UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

Paleyevi grafi in zemljevidi

(Paley graphs and maps)

Ime in priimek: Sanja Vasilić
Študijski program: Matematika
Mentor: izr. prof. dr. István Kovács

Koper, november 2014

Ključna dokumentacijska informacija

Ime in PRIIMEK: Sanja VASILIĆ

Naslov zaključne naloge: Paleyevi grafi in zemljevidi

Kraj: Koper

Leto: 2014

Število listov: 34 Število slik: 5 Število tabel: 4

Število referenc: 12

Mentor: izr. prof. dr. István Kovács

Ključne besede: graf, krepko regularen graf, Paleyev graf, zemljevid, Paleyev zemljevid.

Math. Subj. Class. (2010): 05C10, 05C25, 05E18, 05E30.

Izvleček:
V zaključni nalogi z naslovom Paleyevi grafi in zemljevidi si bomo najprej ogledali osnovne lastnosti in primere končnih polj, permutacijskih grup, grafov in zemljevidov na splošno. Slednje nam bo v pomoč pri razumevanju glavne vsebine zaključne naloge. Poglavje v katerem se bomo začeli ukvarjati z glavno temo zaključne naloge je poglavje o Paleyevih grafih in zemljevidih. Posebej si bomo ogledali primere za grafe in posebej za zemljevide. Glavni del zaključne naloge so poglavja 4, 5 in 6 z rešenimi nalogami 5.7.1 - 5.7.4 iz knjige N. L. Biggs and A. T. White, Permutation groups and combinatorial structures, London Math. Soc. Lecture Notes Ser. 33, Cambridge Univ. Press, Cambridge 1979 (5.7 Project: Paley maps, strani 134-135). S pomočjo definicij in izrekov iz prejšnjih poglavij bomo rešili nalogi in pokazali, da so Paleyevi grafi krepko regularni ter sebikomplementarni. Pri naslednjih dveh nalogah se bomo ukvarjali s Paleyevimi zemljevidi. Z eno rešitvijo naloge bomo pokazali, da so Paleyevi zemljevidi simetrični. Zadnjo nalogo bomo rešili s pomočjo definicij iz poglavja o Paleyevih grafih in zemljevidih izračunali rod Paleyevega zemljevida.

Key words documentation

Name and SURNAME: Sanja VASILIĆ

Title of final project paper: Paley graphs and maps

Place: Koper

Year: 2014

Number of pages: 34 Number of figures: 5 Number of tables: 4

Number of references: 12

Mentor: Assoc. Prof. István Kovács, PhD

Keywords: graph, strongly regular graph, Paley graph, map, Paley map.

Math. Subj. Class. (2010): 05C10, 05C25, 05E18, 05E30.

Abstract: In the thesis, titled Paley graphs and maps, we first review some basic properties and examples about finite fields, permutation groups, graphs and maps in general. The chapter in which we turn to the main subjects of the thesis is the chapter with title Paley graphs and maps. The main results will be presented in Chapters 4,5 and 6, where we solve Problems 5.7.1 - 5.7.4 from the book N. L. Biggs and A. T. White, Permutation groups and combinatorial structures, London Math. Soc. Lecture Notes Ser. 33, Cambridge Univ. Press, Cambridge 1979 (5.7 Project: Paley maps, sides 134 - 135). With the help of definitions and theorems from the preceding chapters we solve Problems and show that the Paley graphs are strongly regular and selfcomplementary respectively. In other Problems we consider Paley maps. By solving another Problem we show that the Paley maps are symmetric, and as the last task we solve and determine the genus of a Paley map.

Zahvala

Zahvaljujem se mentorju izr. prof. dr. István Kovács za vloženi čas, potrpežljivost in pomoč pri nastajanju zaključne naloge.

Hvala moji družini, ker mi je v času študija stala ob strani in omogočila sam študij.

Zahvala gre tudi sošolkama Marini in Tjaši ter sošolcu Eriku za polepšane študijske dneve, skupno učenje in tolažbo v času slabih rezultatov.

Hvala!

Kazalo vsebine

Kazalo tabel

Kazalo slik

1 Uvod

Raymond Edward Alan Christopher Paley (7. januar 1907 - 7. april 1933) je bil angleški matematik. Šolal se je na Etonu, kasneje pa se je vpisal na Trinity College, Cambridge, kjer se je izkazal kot briljanten študent in osvojil razne nagrade (npr. Smithovo nagrado).

Paleyjevi grafi, ki so poimenovani po Raymondu Paleyu, so v teoriji grafov gosti neusmerjeni grafi, skonstruirani iz elementov primernega končnega obsega s povezovanjem parov elementov, ki se razlikujeta v kvadratnem ostanku. Paleyevi grafi omogočajo rabo orodij iz teorije grafov pri raziskovanju teorije števil kvadratnih ostankov in imajo zanimive značilnosti, tako da so v teoriji grafov uporabni splošneje.

Naj bo q potenca praštevila, za katero velja $q \equiv 1 \pmod 4$. Naj $\mathbb{F}_q$ označuje končno polje s q elementi, kjer je q praštevilska potenca. Točke Paleyevega grafa so elementi $\mathbb{F}_q$, kjer obstaja povezava med različnima točkama x in y, če in samo če je $x-y$ kvadrat v $\mathbb{F}_q$.
Po definiciji Paleyevega grafa vidimo, da Paleyevi grafi obstajajo za naslednje rede:

$$5, 9, 13, 17, 25, 29, 37, 41, 49, 53, 61, 73, 81, 89, 97, 101, 109, 113, 121, 125, 137, 149, 157, ...$$

Skozi zaključno nalogo bomo videli, da so Paleyevi grafi posebnost zaradi svojih lastnosti.
Zaključna naloga je razdeljena na sedem poglavij, in sicer: Uvod, Osnovni pojmi, Paleyevi grafi in zemljevidi, Paleyevi grafi so krepko regularni in sebikomplementarni, Paleyevi zemljevidi so simetrični, Rod Paleyevih zemljevidov, Zaključek.
V drugem poglavju si bomo ogledali definicije, trditve in izreke, ki nam bodo v pomoč v naslednjih poglavjih. Definirali bomo končna polja, permutacijske grupe in grafe.
V tretjem poglavju si bomo podrobneje ogledali definicije in primere Paleyevih zemljevidov, kjer bomo uporabljali rotacije na grafu, da lahko sploh poiščemo ploskve Paleyevega zemljevida.
V četrtem poglavju bomo rešili nalogo 5.7.1 in 5.7.2 iz [2], kjer bomo pokazali, da so Paleyevi grafi krepko regularni in sebikomplementarni, kar je ena izmed posebnosti, ki jih Paleyevi grafi posedujejo. Pri nalogi 5.7.1 se bomo ukvarjali z avtomorfizmi in tranzitivno permutacijsko grupo, da dokažemo, da Paleyev graf premore tranzitivno grupo avtomorfizmov ranga 3. Temu sledi naloga 5.7.2, kjer bomo dokazali, da je Paleyev

graf izomorfen svojemu komplementu.
V petem poglavju si bomo ogledali rešitev naloge 5.7.3 iz [2], s katero bomo dokazali, da so Paleyevi zemljevidi simetrični.
V zadnjem poglavju bomo združili teme, ki so potekale skozi celotno zaključno nalogo. Tako bomo v nalogi 5.7.4 izračunali rod Paleyevih zemljevidov.

2 Osnovni pojmi

V tem poglavju si bomo ogledali osnovne definicije, trditve, leme in primere, ki jih bomo uporabljali v nadaljevanju.

2.1 Končna polja

Da bi razumeli vsebino zaključne naloge, moramo najprej poznati snov o končnih poljih. Zato si bomo v tem poglavju ogledali potrebne definicije, trditve, primere in leme iz [5, 8].

Definicija 2.1. Polje $\mathbb{F}$ je množica z najmanj dvema elementoma z operacijama $\oplus$ in $*$, za kateri veljajo naslednji aksiomi:

(i) $(\mathbb{F}, \oplus)$ je abelska grupa (identiteta je označena z 0).

(ii) $(\mathbb{F}^* = \mathbb{F} \setminus \{0\}, *)$ je abelska grupa (identiteta je označena z 1).

(iii) Distributivni zakon: Za vse $a, b, c \in \mathbb{F} : (a \oplus b) * c = (a * c) \oplus (b * c)$.

Pravimo, da je polje $\mathbb{F}$ končno, če ima končno mnogo elementov.

Trditev 2.2. *Število elementov v končnem polju* $\mathbb{F}$ *je enako* p^n*, kjer je* p *praštevilo in* $n \in \mathbb{N}$*.*

Trditev 2.3. *Za vsako praštevilo* p *in* $n \in \mathbb{N}$ *obstaja do izomorfizma natančno enolično določeno končno polje s* p^n *elementi.*

V nadaljevanju bomo končno polje s $q = p^n$ elementi označevali z $\mathbb{F}_q$.

Posledica 2.4. *Če je* p *praštevilo, potem je* $\mathbb{Z}_p$ *polje.*

Izrek 2.5. *Naj bo* R *komutativni kolobar z identiteto. Ideal* M *je maksimalen ideal kolobarja* R*, če je* R/M *polje.*

Izrek 2.6. *Naj bo* $\mathbb{F}_q$ *končno polje. Tedaj je* $\mathbb{F}_p[X]/(f(x))$ *polje natanko tedaj, ko je* $f(x)$ *nerazcepen nad* $\mathbb{F}_q$*.*

Definicija 2.7. Polje E je razširitveno polje polja F, če je $F \leq E$.

Izrek 2.8. *Naj bo F polje in $f(x)$ nekonstanten polinom v $F[X]$. Potem obstaja razširitveno polje E polja F in $\alpha \in E$, tako da velja $f(\alpha) = 0$.*

Primer 2.9. $\mathbb{Z}_3[x]/(x^2+1)$ je polje natanko takrat, ko je (x^2+1) nerazcepen. Ugotovimo, da x^2+1 nima ničel v polju $\mathbb{Z}_3$. Iz tega sledi, da je x^2+1 nerazcepen. Zato lahko $\mathbb{F}_9$ zapišemo kot $\mathbb{Z}_3/(f(x))$. Sledi, da so elemetni $\mathbb{F}_9 = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$.

Oglejmo si še tabelo za seštevanje in množenje elementov v razširitvenem polju $\mathbb{Z}_3(x)$.

Tabela 1: Tabela za seštevanje

+	0	1	2	x	x+1	x+2	$2x$	$2x$+1	$2x$+2
0	0	1	2	x	x+1	x+2	$2x$	$2x$+1	$2x$+2
1	1	2	0	1+x	x+2	x	$2x$+1	$2x$+2	$2x$
2	2	0	1	x+2	x	x+1	$2x$+2	$2x$	$2x$+1
x	x	x+1	x+2	$2x$	$2x$+1	$2x$+2	0	1	2
x+1	x+1	x+2	x	$2x$+1	$2x$+2	$2x$	1	2	0
x+2	x+2	x	x+1	$2x$+2	$2x$	$2x$+1	2	0	1
$2x$	$2x$	$2x$+1	$2x$+2	0	1	2	x	x+1	x+2
$2x$+1	$2x$+1	$2x$+2	$2x$	1	2	0	x+1	x+2	x
$2x$+2	$2x$+2	$2x$	$2x$+1	2	0	1	x+2	x	x+1

Tabela 2: Tabela za množenje

$*$	0	1	2	x	$2x$	x+1	$2x$+1	x+2	$2x$+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$2x$	x+1	$2x$+1	x+2	$2x$+2
2	0	2	1	$2x$	x	$2x$+2	x+2	$2x$+1	x+1
x	0	x	$2x$	2	1	x+2	x+1	$2x$+2	$2x$+1
$2x$	0	$2x$	x	1	2	$2x$+1	$2x$+2	x+1	x+2
x+1	0	x+1	$2x$+2	x+2	$2x$+1	$2x$	2	1	x
$2x$+1	0	$2x$+1	x+2	x+1	$2x$+2	2	x	$2x$	1
x+2	0	x+2	x+1	$2x$+2	x+1	1	$2x$	x	2
$2x$+2	0	$2x$+2	x+1	$2x$+1	x+2	x	1	2	$2x$

Definicija 2.10. Naj bo p poljubno praštevilo. Elementu ω, ki generira multiplikativno grupo neničelnih elementov končnega polja s p^n elementi, pravimo primitivni koren.

Lema 2.11. *Naj bo $q = p^r$, kjer je p liho praštevilo. Potem je število kvadratov v $\mathbb{F}_q \setminus \{0\}$ enako $\frac{1}{2}(q-1)$.*

Definicija 2.12. Definiramo funkcijo $\chi : \mathbb{F}_q \mapsto \{0, -1, 1\}$ takole

$$\chi(x) = \begin{cases} 0 & \text{če } x = 0, \\ 1 & \text{če } x \text{ je kvadrat v } \mathbb{F}_q \setminus \{0\}, \\ -1 & \text{če } x \text{ ni kvadrat v } \mathbb{F}_q. \end{cases}$$

V naslednji lemi smo izbrali nekaj lastnosti funkcije χ.

Lema 2.13. *Naj bo $q = p^r$, kjer je p liho praštevilo.*

(i) $\sum_{x \in \mathbb{F}_q} \chi(x) = 0$.

(ii) $\chi(xy) = \chi(x)\chi(y)$ *za vsaka elementa* $x, y \in \mathbb{F}_q$.

(iii) $\sum_{x \in \mathbb{F}_q} \chi(x)\chi(x+y) = -1$, *če je* $y \neq 0$.

2.2 Permutacijske grupe

V tem poglavju bomo definirali permutacijske grupe in njene lastnosti s pomočjo uporabe [7].

Definicija 2.14. Delovanje grupe G na množici X je preslikava μ: $X \times G \to X$, ki zadošča naslednjim lastnostim, kjer z x^g označimo sliko $\mu((x, g))$ elementa $(x, g) \in X \times G$:

(i) $x^1 = x$ za vsak $x \in X$, kjer je 1 identiteta grupe G;

(ii) $x^{g_1 g_2} = (x^{g_1})^{g_2}$ za vsak $x \in X$ in vsaka $g_1, g_2 \in G$.

Za dano delovanje μ pravimo tudi, da grupa G deluje na množici X ali da je X G-prostor. Moč množice $|X|$ imenujemo red delovanja.

V nadaljevanju bomo označevali grupo vseh permutacij množice X z oznako S_X.

Definicija 2.15. Slika delovanja grupe G na množici X je podgrupa v grupi S_X, ki jo sestavljajo permutacije $\pi_g, g \in G$, kjer je

$$\pi_g : x \mapsto x^g \quad \text{za vsak } x \in X.$$

Definicija 2.16. Orbita elementa $x \in X$, pri delovanju grupe G na množici X, je množica

$$Orb(x) = \{x^g \mid g \in G\}.$$

Definicija 2.17. Stabilizator elementa $x \in X$, pri delovanju grupe G na množici X, je množica

$$G_x = \{g \in G \mid x^g = x\}.$$

Lema 2.18. *(orbita-stabilizator) Za delovanje grupe G na množici X velja, da je $|Orb(x)| \cdot |G_x| = |G|$, kjer je $x \in X$.*

Dokaz. Definirajmo množico

$$\Omega = \{(g, x') \in G \times Orb(x) \mid x^g = x'\}.$$

Izračunajmo moč $|\Omega|$ na dva načina. Najprej dobimo, da je

$$|\Omega| = \sum_{g \in G} |\{x' \in Orb(x) \mid x^g = x'\}| = \sum_{g \in G} 1 = |G|.$$

Po drugi strani pa je

$$|\Omega| = \sum_{x' \in Orb(x)} |\{g \in G \mid x^g = x'\}|.$$

Opazimo, da tisti elementi $g \in G$, ki preslikajo x v x', tvorijo desni odsek podgrupe G_x v G. Zato je število takih elementov enako $|G_x|$. Iz tega sledi, da se zgornja enakost piše kot

$$\sum_{x' \in Orb(x)} |\{g \in G | x^g = x'\}| = \sum_{x' \in Orb(x)} |G_x| = |Orb(x)| \cdot |G_x|.$$

Dokaz leme sledi iz obeh točk. □

Definicija 2.19. Grupa G deluje na množici X tranzitivno, če za vsak par elementov $x, y \in X$ obstaja element $g \in G$, ki preslika x v y (t.j. $x^g = y$).

V bistvu je delovanje grupe G na množici X tranzitivno, če je orbita ena sama (za vsak $x \in X$ je $Orb_G(x) = X$).

Trditev 2.20. *Naj bo X tranzitiven G-prostor. Potem velja:*

(i) $|X|$ deli $|G|$.

(ii) Vsi stabilizatorji G_x za $x \in X$ tvorijo razred konjugiranosti podgrup v grupi G.

Definicija 2.21. Grupa G deluje na množici X polregularno, če je G_x trivialen za vsak $x \in X$.

Delovanje imenujemo regularno, če je hkrati tranzitivno in polregularno.

Definicija 2.22. Tranzitivno permutacijsko grupo G množice X imenujemo Frobeniusova grupa, če je edini element v G, ki fiksira več kot eno točko, identiteta grupe G.

Trditev 2.23. *Naj bo G tranzitivna permutacijska grupa množice X in naj bosta $x, y \in X$. Potem je število orbit stabilizatorja G_x enako številu orbit stabilizatorja G_y.*

Definicija 2.24. Rang tranzitivne permutacijske grupe $G \leq S_X$ je število orbit stabilizatorja G_x za nek element $x \in X$.

Trditev 2.25. *Rang r tranzitivne permutacijske grupe $G \leqslant S_X$ je*

$$r = \frac{1}{|G|} \sum_{g \in G} |fix(g)|^2,$$

kjer $fix(g)$ označuje število elementov $x \in X$, za katere velja $x^g = x$.

2.3 Grafi

Da se lahko začnemo ukvarjati z grafi, moramo najprej poznati nekaj osnovnih definicij. V nadaljevanju bomo spoznali osnovne pojme s pomočjo uporabe [1, 6, 9, 10].

Definicija 2.26. Naj bo V končna neprazna množica in E poljubna družina dvoelementnih podmnožic množice V. Paru $\Gamma = (V, E)$ pravimo graf na množici točk $V = V\Gamma$ in z množico povezav $E = E\Gamma$.
Element $\{u, v\}$ množice E pišemo krajše uv. Kadar je par točk uv element množice $E\Gamma$, pravimo, da sta točki u in v sosednji v grafu Γ.

Definicija 2.27. Regularni graf je v teoriji grafov graf brez zank in večkratnih povezav, v katerem imajo vse točke enako število sosednjih točk oziroma imajo vse točke enako stopnjo.

Definicija 2.28. Avtomorfizem grafa Γ je permutacija g v $S_{V\Gamma}$, za katero velja:

$$\{v_1, v_2\} \in E\Gamma \iff \{v_1^g, v_2^g\} \in E\Gamma \quad \text{za vsak } v_1, v_2 \in V\Gamma.$$

Vsi avtomorfizmi grafa Γ tvorijo podgrupo v $S_{V\Gamma}$, ki jo označimo z $\operatorname{Aut}\Gamma$. Pravimo, da je graf Γ vozliščno tranzitiven, če deluje $\operatorname{Aut}\Gamma$ na $V\Gamma$ tranzitivno.

Definicija 2.29. Dva grafa Γ in Σ sta izomorfna, $\Gamma \cong \Sigma$, če obstaja bijektivna preslikava $\varphi : V\Gamma \longrightarrow V\Sigma$ med množicama vozlišč, za katero velja:

$$uv \in E\Gamma \iff \varphi(u)\varphi(v) \in E\Sigma$$

za poljubni vozlišči $u, v \in V\Gamma$. Preslikavi φ rečemo izomorfizem.

Definicija 2.30. Krepko regularen graf Γ s parametri (n, k, λ, μ) je k-regularen graf na n točkah, pri čemer za λ in μ velja:

(i) za vsak par povezanih točk grafa Γ velja, da imata natanko λ skupnih sosedov in

(ii) za vsak par nepovezanih točk grafa Γ velja, da imata natanko μ skupnih sosedov.

3 Paleyevi grafi in zemljevidi

V tem poglavju se bomo posvetili naši glavni temi in predstavili različne primere s pomočjo [2, 11].

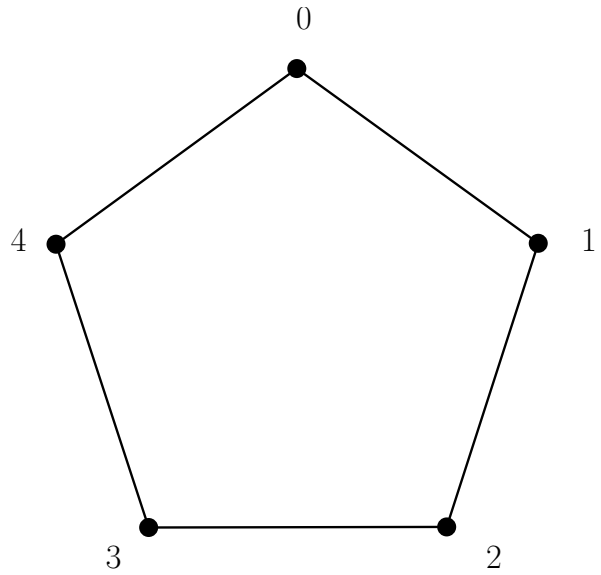
3.1 Paleyev graf

Spoznali bomo definicijo Paleyevega grafa in si ogledali primere s pomočjo [11].

Definicija 3.1. Naj bo q potenca praštevila, za katero velja $q \equiv 1 (\text{mod } 4)$. Paleyev graf $P(q)$ dobimo tako, da za točke vzamemo elemente iz $\mathbb{F}_q$. Točka x je povezana s točko y, če je $(x - y) \in (\mathbb{F}_q)^2$, kjer s $(\mathbb{F}_q)^2$ označimo neničelne kvadrate iz množice $\mathbb{F}_q$.

Primer 3.2. Paleyev graf $P(5)$ reda 5 je cikel C_5. Naj bo $P(5) = (V, E)$ Paleyev graf reda 5. Potem je: $V = \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ in $(\mathbb{F}_5^*)^2 = \{1, 4\}$. Iz tega sledi, da je množica povezav naslednja:

$$E = \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 0\}\}.$$



Slika 1: Paleyev graf P(5).

Primer 3.3. Naj bo $P = (V, E)$ Paleyev graf reda $9 = 3^2$. Vemo, da je $p = 3, n = 2$. Potem je $V(P) = \mathbb{F}_{3^2}$ polje reda 9, ki ga lahko zapišemo kot

$$\mathbb{F}_{3^2} = \{0, 1, 2, a, 2a, 1 + a, 1 + 2a, 2 + a, 2 + 2a\} \cong \mathbb{Z}_3[x]/(x^2 + 1)$$

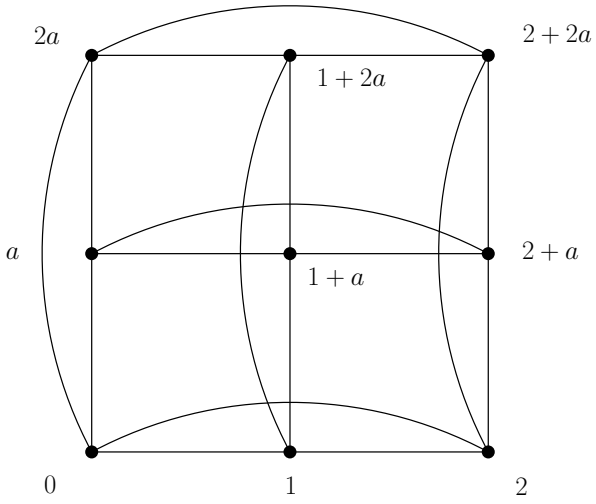
a je koren polinoma $x^2 + 1$. Kvadrate izračunamo takole

$$1^2 = 1, \qquad 2^2 = 1, \qquad a^2 = -1 = 2,$$

$$(2a)^2 = 2, \qquad (1 + a)^2 = 2a, \qquad (1 + 2a)^2 = a,$$

$$(2 + a)^2 = a, \qquad (2 + 2a)^2 = 2a,$$

torej je $(\mathbb{F}_{3^2}^*)^2 = \{1, 2, a, 2a\}$. Iz tega sledi, da je množica povezav naslednja $E = \{\{0, 1\}, \{0, 2\}, \{0, a\}, \{0, 2a\}, \{1, 2\}, \{1, 1+a\}, \{1, 1+2a\}, \{2, 2+a\}, \{2, 2+2a\}, \{a, 1+a\}, \{a, 2+a\}, \{a, 2a\}, \{2a, 1+2a\}, \{2a, 2+2a\}, \{1+a, 2+a\}, \{1+a, 1+2a\}, \{1+2a, 2+2a\}, \{2 + a, 2 + 2a\}\}$.



Slika 2: Paleyev graf P(9).

3.2 Zemljevidi

Za dokončno razumevanje zakjučne naloge si bomo ogledali primere in definicije splošnih ter Paleyevih zemljevidov [2].

Definicija 3.4. Rotacija na grafu $\Gamma = (V, E)$ je množica $\rho = \{\rho_v\}_{v \in V}$, kjer je vsak ρ_v ciklična permutacija točk, sosednjih točki $v \in V$. Zemljevid je par (Γ, ρ), kjer je Γ povezan graf in je ρ rotacija na Γ.

Naj $A\Gamma$ označuje množico lokov grafa Γ:

$$A\Gamma = \{(v, w) | \{v, w\} \text{ je povezava od } \Gamma\}.$$

Definicija 3.5. Naj bo $M = (\Gamma, \rho)$ zemljevid. Ploskve zemljevida M so ciklična zaporedja točk nastopajočih v ciklu ρ^* na $A\Gamma$, kjer je ρ^* definirana na sledeč način $\rho^*(v, w) = (w, \rho_w(v))$.

Primer 3.6. Definirajmo rotacijo polnega grafa K_4 na sledeč način:

$$\rho_1 = (234), \qquad \rho_2 = (143)$$

$$\rho_3 = (124), \qquad \rho_4 = (132).$$

Oglejmo si ploskve zemljevida.
1. ploskev:

$$(43) \mapsto (3, \rho_3(4)) = (31) \mapsto (1, \rho_1(3)) = (14) \mapsto (4, \rho_4(1)) = (43).$$

2. ploskev:

$$(13) \mapsto (3, \rho_3(1)) = (32) \mapsto (2, \rho_2(3)) = (21) \mapsto (1, \rho_1(2)) = (13).$$

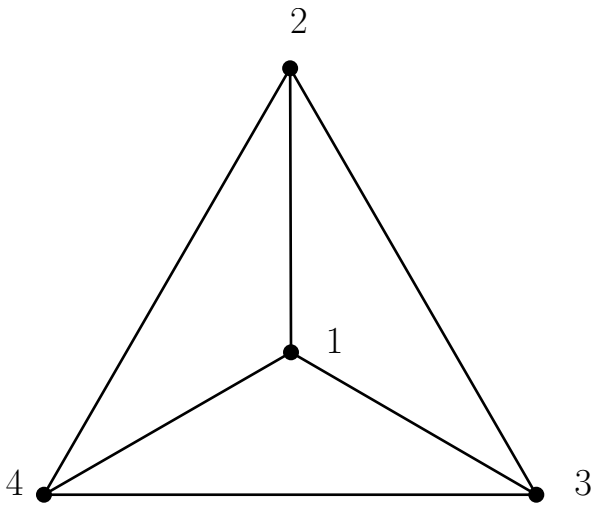
3. ploskev:

$$(41) \mapsto (1, \rho_1(4)) = (12) \mapsto (2, \rho_2(1)) = (24) \mapsto (4, \rho_4(2)) = (41).$$

4. ploskev:

$$(23) \mapsto (3, \rho_3(2)) = (34) \mapsto (4, \rho_4(3)) = (42) \mapsto (2, \rho_2(4)) = (23).$$

S podano rotacijo lahko graf na sliki obravnavamo kot zemljevid.



Slika 3: Zemljevid (K_4, ρ).

Definicija 3.7. Avtomorfizem zemljevida $M = (\Gamma, \rho)$ je tak avtomorfizem g grafa Γ, da velja $\rho^{(g)} = \rho$; kjer je $\rho^{(g)}$ rotacija definirana takole $\rho_{vg}^{(g)} = g^{-1}\rho_v g$ za vsak v $\in V\Gamma$.

Lema 3.8. *Naj bo* $M = (\Gamma, \rho), g \in \operatorname{Aut} M$ *in predpostavimo, da je* $\{v, w\}$ *povezava grafa* Γ. *Če g fiksira obe točki v in w, potem je g identični avtomorfizem.*

Posledica 3.9. $\operatorname{Aut} M \leq 2|E\Gamma|$.

Dokaz. Lema 3.8 pravi, da $\operatorname{Aut} M_{(v,w)} = 1$. Lema 2.18 implicira: $|\operatorname{Aut} M| = |\operatorname{Aut} M_{(v,w)}| \cdot |Orb_{\operatorname{Aut} M}(v, w)| \leq 2|E\Gamma|$. □

Definicija 3.10. Zemljevid $M = (\Gamma, \rho)$ je simetričen, če je vozliščno tranzitiven in $|\operatorname{Aut} M| = 2|E\Gamma|$.

Definicija 3.11. Naj bo t nek primitiven element v $\mathbb{F}_q$. Paleyev zemljevid $MP(q)$ je definiran kot zemljevid $(P(q), \rho)$, kjer je $\rho = \{\rho_x : x \in \mathbb{F}_q\}$, in je ρ_x ciklična permutacija točk sosednjih točki x, za katero velja $\rho_x(x + a) = x + t^2a$, a v $(\mathbb{F}_q)^2$.

Primer 3.12. Ogledali si bomo primer za Paleyev graf P(9). Polje reda 9 lahko zapišemo kot:

$$\mathbb{F}_{3^2} = \{0, 1, 2, a, 2a, 1 + a, 1 + 2a, 2 + a, 2 + 2a\}.$$

Dobili smo točke Paleyevega grafa P(9). Naslednji korak je poiskati primitivni element. Preverimo, da je a primitivni element:

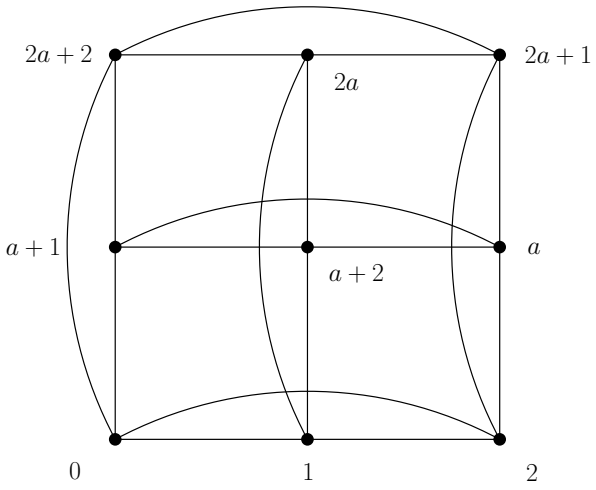
$$a, \qquad a^2 = a + 1, \qquad a^3 = (a + 1)a = a^2 + a = 2a + 1,$$

$$a^4 = a^3a = (2a + 1)a = 2a^2 + a = 2, \qquad a^5 = a^4a = 2a, \qquad a^6 = a^4a^2 = 2a + 2,$$

$$a^7 = a^4a^3 = a + 2, \qquad a^8 = (a^4)^2 = 4 = 1.$$

Ugotovimo, da a generira celotno multiplikativno grupo $\mathbb{F}_9{}^*$.
Dobimo, da so kvadrati naslednji elementi: $a^2, a^4, a^6, a^8 = \{a+1, 2, 2(a+1), 1\}$. Lahko opazimo, da je

$$\mathbb{F}_9 = \{\alpha 1 + \beta(a+1) : \alpha, \beta \in \mathbb{Z}_3\}.$$



Slika 4: Paleyev graf P(9).

Sedaj pa si oglejmo sose??ine $N(x)$ vseh točk:

$$0 \sim \{1, 2, a+1, 2a+2\}, \qquad 1 \sim \{2, 0, a+2, 2a\}, \qquad 2 \sim \{0, 1, a, 2a+1\},$$

$$a \sim \{a+1, a+2, 2a+1, 2\}, \qquad a+1 \sim \{0, a+2, , 2a+2, a\}, \qquad a+2 \sim \{1, a, a+1, 2a\}$$

$$2a+1 \sim \{a, 2a, 2, 2a+2\}, \qquad 2a \sim \{1, a+2, 2a+2, 2a+1\}, \qquad 2a+2 \sim \{2a, a+1, 2a+1, 0\}.$$

Da lahko definiramo Paleyev zemljevid potrebujemo še rotacije.

Tabela 3: Tabela rotacij

x	ρ_x	x	ρ_x
0	$(1, a+1, 2, 2a+2)$	$a+1$	$(a+2, 2a+2, a, 0)$
1	$(2, a+2, 0, 2a)$	$a+2$	$(a, 2a, a+1, 1)$
2	$(0, a, 1, 2a+1)$	$2a+1$	$(2a+2, 2, 2a, a)$
a	$(a+1, 2a+1, a+2, 2)$	$2a$	$(2a+1, 1, 2a+2, a+2)$
		$2a+2$	$(2a, 0, 2a+1, a+1)$

Ker vemo, da za Paleyev graf velja $\rho_x = t^2 x$, kjer je t primitivni koren, lahko naredimo naslednje: $t = a$, zato je $t^2 = a^2 = (a+1)$. Iz tega sledi:

$$\rho_0 : x \mapsto t^2 x = a^2 x = (a+1)x; x \in (\mathbb{F}_9)^2,$$

Ker smo elemente $(\mathbb{F}_9)^2 = (1, a+1, 2, 2a+2)$ že prej določili, nam ostane le še, da preverimo ρ_x ciklično permutacijo.

$$1 \mapsto (a+1)1 = a+1$$

$$a+1 \mapsto (a+1)(a+1) = 2$$

$$2 \mapsto (a+1)2 = 2a+2$$

$$2a+2 \mapsto (a+1)(2a+2) = 1$$

Pri naslednjem koraku bomo določili ploskve zemljevida $M = (\Gamma, \rho)$ s pomočjo Definicije 3.5 in Tabele 3.

$$(0,1) \mapsto (1, \rho_1(0)) = (1, 2a) \mapsto (2a, \rho_{2a}(1)) = (2a, 2a+2) \mapsto (2a+2, \rho_{2a+2}(2a)) = (2a+2, 0)$$

$$\mapsto (0, \rho_0(2a+2)) = (0,1).$$

Dobili smo prvo ploskev zemljevida.

$$(1,2) \mapsto (2, \rho_2(1)) = (2, 2a+1) \mapsto (2a+1, \rho_{2a+1}(2)) = (2a+1, 2a) \mapsto (2a, \rho_{2a}(2a+1)) = (2a, 1)$$

$$\mapsto (1, \rho_1(2a)) = (1,2).$$

Dobili smo drugo ploskev zemljevida.

$$(2,a) \mapsto (a, \rho_a(2)) = (a, a+1) \mapsto (a+1, \rho_{a+1}(a)) = (a+1, 0) \mapsto (0, \rho_0(a+1)) = (0,2)$$

$$\mapsto (2, \rho_2(0)) = (2,a).$$

Dobili smo tretjo ploskev zemljevida.

$$(1, a{+}2) \mapsto (a{+}2, \rho_{a+2}(1)) = (a{+}2, a) \mapsto (a, \rho_a(a{+}2)) = (a, 2) \mapsto (2, \rho_2(a)) = (2, 1) \mapsto (1, \rho_1(2))$$
$$= (1, a + 2).$$

Dobili smo četrto ploskev zemljevida.

$$(a, 2a{+}1) \mapsto (2a{+}1, \rho_{2a+1}(a)) = (2a{+}1, 2a{+}2) \mapsto (2a{+}2, \rho_{2a+2}(2a{+}1)) = (2a{+}2, a{+}1)$$
$$\mapsto (a + 1, \rho_{a+1}(2a + 2)) = (a + 1, a) \mapsto (a, \rho_a(a + 1)) = (a, 2a + 1).$$

Dobili smo peto ploskev zemljevida.

$$(a{+}2, 2a) \mapsto (2a, \rho_{2a}(a{+}2)) = (2a, 2a{+}1) \mapsto (2a{+}1, \rho_{2a+1}(2a)) = (2a{+}1, a) \mapsto (a, \rho_a(2a{+}1))$$
$$= (a, a + 2) \mapsto (a + 2, \rho_{a+2}(a)) = (a + 2, 2a)$$

Dobili smo šesto ploskev zemljevida.

$$(0, 2a{+}2) \mapsto (2a{+}2, \rho_{2a+2}(0)) = (2a{+}2, 2a{+}1) \mapsto (2a{+}1, \rho_{2a+1}(2a{+}2)) = (2a{+}1, 2)$$
$$\mapsto (2, \rho_2(2a + 1)) = (2, 0) \mapsto (0, \rho_0(2)) = (0, 2a + 2).$$

Dobili smo sedmo ploskev zemljevida.

$$(1, 0) \mapsto (0, \rho_0(1)) = (0, a{+}1) \mapsto (a{+}1, \rho_{a+1}(0)) = (a{+}1, a{+}2) = (a{+}2, \rho_{a+2}(a{+}1)) = (a{+}2, 1)$$
$$\mapsto (1, \rho_1(a + 2)) = (1, 0).$$

Dobili smo osmo ploskev zemljevida.

$$(a{+}2, a{+}1) \mapsto (a{+}1, \rho_{a+1}(a{+}2)) = (a{+}1, 2a{+}2) \mapsto (2a{+}2, \rho_{2a+2}(a{+}1)) = (2a{+}2, 2a)$$
$$\mapsto (2a, \rho_{2a}(2a + 2)) = (2a, a + 2) \mapsto (a + 2, \rho_{a+2}(2a)) = (a + 2, a + 1).$$

Dobili smo deveto ploskev zemljevida.

Izrek 3.13. *Naj bo $\Gamma = (V, E)$ povezan graf in ρ rotacija Γ. Naj F označuje množico ploskev zemljevida $M = (\Gamma, \rho)$. Potem obstaja tako nenegativno celo število $g(M)$, da velja*

$$|V| - |E| + |F| = 2 - 2g(M).$$

Definicija 3.14. Nenegativno celo število $g(M)$ nastopajoče v Izreku 3.13 imenujemo rod zemljevida M.

Primer 3.15. Oglejmo si primer rodu za zemljevida P(5) in P(9).

Tabela 4: Tabela zemljevidov

Zemljevid	Število točk	Število povezav	Število ploskev	Rod
P(5)	5	5	2	0 (Sfera)
P(9)	9	18	9	1 (Torus)

Rod smo izračunali s pomočjo naslednje formule:

$$|V| - |E| + |F| = 2 - 2g(M).$$

$$P(5) : 5 - 5 + 2 = 2 - 2g(M)$$

$$g(M) = 0$$

$$P(9) : g(M) = \frac{1}{2}(18 + 2 - 9 - 9) = 1$$

Definicija 3.16. Naj bo ρ ciklična permutacija okoli točke 0 pri Paleyevem zemljevidu $MP(q)$. Naj bo $\overline{\rho}$ permutacija od Ω, kjer $\Omega := (\mathbb{F}_q)^2$ za katero velja $\overline{\rho}(\omega) = \rho(-\omega)$ za vse $\omega \in \Omega$. Naj ima $\overline{\rho}$ cikle $\Omega_1, \Omega_2, ..., \Omega_t$ v njeni ciklični dekompoziciji, in sicer pišemo $\Omega_i = (\omega_{i1}, \omega_{i2}, ..., \omega_{ik_i}), 1 \leq i \leq t$. Potem je perioda m_i od $MP(q)$ za $1 \leq i \leq t$ definirana kot red vsote $\omega_{i1} + \omega_{i2} + ... + \omega_{ik_i}$ v $(\mathbb{F}_q, +)$.

Izrek 3.17. *Naj bodo $m_1, m_2, ..., m_t$ periode Paleyevega zemljevida $MP(q)$; potem je rod g zemljevida $MP(q)$ podan z*

$$4(g-1) = |q|(\frac{q-1}{2} - 2 - 2\sum_{i=1}^{t} 1/m_i).$$

Primer 3.18. V tem primeru si bomo ogledali rod od $MP(13)$.
Najprej poiščimo sosede točke 0. Vemo, da so sosedi točke 0 kvadrati od $\mathbb{Z}_{13}$.

$$0 \sim 1, 4, 9, 3, 12, 10$$

Poiskati moramo še primitivni koren v $\mathbb{Z}_{13}$. Ugotovimo, da je primitivni koren enak $t = 2$. Dobimo naslednje:

$$\rho = (1, 4, 3, 12, 9, 10)$$

Opazimo, da so inverzi naslednji:

$$-1 = 12 \qquad -4 = 9 \qquad -3 = 10$$

Sedaj lahko izračunamo periode zemljevida s pomočjo naslednje formule $\overline{\rho}(w) = \rho(-w)$. Tako dobimo $\overline{\rho}$

$$\overline{\rho} = (1, 9, 3)(4, 10, 12).$$

Iz tega sledi, da je $\Omega_1 = (1, 9, 3)$ in $\Omega_2 = (4, 10, 12)$. Vsota elementov v Ω_1 in Ω_2 je enaka 0. Iz tega sledi, da sta periodi enaki $m_1 = 1$ in $m_2 = 1$. Sedaj lahko izračunamo rod s pomočjo formule iz Izreka 2.43.:

$$\begin{aligned} 4(g-1) &= |q|(|\frac{q-1}{2}| - 2 - 2\sum_{i=1}^{t} 1/m_i) \\ &= 13(6 - 2 - 2(1+1)) = 0 \end{aligned}$$

Iz tega sledi $g = 1$.

4 Paleyevi grafi so krepko regularni in sebikomplementarni

V tem poglavju bomo rešili nalogi 5.7.1 in 5.7.2 iz [2].

Naloga 4.1. [2, Naloga 5.7.1]

(a) Dokažite, da Paleyev graf $P(q)$ premore tranzitivno grupo avtomorfizmov, ki ima rang 3.

(b) Dokažite, da je $P(q)$ krepko regularen graf in najdite njegove parametre.

Rešitev: Za (a) definirajmo permutacijsko grupo G, ki vsebuje vse permutacije od $\mathbb{F}_q$ naslednje oblike:

$$x \mapsto a^2x + b \quad \text{za vsak } x \in \mathbb{F}_q; \tag{4.1}$$

kjer sta $a, b \in \mathbb{F}_q$ in $a \neq 0$. Označimo s ϕ permutacijo podano v (4.1).
Dokažimo najprej, da je ϕ avtomorfizem. Naj bo $\{v_1, v_2\}$ poljubna povezava grafa $P(q)$. Torej je $v_2 - v_1 = u^2$ za nek $u \in \mathbb{F}_q$. Po definiciji ϕ velja naslednje:

$$v_1^\phi = a^2v_1 + b \quad in \quad v_2^\phi = a^2v_2 + b.$$

Sliki v_1^ϕ in v_2^ϕ sta povezani natanko tedaj, ko velja $v_2^\phi - v_1^\phi \in (\mathbb{F}_q)^2$. Torej sledi:

$$v_2^\phi - v_1^\phi = a^2v_2 + b - (a^2v_1 + b) = a^2(v_2 - v_1) + b - b = a^2u^2 = (au)^2 \neq 0$$

Dokazali smo, da je ϕ res avtomorfizem.

Sedaj bomo dokazali, da je G tranzitivna permutacijska grupa.

$$Orb_G(0) = \{0^\phi : \phi \in G\} = \{b : b \in \mathbb{F}_q\} = \mathbb{F}_q.$$

Vidimo, da ima G eno orbito. Po Definiciji 2.19 je G tranzitivna.

Dokazati moramo še, da ima G rang 3. Najprej si oglejmo stabilizator G_0, kjer je $0 \in \mathbb{F}_q$. Grupa G_0 vsebuje permutacije v naslednji obliki $x \mapsto a^2x$.

$$Orb_{G_0}(0) = \{0\}$$

$$Orb_{G_0}(1) = \{a^2 : a \in \mathbb{F}_q, a \neq 0\} = (\mathbb{F}_q)^2$$

$$Orb_{G_0}(u) = \{ua^2 : a \in \mathbb{F}_q, a \neq 0\}$$

Skupaj smo našli $1 + \frac{q-1}{2} + \frac{q-1}{2} = q$ elementov. To pomeni, da ni več orbit. Sledi G ima rang 3.

Za (b) bomo dokazali, da je Paleyev graf $P(q)$ krepko regularen in sicer s parametri $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

Naj bo $A = A(P(q))$ matrika sosednosti grafa $P(q)$. Pišimo $GF(q) = \{a_1, \ldots, a_q\}$. Definiramo matriko $Q = (q_{ij})$ velikosti $q \times q$ takole:

$$(q_{ij}) = \chi(a_i - a_j) \quad \text{za vsaka } i, j \in \{1, \ldots, q\}.$$

Vpeljali bomo nekaj lastnosti matrik A in Q. Najprej z I označimo identično matriko velikosti $q \times q$ in z J matriko velikosti $q \times q$ v kateri so vsi elementi enaki 1. Iz definicije sledi takoj:

$$Q + J = 2A + I. \tag{4.2}$$

Potem trdimo, da je

$$QJ = JQ = 0. \tag{4.3}$$

Izračunajmo element $(QJ)_{i,j}$:

$$(QJ)_{i,j} = \sum_{k=1}^{q} q_{i,k} = \sum_{k=1}^{q} \chi(a_i - a_k) = \sum_{x \in GF(q)} \chi(x) = 0,$$

kjer zadnja enakost sovpada točki (i) v 2.13 Torej je $QJ = 0$. Da dobimo $JQ = 0$ je dovolj, da opazimo, da je $JQ = J^T Q^T = (QJ)^T = 0^T = 0$.
Na koncu trdimo, da je:

$$Q^2 = qI - J. \tag{4.4}$$

Izračunajmo element $(Q^2)_{i,j} = (QQ^T)_{i,j}$:

$$(QQ^T)_{i,j} = \sum_{i=1}^{k} q_{i,k} q_{j,k} = \sum_{i=1}^{k} \chi(a_i - a_k)\chi(a_j - a_k)$$

$$= \sum_{x \in GF(q)} \chi(x)\chi(x + y)$$

$$= \begin{cases} -1 & \text{če } i \neq j \\ q - 1 & \text{če } i = j. \end{cases}$$

S tem je enakost (4.4) dokazana.
Z uporabo (4.2), (4.3) in (4.4) lahko zapišemo, da je

$$AA^T = -A + \frac{1}{4}(q-1)I + \frac{1}{4}(q-1)J.$$

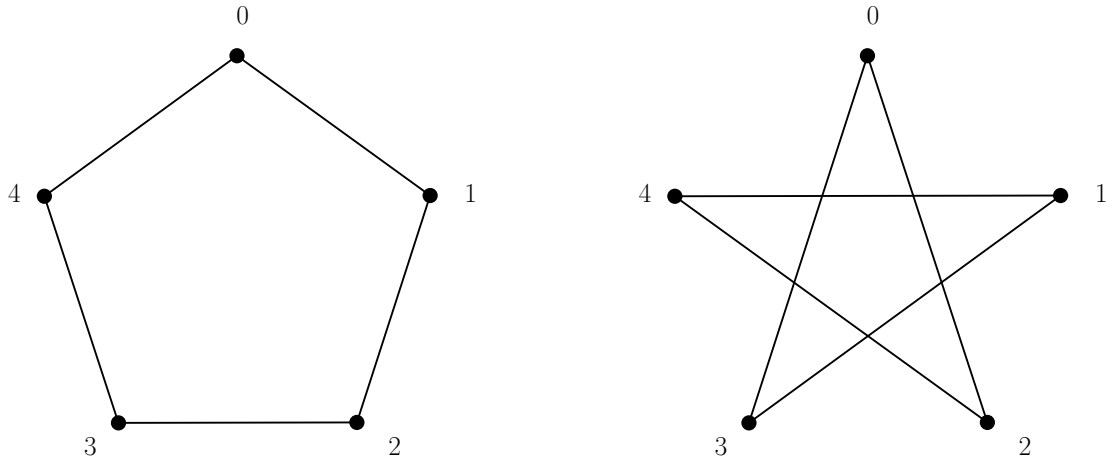
To pa pomeni natanko to, da je

$$k = \frac{1}{2}(q-1), \lambda = \frac{1}{4}(q-5) \quad \text{in } \mu = \frac{1}{4}(q-1).$$

□

Primer 4.2.

$$P(5) \cong C_5 \qquad\qquad \overline{P(5)} \cong C_5$$



Slika 5: Grafa $P(5)$ in $\overline{P(5)}$.

Definicija 4.3. Graf Γ je sebikomplementaren, če je izomorfen svojemu komplementu.

Naloga 4.4. [2, Naloga 5.7.2] Dokažite, da je $P(q)$ izomorfen svojemu komplementu $\overline{P(q)}$.

Rešitev: Definirajmo preslikavo $f : \mathbb{F}_q \to \mathbb{F}_q$, za katero velja:

$$x \mapsto wx;$$

kjer je w fiksiran nekvadrat v $\mathbb{F}_q$. Vemo, da velja naslednje:

$$P(q) : v_1 \sim v_2 \Leftrightarrow v_1 - v_2 \in (\mathbb{F}_q)^2,$$

$$\overline{P(q)} : v_1 \sim v_2 \Leftrightarrow v_1 \nsim v_2 \in P(q) \Leftrightarrow v_1 - v_2 \notin (\mathbb{F}_q)^2,$$

$$\{v_1, v_2\} \in E(P(q)), \qquad \{v_1^f, v_2^f\} \in E(\overline{P(q)}).$$

Naj bo $\{v_1, v_2\}$ poljubna povezava v $P(q)$. Dokažimo, da je $P(q) \cong \overline{P(q)}$. Naj bo:

$$v_2 - v_1 = u^2, \quad \text{kjer je } u \in \mathbb{F}_q.$$

Po definiciji f velja naslednje:

$$v_1^f = wv_1 \quad in \quad v_2^f = wv_2.$$

v_1^f in v_2^f sta povezani natanko takrat, ko velja:

$$v_2^f - v_1^f \notin (\mathbb{F}_q)^2$$

To velja, ker je:

$$v_2^f - v_1^f = wv_2 - wv_1 = w(v_2 - v_1)$$

Dokazali smo, da je $P(q) \cong \overline{P(q)}$. □

5 Paleyevi zemljevidi so simetrični

V tem poglavju si bomo ogledali rešitev naloge 5.7.3 iz [2].

Naloga 5.1. [2, Naloga 5.7.3] Dokažite, da so Paleyevi zemljevidi simetrični.

Rešitev: Vemo, da je vsak avtomorfizem $MP(q)$ avtomorfizem $P(q)$ in da obratno ne velja.

V nalogi 3.1. smo že definirali avtomorfizme od $P(q)$ na sledeč način:

$$\phi : x \mapsto a^2x + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$$

$$\phi^{-1} : x \mapsto a^{-2}x - ba^{-2}$$

Dokazali bomo, da so takšni ϕ avtomorfizmi tudi od $MP(q)$. Po definiciji 3.7 moramo preveriti, da velja: $\rho^{(\phi)} = \rho$, to je, $\rho_{x^\phi} = \phi^{-1}\rho\phi$. Vemo, da je

$$\rho_x(x + c) = x + t^2c, c \in (F_q^*)^2$$

$$\rho_{x^\phi}(x^\phi + c) = x^\phi + t^2c, c \in (F_q^*)^2.$$

Potem lahko pišemo

$$\begin{aligned}(x^\phi + c)^{\phi^{-1}} &= a^{-2}(a^2x + b + c) - ba^{-2} \\ &= x + a^{-2}b + a^{-2}c - ba^{-2} \\ &= x + a^{-2}c,\end{aligned}$$

in s tem dobimo

$$\begin{aligned}(x^\phi + c)^{\phi^{-1}\rho_x\phi} &= (x + a^{-2}c)^{\rho_x\phi} \\ &= (x + t^2a^{-2}c)^\phi \\ &= a^2x + t^2a^{-2}ca^2 + b \\ &= a^2x + b + t^2c \\ &= x^\phi + t^2c.\end{aligned}$$

Vidimo, da je $\rho_{x^\phi} = \phi^{-1}\rho\phi$, zato je ϕ res avtomorfizem od $MP(q)$.
Dobili smo, da $\operatorname{Aut} MP(q) \geq q \cdot \dfrac{q-1}{2} = 2 \cdot |EP(q)|$. Vemo tudi, da velja $\operatorname{Aut} MP(q) \leq 2 \cdot |EP(q)|$, torej iz tega sledi

$$2 \cdot |EP(q)| \leq |\operatorname{Aut} MP(q)| \leq 2 \cdot |EP(q)|,$$

torej

$$|\operatorname{Aut} MP(q)| = 2 \cdot |EP(q)|,$$

zato je $MP(q)$ simetričen.

□

6 Rod Paleyevih zemljevidov

V tem poglavju si bomo ogledali rešitev naloge 5.7.4 iz [2].

Naloga 6.1. [2, Naloga 5.7.4] Poiščite rod zemljevida $MP(q)$. Razlikujte dva primera $q \equiv 1, 5 (\mathrm{mod}\ 8)$.

Rešitev: Vemo, da rod izračunamo na sledeč način:

$$4(g-1) = |q|(|\frac{q-1}{2}| - 2 - 2\sum_{i=1}^{t} 1/m_i).$$

Izračunati moramo še periode $m_1, m_2, ..., m_t$. Sedaj moramo poiskati $\Omega = (\mathbb{F}_q^{\times})^2$. Naj bo t primitivni element in ρ ciklična permutacija. Po definiciji Paleyevega grafa vemo, da je $\rho(\omega) = t^2\omega$. Iz enačbe sledi $1 \mapsto t^2, t^2 \mapsto t^4, t^4 \mapsto t^6, ...$ Dobimo, da je rotacija ρ enaka:

$$\rho = (1, t^2, t^4, ..., t^{q-3}).$$

Zanima nas, koliko ciklov ima $\overline{\rho}$, kjer je $\overline{\rho}$ permutacija od $\Omega = (\mathbb{F}_q^{\times})^2$ definirana kot $\overline{\rho}(\omega) = \rho(-\omega)$, $\omega \in \Omega$. Ker je t primitivni element, velja $t^{\frac{q-1}{2}} = -1$. Zato lahko izračunamo naslednje:

$$\overline{\rho}(\omega) = \rho(-\omega) = (-\omega)t^2 = (-1)\omega t^2 = t^{\frac{q-1}{2}}\omega t^2 = \omega t^{2+\frac{q-1}{2}}.$$

Vemo:

$$\begin{aligned} \rho(\omega) &= \omega t^2 \\ \overline{\rho}(\omega) &= \omega t^{2+\frac{q-1}{2}}. \end{aligned}$$

Opazimo: če sta $1 + \frac{q-1}{4}$ in $\frac{q-1}{2}$ tuji, potem ima $\overline{r}$ samo eno orbito. Če nista tuji, ima dve orbiti. Spodaj bomo izačunali, da velja:

$$nsd(1 + \frac{q-1}{4}, \frac{q-1}{2}) = \begin{cases} 1 & \frac{q-1}{4} \text{ je soda} \\ 2 & \frac{q-1}{4} \text{ je liha.} \end{cases}$$

Naj bo $d = nsd(1+\frac{q-1}{4}, \frac{q-1}{2})$. Potem $d|(2(\frac{q-1}{4}+1)-(\frac{q-1}{2})) = 2$, torej $d = 1$ ali 2. Torej ima $\overline{\rho}$ en cikel, če je $\frac{q-1}{4}$ soda. Če pa je $\frac{q-1}{4}$ liha, ima dva cikla.

Če ima $\overline{\rho}$ en cikel, je $\sum_{\omega\in\Omega}\omega = 0$ in dobimo, da je perioda $m_1 = 1$.

Če ima $\overline{\rho}$ dva cikla, dobimo, da je $\sum_{\omega\in\Omega_1}\omega = 0$ in $\sum_{\omega\in\Omega_2}\omega = 0$. Če je $q > 5$ dobimo, da sta periodi $m_1 = m_2 = 1$. Če pa je $q = 5$, potem $m_1 = m_2 = 5$.

Sedaj lahko izačunamo rod:

$$4(g-1) = q(\frac{q-1}{2} - 2 - 2\sum_{i=1}^{t} 1/m_i) = q(\frac{q-5}{2} - 2q\sum_{i=1}^{t} 1/m_i).$$

Za $2q\sum_{i=1}^{t} 1/m_i$ imamo dve možnosti, če $q > 5$:

$$2q\sum_{i=1}^{t} 1/m_i = \begin{cases} 2q, & \text{če } q \equiv 1 \pmod 8 \\ 4q, & \text{če } q \equiv 5 \pmod 8). \end{cases}$$

Torej rod g za $q > 5$ je enak

$$4(g-1) = \begin{cases} \dfrac{q^2-9q}{2}, & \text{če } q \equiv 1 \pmod 8 \\ \dfrac{q^2-13q}{2}, & \text{če } q \equiv 5 \pmod 8). \end{cases}$$

$$g = \begin{cases} \dfrac{q^2-9q}{8} + 1, & \text{če } q \equiv 1 \pmod 8 \\ \dfrac{q^2-13q}{8} + 1, & \text{če } q \equiv 5 \pmod 8). \end{cases}$$

□

7 Zaključek

Skozi zaključno nalogo smo s pomočjo poznavanja končnih polj in permutacijskih grup spoznali nekaj lastnosti Paleyevih grafov in zemljevidov. Obstaja pa še veliko lastnosti in zanimivosti o Paleyevih grafih v [2–4, 11, 12].

8 Literatura

[1] D. Bajc in T. Pisanski, *Najnujnejše o grafih*, Društvo matematikov, fizikov in astronomov SRS, Ljubljana 1985. *(Citirano na strani 7.)*

[2] N. L. Biggs in A. T. White, *Permutation groups and combinatorial structures*, London Math. Soc. Lecture Notes Ser. 33, Cambridge Univ. Press, Cambridge 1979. *(Citirano na straneh 1, 2, 8, 9, 17, 19, 21, 23 in 25.)*

[3] P.J. Cameron in D. Stark, *A prolific construction of strongly regular graphs with the n-e.c. property*, Queen Mary, University of London. *(Citirano na strani 25.)*

[4] A.N. Elsawy, *Paley Graphs and Their Generalizations*, Heinrich Heine University, Dusseldorf, Germany, for the Degree of Master of Science 2009. *(Citirano na strani 25.)*

[5] J.B. Fraleigh, *A First Course In Abstract Algebra*, Addison-Wesley, 7th edition, 2002 . *(Citirano na strani 3.)*

[6] M. Juvan in P. Potočnik, *Teorija grafov in kombinatorika*, DMFA - založništvo, Ljubljana 2007. *(Citirano na strani 7.)*

[7] I. Kovács, *Permutacijske grupe*, Zapiski 2014. *(Citirano na strani 5.)*

[8] J.H. van Lint in R.M. Wilson, *A Course in Combinatorics - 2nd edition*, Cambridge University Press, Cambridge 2001. *(Citirano na strani 3.)*

[9] R. J. Wilson in J. J. Watkins, *Uvod v teorijo grafov*, Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana 1997. *(Citirano na strani 7.)*

[10] J. Žerovnik, *Osnove teorije grafov in diskretne optimizacije*, Fakulteta za strojništvo, Maribor 2005 (druga izdaja). *(Citirano na strani 7.)*

[11] *Paleyjevi grafi*, `http://mathworld.wolfram.com/PaleyGraph.html`. (Datum ogleda: 15. 2. 2014.) *(Citirano na straneh 8 in 25.)*

[12] *Paley graf*,
`http://en.wikipedia.org/wiki/Paleygraph`. (Datum ogleda: 10. 9. 2014.) *(Citirano na strani 25.)*