tranzitivno na $\mathcal{B}$.*

Dokaz. Pokazali bomo, da sta vsaki dve t-podmnožici množice X vsebovani v istem številu blokov. Naj bosta S in T t-podmnožici množice X. Ker G deluje t-tranzitivno na X, obstaja tak $h \in G$, da $h(S) = T$. Vsak blok je oblike $g(\beta)$ za nek $g \in G$. Iz $S \subseteq g(\beta)$ sledi $h(S) = T \subseteq h(g(\beta)) = (g * h)(\beta)$. Iz $T \subseteq g(\beta)$ sledi $h^{-1}(T) = S \subseteq h^{-1}(g(\beta)) = (g * h^{-1})(\beta)$. Torej $S \subseteq g(\beta) \iff T \subseteq (g * h)(\beta)$. Od tod sledi, da sta S in T vsebovani v istem številu blokov. □

Primer 5.9. Naj bodo

$$\begin{aligned}
\pi_1 &= (1\ 2\ 3)(4\ 5\ 6),\\
\pi_2 &= (1\ 2)(5\ 6)(7\ 9),\\
\pi_3 &= (1\ 4)(2\ 6)(3\ 5)\\
\pi_4 &= (1\ 7)(2\ 5)(4\ 8),\\
\pi_5 &= (2\ 3)(5\ 6)(7\ 8).
\end{aligned}$$

Grupa $G = \langle \pi_1, \pi_2, \ldots, \pi_5 \rangle \leq S_9$ deluje na množici $X = \{1, 2, \ldots, 9\}$. S pomočjo SageMath lahko preverimo, da je G grupa reda 432 in da G deluje 2-tranzitivno na množici X.

```
pi_1 = [(1, 2, 3), (4, 5, 6)]
pi_2 = [(1, 4), (3, 5), (2, 6)]
pi_3 = [(7, 8), (3, 2), (5, 6)]
pi_4 = [(7, 1), (8, 4), (2, 5)]
pi_5 = [(9, 7), (1, 2), (5, 6)]
G = PermutationGroup([pi_1, pi_2, pi_3, pi_4, pi_5])
print(G.order()) # 432
print(G.orbit(1)) # (1, 3, 2, 4, 5, 6, 9, 7, 8)
G_1 = G.stabilizer(1)
print(G_1.orbit(2)) # (2, 3, 6, 7, 5, 8, 9, 4)
```

Izberimo si $\beta = \{1, 2, 3\}$. Po izreku 5.8 dobimo, da so bloki načrta

$$\begin{aligned}
\mathcal{B} = \{&\{1,2,3\}, \{1,4,9\}, \{1,5,8\}, \{1,6,7\}, \{2,4,7\}, \{2,5,9\},\\
&\{2,6,8\}, \{3,4,8\}, \{3,5,7\}, \{3,6,9\}, \{4,5,6\}, \{7,8,9\}\}.
\end{aligned}$$

Par $(X, \mathcal{B})$ je 2-$(9, 3, 1)$ načrt. Ker je red grupe 432, smo si pri iskanju blokov pomagali s programom v SageMath.

```
vsi_bloki = []
beta = [1, 2, 3]
for g in G:
    nov_blok = []
    for x in beta:
        nov_blok.append(g(x))
    nov_blok.sort()
    if nov_blok not in vsi_bloki:
        vsi_bloki.append(nov_blok)
vsi_bloki.sort()
print(vsi_bloki)
```

6 Skrčitve in razširitve načrtov

V tem poglavju predstavimo skrčitve in razširitve načrtov. Načrt "skrčimo" tako, da odstranimo eno od njegovih točk ter temu ustrezno popravimo tudi množico njegovih blokov. Načrt "razširimo" tako, da mu dodamo novo točko, hkrati pa mu dodamo nove bloke ter dodamo novo točko obstoječim blokom. Izkaže se, da ni mogoče razširiti kar vsakega načrta. Videli bomo, da načrta s parametri 3-$(8, 4, 1)$ in 2-$(13, 4, 1)$ nista razširljiva.

Trditev 6.1. *Naj bo $D = (X, \mathcal{B})$ t-(v, k, λ) načrt in $x \in X$ poljubna točka. Naj bo*

$$\mathcal{B}_x = \{\beta \setminus \{x\} : \beta \in \mathcal{B}, x \in \beta\}.$$

Par $(X \setminus \{x\}, \mathcal{B}_x)$ je načrt s parametri $(t-1)$-$(v-1, k-1, \lambda)$.

Dokaz te trditve je za primer, ko je $t = 3$, že vsebovan v dokazu izreka 3.2. Dokaz v splošnem poteka na enak način.

Definicija 6.2. Naj bo $D = (X, \mathcal{B})$ načrt in $x \in X$ poljubna točka. Načrtu $(X \setminus \{x\}, \mathcal{B}_x)$ pravimo *skrčitev* načrta D in ga označimo z D_x.

Primer 6.3. Naj bo $X = \{1, 2, \ldots, 8\}$ množica točk in naj bo

$$\begin{aligned}\mathcal{B} = \{&\{1,2,3,4\},\{1,2,5,6\},\{1,2,7,8\},\{1,3,5,7\},\{1,3,6,8\},\{1,4,5,8\},\{1,4,6,7\},\\ &\{2,3,5,8\},\{2,3,6,7\},\{2,4,5,7\},\{2,4,6,8\},\{3,4,5,6\},\{3,4,7,8\},\{5,6,7,8\}\}\end{aligned}$$

množica blokov. Par $(X, \mathcal{B})$ je 3-$(8, 4, 1)$ načrt. Iz množice X odstranimo točko $x = 8$. Bloki skrčitve so:

$$\mathcal{B}_8 = \{\{1,2,7\},\{1,3,6\},\{1,4,5\},\{2,3,5\},\{2,4,6\},\{3,4,7\},\{5,6,7\}\}.$$

Načrt $(X \setminus \{8\}, \mathcal{B}_8)$ je izomorfen Fanovi ravnini. Permutacija (3 7 6) je izomorfizem med $(X \setminus \{8\}, \mathcal{B}_8)$ in Fanovo ravnino iz primera 2.14.

Trditev 6.4. *Naj bo $D = (X, \mathcal{B})$ načrt s parametri t-(v, k, λ) in naj bo D_x njegova skrčitev. Naj b označuje število blokov načrta D, b_x pa število blokov načrta D_x. Potem velja:*

$$b_x = \frac{bk}{v}.$$

Dokaz. Iz definicije $\mathcal{B}_x$ sledi, da je $b_x = |\mathcal{B}_x| = \lambda_1 = r$. V enačbo (2.7) vstavimo $b_x = r$, pa dobimo $vb_x = bk$ od koder sledi trditev. □

Definicija 6.5. Načrt $D^+ = (X^+, \mathcal{B}^+)$ je *razširitev* načrta $D = (X, \mathcal{B})$, če velja:

1. $X^+ = X \cup \{z\}$ za nek $z \notin X$;
2. $(D^+)_z = D$ (tj. načrt D je skrčitev načrta D^+, pri čemer smo odstranili točko z).

Definicija 6.6. Pravimo, da je načrt $D = (X, \mathcal{B})$ *razširljiv*, če obstaja vsaj en načrt D^+, tako da je D^+ razširitev načrta D.

Primer 6.7. Načrt iz primera 6.3 je razširitev Fanove ravnine. Fanova ravnina je razširljiv načrt.

Lema 6.8. *Naj bo $(X, \mathcal{B})$ t-(v, k, λ) načrt z b bloki. Če je načrt $(X, \mathcal{B})$ razširljiv, potem velja:*

$$k + 1 \mid b(v + 1).$$

Dokaz. Naj bo $(X^+, \mathcal{B}^+)$ razširitev načrta $(X, \mathcal{B})$. Po trditvi 6.1 je $(X^+, \mathcal{B}^+)$ načrt s parametri $(t + 1)$-$(v + 1, k + 1, \lambda)$ in z b^+ bloki. Po trditvi 6.4 je $b = \frac{b^+(k+1)}{v+1}$. Od tod $b^+ = \frac{b(v+1)}{k+1}$. Ker je b^+ celo število, sledi da $k + 1 \mid b(v + 1)$. □

Primer 6.9. Naj bo $(X, \mathcal{B})$ načrt s parametri 3-$(8, 4, 1)$ iz primera 6.3. Če bi bil načrt raširljiv, bi po lemi 6.8 moralo veljati $4 + 1 \mid 14 \cdot 9$, tj. $5 \mid 2 \cdot 3^2 \cdot 7$. To pa ne velja, torej načrt $(X, \mathcal{B})$ iz primera 6.3 ni razširljiv.

Izrek 6.10. *Naj bo q potenca praštevila. Če je načrt s parametri 2-$(q^2 + q + 1, q + 1, 1)$ razširljiv, potem je $q = 2$ ali $q = 2^2$.*

Dokaz. Iz leme 6.8 sledi, da $q + 2$ deli $(q^2 + q + 1)(q^2 + q + 2)$. To pomeni, da je

$$\begin{aligned}\frac{(q^2 + q + 1)(q^2 + q + 2)}{q + 2} &= \frac{q^4 + 2q^3 + 4q^2 + 3q + 2}{q + 2} \\ &= q^3 + 4q - 5 + \frac{12}{q + 2}\end{aligned}$$

celo število. Od tod sledi, da je tudi $\frac{12}{q+2}$ celo število. Deljitelji števila 12 so: $1, 2, 3, 4, 6$ in 12. Število $q + 2$ mora biti enako enemu od teh deliteljev. Iz $q + 2 = 4$ sledi $q = 2$, iz $q + 2 = 6$ pa sledi $q = 4 = 2^2$. Ostali delitelji ne pridejo v poštev, saj je q po predpostavki potenca praštevila. Na primer, iz $q + 2 = 12$ sledi $q = 10 = 2 \cdot 5$, kar ni potenca praštevila. □

Primer 6.11. Naj bo $X = \{1, 2, \ldots, 13\}$ množica točk in naj bo

$$\begin{aligned}\mathcal{B} = \{&\{1,2,3,4\},\{1,5,6,7\},\{1,8,9,10\},\{1,11,12,13\},\{2,5,8,11\},\\ &\{2,6,9,12\},\{2,7,10,13\},\{3,5,10,12\},\{3,6,8,13\},\{3,7,9,11\},\\ &\{4,5,9,13\},\{4,6,10,11\},\{4,7,8,12\}\}\end{aligned}$$

množica blokov. $(X, \mathcal{B})$ je načrt s parametri 2-$(13, 4, 1)$. Načrt zadošča predpostavkam izreka 6.10, saj je $q = 3$ potenca praštevila. Izrek nam pove, da načrt ni razširljiv.

7 Hadamardove matrike in načrti

To poglavje je posvečeno Hadamardovim matrikam. To so matrike s koeficienti iz $\{-1, 1\}$, katerih vrstice (in tudi stolpci) so ortogonalne. Najprej si ogledamo nekaj operacij na matrikah, ki iz Hadamardove matrike ponovno naredijo Hadamardovo matriko. Nato pokažemo, da je red Hadamardove matrike večkratnik števila 4, čim je večji od 2. Pokažemo, da lahko iz normalizirane Hadamardove matrike reda $4\lambda + 4$ dobimo simetrični načrt s parametri 2-$(4\lambda+3, 2\lambda+1, \lambda)$. Velja tudi obratno, iz vsakega takšnega načrta lahko dobimo normalizirano Hadamardovo matriko. To ponazorimo s konkretnimi primeri.

Definicija 7.1. Naj bo $H = (h_{i,j})_{1\leq i,j\leq n}$ $n \times n$ matrika s koeficienti iz $\{-1, 1\}$ (tj. $h_{i,j} \in \{-1, 1\}$ za vsak $1 \leq i, j \leq n$). Matrika H je *Hadamardova matrika reda n*, če velja:

$$HH^T = nI_{n\times n}. \tag{7.1}$$

Primer 7.2. Naj bodo

$$H_1 = \begin{bmatrix} 1 \end{bmatrix}, \qquad H_2 = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}, \qquad H_4 = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}.$$

Ni težko videti, da matrike H_1, H_2 in H_4 ustrezajo pogoju (7.1), torej so Hadamardove matrike.

Iz definicije produkta matrik dobimo

$$(HH^T)_{i,j} = h_{i,1}h_{j,1} + h_{i,2}h_{j,2} + h_{i,3}h_{j,3} + \cdots + h_{i,n}h_{j,n} = \sum_{k=1}^{n} h_{i,k}h_{j,k}. \tag{7.2}$$

Če je $i = j$, dobimo $\sum_{k=1}^{n} h_{i,k}h_{j,k} = \sum_{k=1}^{n} h_{i,k}^2 = \sum_{k=1}^{n} 1 = n$ (saj so koeficienti iz $\{-1, 1\}$, torej je $h_{i,j}^2 = 1$ za vse $1 \leq i, j \leq n$). Če je $i \neq j$, pa imamo $\sum_{k=1}^{n} h_{i,k}h_{j,k} = 0$. Izraz $\sum_{k=1}^{n} h_{i,k}h_{j,k}$ je (standardni) skalarni produkt i-te in j-te vrstice matrike H. To pomeni, da so vrstice matrike H *ortogonalne*.

Trditev 7.3. *Naj bo H Hadamardova matrika. Matrika, ki jo dobimo iz H z eno od naslednjih operacij, je tudi Hadamardova:*

(i) medsebojna zamenjava dveh vrstic;

(ii) množenje vrstice z -1;

(iii) medsebojna zamenjava dveh stolpcev;

(iv) množenje stolpca z -1;

(v) transponiranje.

Dokaz. (i): Pogoj (7.1) pomeni, da so vrstice matrike H ortogonalne. Menjava vrstnega reda vrstic ne vpliva na njihovo ortogonalnost.

(ii): Iz linearne algebre vemo, da dva vektorja ostaneta ortogonalna, če enega izmed njiju pomnožimo s skalarjem.

(v): Iz (7.1) sledi $\det(H) \cdot \det(H^T) = \det(HH^T) = n^n \neq 0$. To pomeni, da je $\det(H) \neq 0$, se pravi H^{-1} obstaja. Če (7.1) z leve pomnožimo z H^{-1}, dobimo $H^T = nH^{-1}$. Torej,

$$H^T(H^T)^T = H^T H = nH^{-1}H = nI_{n\times n}.$$

Res, H^T je tudi Hadamardova.

(iii): Sledi iz (i) in (v). (Če matriko transponiramo, zamenjamo med seboj dve vrstici in jo nato ponovno transponiramo, je to enako, kot če bi med seboj zamenjali dva stolpca.)

(iv): Sledi iz (ii) in (v). □

Iz trditve 7.3 sledi, da so tudi stolpci Hadamardove matrike ortogonalni.

Posledica 7.4. *Naj bo H Hadamardova matrika. Matrika, ki jo dobimo iz H s poljubnim številom operacij iz trditve 7.3 v poljubnem vrstnem redu, je tudi Hadamardova.*

Dokaz. Sledi direktno iz trditve 7.3. □

V primeru 7.2 smo si ogledali tri majhne primere Hadamardovih matrik, med katerim pa ni bilo matrike velikosti 3×3. Naslednja trditev bo povedala, da takšne matrike ne obstajajo.

Trditev 7.5. *Naj bo H Hadamardova matrika reda n, kjer je $n > 2$. Potem $4 \mid n$.*

Dokaz. Predpostavimo lahko, da so vsi elementi v prvem stolpcu matrike H enaki 1 (zaradi trditve 7.3). Vsaka vrstice matrike H je enega od naslednjih štirih tipov:

(T1) vrstica oblike $\begin{bmatrix} 1 & 1 & 1 & \dots \end{bmatrix}$;

(T2) vrstica oblike $\begin{bmatrix} 1 & 1 & -1 & \dots \end{bmatrix}$;

(T3) vrstica oblike $\begin{bmatrix} 1 & -1 & 1 & \dots \end{bmatrix}$;

(T4) vrstica oblike $\begin{bmatrix} 1 & -1 & -1 & \dots \end{bmatrix}$.

Zaradi trditve 7.3 lahko predpostavimo, da je prvih a vrstic matrike H tipa (T1), tem sledi b vrstic tipa (T2), naslednjih c vrstic je tipa (T3), zadnjih d vrstic pa tipa (T4). Velja:

$$a + b + c + d = n, \tag{7.3}$$

$$a + b - c - d = 0, \tag{7.4}$$

$$a - b + c - d = 0, \tag{7.5}$$

$$a - b - c + d = 0. \tag{7.6}$$

Enačba (7.3) velja, ker ima matrika H n vrstic. Enačbo (7.4) dobimo, če izračunamo skalarni produkt prvih dveh stolpcev matrike H. Podobno, enačbo (7.5) dobimo, tako da izračunamo skalarni produkt prvega in tretjega stolpca matrike H. Prav tako enačbo (7.6) dobimo, če izračunamo skalarni produkt drugega in tretjega stolpca matrike H. Če seštejemo enačbi (7.3) in (7.4) dobimo

$$2a + 2b = n. \tag{7.7}$$

Če seštejemo enačbi (7.5) in (7.6) dobimo

$$2a - 2b = 0. \tag{7.8}$$

Če seštejemo enačbi (7.7) in (7.8) dobimo $4a = n$. To pomeni, da 4 deli n. Poleg tega vidimo tudi, da je vrstic tipa (T1) natanko $\frac{n}{4}$. □

Definicija 7.6. Hadamardova matrika je *normalizirana*, če so vsi elementi v prvi vrstici in v prvem stolpcu enaki 1.

Trditev 7.3 nam pove, da lahko vsako Hadamardovo matriko pretvorimo v normalizirano Hadamardovo matriko.

Izrek 7.7 (Naloga 3.7.1 v [1])**.** *Naj bo H normalizirana Hadamardova matrika reda $n = 4\lambda + 4$, kjer je $\lambda \geq 1$. Naj bo A matrika, ki jo dobimo iz matrike H, tako da ji odstranimo prvi stolpec in prvo vrstico ter vse elemente -1 nadomestimo z 0. Potem je A incidenčna matrika simetričnega načrta s parametri* $2\text{-}(4\lambda + 3, 2\lambda + 1, \lambda)$.

Dokaz. Naj bo $X = \{x_2, x_3, \ldots, x_n\}$ in naj bo $\mathcal{B} = \{\beta_2, \beta_3, \ldots, \beta_n\}$ družina podmnožic množice X, kjer velja naslednje:

$$x_i \in \beta_j \iff h_{i,j} = 1. \tag{7.9}$$

Incidenčna struktura $(X, \mathcal{B})$ pripada incidenčni matriki A. Naj bo j poljubno število, za katero velja $2 \leq j \leq n$. Naj bo a_j število elementov 1 v j-tem stolpcu in naj bo b_j število elementov -1 v j-tem stolpcu. Če izračunamo skalarni produkt prvega in j-tega stolpca, dobimo $a_j - b_j = 0$, torej $a_j = b_j = \frac{n}{2}$. To pomeni, da je $|\beta_j| = \frac{n}{2} - 1 = \frac{4\lambda+4}{2} - 1 = 2\lambda + 2 - 1 = 2\lambda + 1$.

Pokažimo še, da se vsak par točk pojavi v natanko λ blokih. Brez škode za splošnost si oglejmo par $\{x_2, x_3\}$. Ta par bo vsebovan v bloku β_j, če bo $h_{2,j} = h_{3,j} = 1$. Štejemo torej stolpce, ki imajo v drugi in tretji vrstici element 1. To pa je isto, kot če bi v matriki H^T šteli vrstice tipa (T1), kot v dokazu trditve 7.5. V dokazu trditve 7.5 smo videli, da je takih vrstic natanko $\frac{n}{4}$. Med stolpci matrike H, za katere velja $h_{2,j} = h_{3,j} = 1$, je tudi njen prvi stolpec, ki ne pripada incidenčni matriki. Blokov, ki vsebujejo par $\{x_2, x_3\}$, je torej $\frac{n}{4} - 1 = \frac{4\lambda+4}{4} - 1 = \lambda$.

Očitno je $|X| = n - 1 = 4\lambda + 4 - 1 = 4\lambda + 3$. Incidenčna struktura $(X, \mathcal{B})$ je torej načrt s parametri 2-$(4\lambda + 3, 2\lambda + 1, \lambda)$. □

Izrek 7.7 nam pove, da lahko iz Hadamardove matrike, ki je reda 8 ali več, dobimo simetričen 2-$(4\lambda + 3, 2\lambda + 1, \lambda)$ načrt. To osmisli naslednjo definicijo.

Definicija 7.8. Simetričnemu načrtu s parametri 2-$(4\lambda + 3, 2\lambda + 1, \lambda)$ pravimo *Hadamardov načrt*.

Primer 7.9. Vzemimo matriko

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

Matrika H je normalizirana Hadamardova matrika. Če matriki H odstranimo prvo

vrstico in prvi stolpec ter elemente -1 zamenjamo z 0, dobimo matriko

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

Incidenčni matriki A pripada načrt $(X, \mathcal{B})$, kjer je $X = \{1, 2, \ldots, 7\}$ in

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

Načrt $(X, \mathcal{B})$ je izomorfen Fanovi ravnini iz primera 2.14. Permutacija (6 7) je izomorfizem med $(X, \mathcal{B})$ in Fanovo ravnino iz primera 2.14.

Primer 7.10. Naj bo

$$H_{12} = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \end{bmatrix}.$$

Če vsak stolpec matrike H_{12}, razen prvega, pomnožimo z -1, dobimo normalizirano

Hadamardovo matriko

$$\widetilde{H}_{12} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \end{bmatrix}.$$

Če matriki $\widetilde{H}_{12}$ odstranimo prvo vrstico in prvi stolpec ter elemente -1 zamenjamo z 0, dobimo matriko

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

Incidenčni matriki A pripada načrt $(X, \mathcal{B})$, kjer je $X = \{1, 2, \ldots, 11\}$ in

$$\begin{aligned} \mathcal{B} = \{&\{3,7,8,9,11\},\{1,4,8,9,10\},\{2,5,9,10,11\},\{1,3,6,10,11\},\\ &\{1,2,4,7,11\},\{1,2,3,5,8\},\{2,3,4,6,9\},\{3,4,5,7,10\},\\ &\{4,5,6,8,11\},\{1,5,6,7,9\},\{2,6,7,8,10\}\}. \end{aligned}$$

$(X, \mathcal{B})$ je načrt s parametri 2-$(11, 5, 2)$, ki je izomorfen načrtu iz primera 2.2. Permutacija (3 11 10 5 6 8 9 4) je izomorfizem med $(X, \mathcal{B})$ in načrtom iz primera 2.2.

Izrek 7.11 (Naloga 3.7.2 v [1])**.** *Naj bo* $(X, \mathcal{B})$ *načrt s parametri* 2-$(4\lambda + 3, 2\lambda + 1, \lambda)$, *kjer je* $\lambda \geq 1$, $X = \{x_2, x_3, \ldots, x_{4\lambda+4}\}$ *in* $\mathcal{B} = \{\beta_2, \beta_3, \ldots, \beta_{4\lambda+4}\}$. *Naj bo* $H =$

$(h_{i,j})_{1\leq i,j\leq 4\lambda+4}$ *matrika definirana z*

$$h_{i,j} = \begin{cases} 1, & \text{če } i = 1 \text{ ali } j = 1; \\ 1, & \text{če je } i,j \geq 2 \text{ in } x_i \in \beta_j; \\ -1, & \text{sicer.} \end{cases}$$

Potem je H normalizirana Hadamardova matrika reda $4\lambda + 4$.

Dokaz. Pokazati moramo, da je skalarni produkt poljubnih dveh različnih vrstic (i-te in j-te) enak 0.

Najprej obravnavajmo primer, ko je $i, j \geq 2$. Ker je $(X, \mathcal{B})$ 2-načrt, se vsak par različnih točk pojavi v λ blokih. Ker je načrt simetričen, je $r = 2\lambda + 1$. Torej, vsaka točka se pojavi v $2\lambda + 1$ blokih. Bloke lahko razdelimo v štiri skupine:

(i) blokov, ki vsebujejo x_i in x_j, je λ, pripadajoči stolpci pa vsebujejo element 1 v i-ti in j-ti vrstici;

(ii) blokov, ki vsebujejo x_i in ne vsebujejo x_j, je $2\lambda + 1 - \lambda = \lambda + 1$, pripadajoči stolpci pa vsebujejo element 1 oz. -1 v i-ti oz. j-ti vrstici;

(iii) blokov, ki ne vsebujejo x_i in vsebujejo x_j, je $2\lambda + 1 - \lambda = \lambda + 1$, pripadajoči stolpci pa vsebujejo element -1 oz. 1 v i-ti oz. j-ti vrstici;

(iv) blokov, ki ne vsebujejo x_i niti x_j, je $4\lambda + 3 - (3\lambda + 2) = \lambda + 1$, pripadajoči stolpci pa vsebujejo element -1 v i-ti in j-ti vrstici.

Prvi stolpec matrike H, ki vsebuje same enke, ne pripada nobenemu bloku načrta. Zdaj lahko izračunamo skalarni produkt i-te in j-te vrstice:

$$\sum_{k=1}^{4\lambda+4} h_{i,k} \cdot h_{j,k} = 1 + \lambda - (\lambda + 1) - (\lambda + 1) + (\lambda + 1) = 0. \tag{7.10}$$

Skalarni produkt dveh različnih vrstic je enak 0, torej je H res Hadamardova matrika.

Obravnavajmo primer, ko je $i = 1$ in $j \geq 2$. Ker je $h_{1,k} = 1$ za vse k, dobimo

$$\sum_{k=1}^{4\lambda+4} h_{1,k} \cdot h_{j,k} = \sum_{k=1}^{4\lambda+4} h_{j,k} = 1 + (2\lambda + 1) - (2\lambda + 2) = 0. \tag{7.11}$$

Utemeljimo, da velja drugi enačaj v 7.11. Velja $h_{j,1} = 1$. Med števili $h_{j,2}, \ldots, h_{j,4\lambda+4}$ je $2\lambda + 1$ enic, saj je točka x_j vsebovana v natanko $2\lambda + 1$ blokih, ostala števila pa so -1.

Iz definicije matrike H je očitno, da je normalizirana. □

Primer 7.12 (Naloga 3.7.3 v [1])**.** Naj bo $(X, \mathcal{B})$ načrt, kjer so točke načrta $X = \{1, 2, \ldots, 15\}$ in so bloki

$$\begin{aligned}\mathcal{B} = \{&\{1,2,3,4,5,6,7\}, \{1,2,3,8,9,14,15\}, \{1,2,3,10,11,12,13\},\\ &\{1,4,5,8,9,12,13\}, \{1,4,5,10,11,14,15\}, \{1,6,7,8,11,13,14\},\\ &\{1,6,7,9,10,12,15\}, \{2,4,6,8,9,10,11\}, \{2,4,6,12,13,14,15\},\\ &\{2,5,7,8,11,12,15\}, \{2,5,7,9,10,13,14\}, \{3,4,7,8,10,12,14\},\\ &\{3,4,7,9,11,13,15\}, \{3,5,6,8,10,13,15\}, \{3,5,6,9,11,12,14\}\}.\end{aligned}$$

Parametri načrta $(X, \mathcal{B})$ so 2-$(15, 7, 3)$. Ta načrt ustreza pedpostavkam izreka 7.11. Po izreku je

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

normalizirana Hadamardova matrika reda 16, kar lahko bralec tudi sam preveri.

8 Zaključek

Izpostavimo nekatere rezultate, ki smo jih bralcu predstavili v tem delu.

Videli smo, da so končne projektivne ravnine reda n simetrični načrti s parametri 2-$(n^2+n+1, n+1, 1)$. Spoznali smo, da končne projektivne ravnine reda 6 ne obstajajo. Poiskali smo grupo avtomorfizmov Fanove ravnine. S pomočjo 2-tranzitivne grupe reda 432 smo konstruirali 2-$(9, 3, 1)$ načrt. Poiskali smo razširitev Fanove ravnine in pokazali, da ta načrt ni razširljiv. Zdaj znamo konstruirati načrt s parametri 2-$(4\lambda+3, 2\lambda+1, \lambda)$, če le poznamo kakšno Hadamardovo matriko reda $4\lambda + 4$. In pa seveda tudi obratno, če poznamo kakšen načrt s parametri 2-$(4\lambda + 3, 2\lambda + 1, \lambda)$, lahko iz njega naredimo Hadamardovo matriko reda $4\lambda + 4$.

O načrtih je znanega mnogo več. Bralec, ki ga je tema pritegnila si lahko razširi obzorja z [2, 4, 5, 8, 11].

9 Literatura in viri

[1] N. L. Biggs in A. T. White, *Permutation Groups and Combinatorial Structures*. Cambridge University Press, Cambridge, 1979. *(Citirano na straneh 1, 18, 36, 39 in 41.)*

[2] P. J. Cameron, *Parallelisms of Complete Designs*, Cambridge University Press, Cambridge, 1976. *(Citirano na strani 42.)*

[3] P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin, 1997. *(Citirano na strani 1.)*

[4] R. H. F. Denniston, Some new 5-designs. *Bull. London Math. Soc.* 8 (1976) 263–267. *(Citirano na strani 42.)*

[5] M. Hall, Jr., Construction of block designs. V *Proceedings of the International Symposium on Combinatorial Mathematics and its Applications*, 1973, 251–258. *(Citirano na strani 42.)*

[6] M. Hall, Jr., *Combinatorial Theory*, John Wiley & Sons, New York, Second Edition, 1998. *(Citirano na strani 1.)*

[7] G. H. Hardy in E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, Sixth Edition, 2008. *(Citirano na strani 1.)*

[8] D. R. Hughes, On t-designs and groups. *Amer. J. Math.* 87 (1965) 761–778. *(Citirano na strani 42.)*

[9] J. D. Dixon in B. Mortimer, *Permutation Groups*. Springer, 1996. *(Citirano na straneh 20 in 23.)*

[10] P. J. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999. *(Citirano na strani 20.)*

[11] P. J. Cameron in J. H. van Lint, *Designs, Graphs, Codes and their Links*. Cambridge University Press, Cambridge, 1991. *(Citirano na straneh 3 in 42.)*

[12] C. J. Colbourn in J. H. Dinitz, *Handbook of Combinatorial Designs*. Chapman & Hall/CRC, Boca Raton, Florida, Second Edition, 2007. *(Citirano na strani 1.)*

[13] N. J. A. Sloane, *A Library of Hadamard Matrices*, `http://neilsloane.com/hadamard/`. (Datum ogleda: 4. 8. 2020.) *(Ni citirano.)*

[14] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.1)*, 2020, `https://www.sagemath.org`. *(Citirano na straneh 24 in 28.)*