UNIVERZA NA PRIMORSKEM
Fakulteta za matematiko, naravoslovje in informacijske tehnologije

Matematika – 1. stopnja

Marija Jurkovič

Rank 3 grupe in krepko regularni grafi

Zaključna projektna naloga

Mentorica: doc. dr. Klavdija Kutnar

Koper, 2011

UNIVERSITY OF PRIMORSKA
Faculty of Mathematics, Natural Sciences and Information Technologies

Mathematics – 1^{st} degree

Marija Jurkovič

Rank 3 groups and strongly regular graphs

Final Project Paper

Mentor: doc. dr. Klavdija Kutnar

Koper, 2011

Zahvala

Zahvaljujem se mentorici doc. dr. Klavdiji Kutnar za pomoč pri nastajanju zaključne projektne naloge. Za vso podporo, vzpodbujanje in vloženi čas.

Poljubček Nastji in Vidi za 3-letno fenomenalno sodelovanje pri študiju in vsemu, kar sodi zraven. Ostanita vedno taki super matematični zagrizenki.

Hvala prijateljem in vsem tistim, ki so mi v teh zadnjih treh letih znali narisati nasmeh na obrazu.

Objemček moji družini in fantu, ker ste mi stali ob strani in me razumeli tudi, ko sem bila na meji nemogočega.

Posebna hvala pa gre moji mami, ki je žal danes ni več med nami. Dala si mi veliko in neskončno te pogrešam.

Hvala vsem.

Povzetek

Zaključna projektna naloga proučuje rank 3 grupe in krepko regularne grafe. Krepko regularni grafi imajo poleg tega, da so regularni, še eno zanimivo lastnost. Število skupnih sosedov dveh točk v grafu je odvisno le od tega, ali sta ti dve točki povezani ali nepovezani. Rank 3 grupe pa so tranzitivne grupe, za katere velja, da imajo natanko 3 orbite pri delovanju na množici $X \times X$. V zaključni projektni nalogi bomo dokazali, da vsaka rank 3 grupa porodi krepko regularen graf in opisali lastnosti teh grafov. Spoznali bomo tudi Paleyjeve grafe in dokazali, da so krepko regularni.

Abstract

In the final project paper we explore rank 3 groups and strongly regular graphs. Beside being regular, strongly regular graphs possess one other interesting property. The number of common neighbours of two vertices depends only on whether the two vertices are connected or not. Rank 3 groups are transitive groups that have 3 orbits on a set $X \times X$. In the final project paper we will prove that from every rank 3 group we can derive a strongly regular graph and will describe the properties of these graphs. We will also take a look at the Paley graphs and prove that they are strongly regular.

Math. Subj. Class. (2010): 05E30

Ključne besede: rank 3 grupa, orbitala, krepko regularni grafi
Keywords: rank 3 group, orbital, strongly regular graphs

Kazalo

Slike

Poglavje 1

Uvod

Pojem krepko regularnih grafov je prvi vpeljal Bose, in sicer leta 1963. Leto kasneje je Higman začel raziskovati povezavo med rank 3 grupami in krepko regularnimi grafi. Glede na te letnice lahko sklepamo, da je veja raziskovanja rank 3 grafov (v nadaljevanju bomo tako pravili krepko regularnim grafom, na katerih deluje rank 3 grupa) razmeroma mlada in se tako s kombinatoričnega kot tudi z grupnega vidika še vedno razvija.

Krepko regularni grafi imajo to lastnost, da je število skupnih sosedov dveh točk v grafu odvisno le od tega, ali sta ti dve točki povezani ali ne. Z algebraičnega vidika je graf krepko regularen graf natanko takrat, ko ima matrika sosednosti natanko tri lastne vrednosti. Krepko regularen graf pa ima tudi nekaj zelo zanimivih algebraičnih lastnosti, ki so ravno posledica krepke regularnosti. Spoznali bomo nekaj takih grafov, med njimi sta tudi Petersenov graf (glej sliko 7.1) in Hoffman-Singletonov graf (glej sliko 1.1).

Veliko krepko regularnih grafov je znanih po tem, da imajo zelo velike grupe avtomorfizmov [11]. V [11] je prav tako omenjeno, da je skoraj vsak krepko regularen graf asimetričen. V algebraični teoriji grafov je graf asimetričen, ko je neusmerjen in nima netrivialnih simetrij. Zanimivo je tudi omeniti trditev Petra Camerona, ki pravi, da krepko regularni grafi ležijo na prelomu med visoko strukturiranimi in ne strukturiranimi grafi. Čeprav so krepko regularni grafi zelo obsežno raziskovani, povezava med parametri, s katerimi je krepko regularen graf podan, in močjo grupe avtomorfizmov tega grafa še vedno ni dobro poznana. Več o avtomorfizmih grafa si lahko preberete v [11]. Pojem krepko regularnega grafa se je uveljavil tudi v tako imenovanem izreku Friendship Theorem [19].

V pričujoči zaključni projektni nalogi bomo predstavili nekaj dejstev, ki so pomembna za to vejo algebraične teorije grafov. Projektna naloga je razdeljena na devet poglavij, in sicer: Uvod, O grupah, Osnovne lastnosti grafov, Matrike in lastne vrednosti, Orbitale in rank 3 grupe, Rank 3 grafi, Krepko regularni grafi in njihove lastnosti, Paleyevi grafi in njihove lastnosti, Zaključek.

V drugem poglavju bomo najprej navedli potrebne definicije, izreke in trditve iz teorije grup, ki jih bomo potrebovali v naslednjih poglavjih. Definirali bomo nekatere od družin grup, definirali delovanje na grupah, uvedli pojme, kot sta orbita in stabilizator, in definirali relacije med njimi.

Tretje poglavje bomo namenili spoznavanju grafov. Definirali bomo nekatere od relacij med točkami, ki so vsebovane v grafu, in uvedli pojem avtomorfizma grafa.

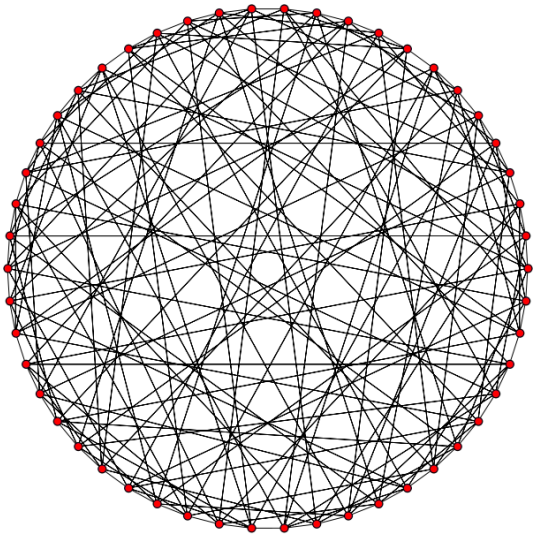
V četrtem poglavju bomo na kratko predstavili matriko sosednosti in lastne vrednosti.

V petem poglavju se bomo približali glavni temi zaključne projektne naloge in spoznali pojem orbitale, primitivnosti grupe ter definirali rank 3 grupo.

Šesto poglavje je namenjeno rank 3 grafom, kjer bomo povezali pojma rank 3 grupe s pojmom krepko regularnega grafa. V tem razdelku bomo tudi dokazali, da vsaka rank 3 grupa premore krepko regularen graf.

V sedmem poglavju si bomo ogledali lastnosti krepko regularnih grafov. V drugem razdelku bomo poudarili povezanost parametrov (n, k, λ, μ), pri čemer je n število točk, ki so vsebovane v grafu, k regularnost grafa, λ število skupnih sosedov dveh povezanih točk in μ število skupnih sosedov dveh nepovezanih točk. Izračunali bomo tudi lastne vrednosti krepko regularnih grafov in njihove večkratnosti.

V osmem poglavju bomo podrobneje spoznali eno od družin krepko regularnih grafov, in sicer družino Paleyevih grafov. Ti grafi so posebni zaradi vseh lastnosti, ki jih posedujejo.



Slika 1.1: Hoffman-Singletonov graf [22]

Poglavje 2

O grupah

Da bi razumeli vsebino zaključne projektne naloge, je nujno potrebno poznavanje grup in njihovih lastnosti. Zato bomo v tem poglavju spoznali grupe in grupna delovanja. Vedno bomo imeli opravka s končnimi grupami.

2.1 Osnovne lastnosti grup

Definicija 2.1.1 *Binarna operacija $\star$ na neprazni množici G je poljubna preslikava $\star$: $G \times G \to G$. Pri čemer je slika elementa $(x, y) \in G \times G$ enaka $\star(x, y) = x \star y = k \in G$. Urejenemu paru $(G, \star)$ pravimo grupoid.*

Definicija 2.1.2 *Urejenemu paru $(G, \star)$ pravimo grupa, če za binarno operacijo $\star$ velja:*

i) asociativnost: za vse $x, y, z \in G$ velja

$$(x \star y) \star z = x \star (y \star z),$$

ii) obstoj nevtralnega elementa: obstaja tak $e \in G$, da za poljuben $x \in G$ velja

$$x \star e = e \star x = x,$$

iii) obstoj inverznega elementa: za vsak $x \in G$ obstaja tak $x' \in G$, da je

$$x \star x' = e = x' \star x.$$

Definicija 2.1.3 *Neprazna podmnožica $H \subseteq G$ je podgrupa v grupi $(G, \star)$, ko je tudi sama grupa glede na operacijo $\star$. Oznaka: $(H, \star) \leq (G, \star)$.*

V nadaljevanju bomo operacijo $\star$ imenovali kar množenje in grupo $(G, \star)$ označevali krajše le z G. Nevtralni element bomo označevali z id, 0 ali 1. Inverz danega elementa x pa bomo označevali z x^{-1}.

Trditev 2.1.4 *Podmnožica H v grupi G je podgrupa, če za vsak $x, y \in H$ velja:*

i) $id_G \in H$,

ii) $xy \in H$,

iii) $x^{-1} \in H$.

Dokaz si lahko pogledate v [7].

Definicija 2.1.5 *Naj bo G grupa. Red grupe G je kardinalnost množice G. Oznaka: $|G|$. Red elementa $g \in G$ je najmanjše naravno število $r \in \mathbb{N}$, da velja $g^r = e$, kjer je e nevtralni element grupe G.*

Definicija 2.1.6 *Naj bo G grupa in S podmnožica grupe G. Potem obstaja najmanjša podgrupa grupe G, ki vsebuje S. Oznaka: $\langle S \rangle$. Pravimo, da S generira podgrupo $\langle S \rangle$.*

Primer 2.1.7 *Naj bo $G = \mathbb{Z}$ in $S = \{1\}$. Potem je $\langle S \rangle = \mathbb{Z}$. Če je $S = \{2\}$, pa je $\langle S \rangle = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$.*

Definicija 2.1.8 *Simetrična grupa S_X neprazne množice X je grupa vseh permutacij (bijektivnih preslikav) množice X z operacijo sestavljanja preslikav.*

Simetrično grupo S_X na množici $X = I_n = \{1, 2, \ldots, n\}$ označujemo z oznako S_n in njen nevtralni element, ki ga imenujemo tudi identiteta, označujemo z oznako id_n.

Definicija 2.1.9 *Permutacijska grupa G je neka podgrupa $G \leq S_X$ za poljubno množico X.*

Definicija 2.1.10 *Diedrska grupa D_{2n} je grupa simetrij pravilnega n-kotnika. Generirata jo rotacija ρ in zrcaljenje τ:*

$$D_{2n} = \langle \rho, \tau \mid \rho^n = \tau^2 = id, \tau\rho\tau = \rho^{-1} \rangle.$$

Hitro se lahko prepričamo, da je red simetrične grupe S_n enak $n!$ in red diedrske grupe D_{2n} enak $2n$.

Definicija 2.1.11 *Permutacija $g \in S_X$ je cikel dolžine k, če v množici X obstajajo taki različni elementi $x_1, \ldots, x_k$, da veljajo naslednje enakosti:*

i) ${x_i}^g = x_{i+1}$ *za vsak* $i \in \{1, \ldots, k-1\}$,

ii) ${x_k}^g = x_1$,

iii) $x^g = x$ *za vsak* $x \in X \setminus \{x_1, \ldots, x_k\}$.

Cikel g *označujemo z* $(x_1 \ldots x_k)$. *Ciklu dolžine* 2 *pravimo transpozicija, ciklu dolžine* $m \geq 2$ *pa* m*-cikel.*

Pravimo, da sta cikla $\alpha, \beta \in S_n$ ločena, če permutirata različne elemente množice I_n. Vsako permutacijo lahko zapišemo kot produkt ločenih ciklov. In vsako permutacijo lahko zapišemo kot produkt transpozicij. Le-ta ni enoličen, je pa enoličen do sodosti/lihosti števila transpozicij natančno (glej [10]).

Primer 2.1.12 *Naj bo* (1 2 4 5 3) *permutacija iz simetrične grupe* S_5. *Potem jo lahko zapišemo kot produkt transpozicij, in sicer kot*
(1 2)(1 4)(1 5)(1 3) *ali* (5 3)(4 5)(2 4)(1 2).

Za razumevanje definicije 2.1.14 vpeljimo naslednjo relacijo na množicah.

Definicija 2.1.13 *Relacija* R *na množici* X *je ekvivalenčna relacija, če veljajo naslednje lastnosti:*

i) (refleksivnost) $\forall x \in X : xRx$,

ii) (simetričnost) $\forall x, y \in X : xRy \Longrightarrow yRx$,

iii) (tranzitivnost) $\forall x, y, z \in X : xRy$ *in* $yRz \Longrightarrow xRz$.

Naj bo R ekvivalenčna relacija na množici X. Potem je ekvivalenčni razred $[x]_R$ elementa $x \in X$ glede na relacijo R množica vseh tistih elementov množice X, ki so z elementom x v relaciji R, tj. $[x]_R = \{y \in X \mid xRy\}$.

Definicija 2.1.14 *Naj bo* H *podgrupa grupe* G. *Definiramo relacijo na* G *takole:*

$$x \sim y \Longleftrightarrow x^{-1}y \in H.$$

Izkaže se, da je relacija iz definicije 2.1.14 ekvivalenčna relacija in da je ekvivalenčni razred, ki pripada elementu x, levi odsek $xH = \{xh | h \in H\}$. Podobno definiramo desne odseke.

Poglejmo si še poseben primer ekvivalenčnih razredov, ki jih bomo potrebovali v poglavju 8.

Primer 2.1.15 *Naj bo* $G = \mathbb{Z}$. *Definirajmo relacijo* $\sim^n$ *na množici* G *na sledeči način:* $x, y \in \mathbb{Z} : x \sim^n y$ *natanko tedaj, ko velja, da je* $x - y$ *večkratnik števila* n. *Izkaže se, da je* $\sim^n$ *ekvivalenčna relacija. Pripadajoči ekvivalenčni razredi so razredi ostankov pri deljenju z* n. *Množico vseh ekvivalenčnih razredov označujemo z* $\mathbb{Z}_n = \{[x]_{\sim^n} \mid x \in \mathbb{Z}\}$. *Konkreten primer:* $\mathbb{Z}_3 = \{[0]_{\sim^3}, [1]_{\sim^3}, [2]_{\sim^3}\}$. *Kar pišemo površno kar* $\{0, 1, 2\}$.

Izkaže se, da je $\mathbb{Z}_n$, skupaj z operacijo seštevanja, grupa reda n. Imenujemo jo aditivna grupa $\mathbb{Z}_n$.

Lema 2.1.16 *Elementi aditivne grupe $\mathbb{Z}_n$, ki so tuji številu n, tvorijo grupo za množenje po modulu n. Imenujemo jo multiplikativna grupa enot $\mathbb{Z}_n^*$.*

Dokaz si lahko preberete v [10].

Definicija 2.1.17 *Naj bosta $(G, *)$ in $(H, \circ)$ grupi. Potem je preslikava $f : G \to H$ homomorfizem grup, če za vsak $x, y \in G$ velja:*

$$f(x * y) = f(x) \circ f(y).$$

Definicija 2.1.18 *Naj bo $f : G \to H$ homomorfizem grup.*

i) Če je f injektivna preslikava, potem f imenujemo monomorfizem.

ii) Če je f surjektivna preslikava, potem f imenujemo epimorfizem.

iii) Če je f monomorfizem in epimorfizem, potem f imenujemo izomorfizem.

iv) Če je $G = H$, potem f imenujemo enodomorfizem.

v) Če je f izomorfizem in endomorfizem, potem f imenujemo avtomorfizem.

2.2 Grupna delovanja

Definicije, trditve, lema in izrek so povzeti po [5].

Definicija 2.2.1 *Grupa G deluje na množici X (X je G-prostor) z desne, če za vsak urejeni par $(x, g) \in X \times G$ obstaja tak $x^g \in X$, da je*

i) $x^1 = x$ za vsak $x \in X$, kjer je 1 nevtralni element grupe G,

ii) $(x^g)^h = x^{(gh)}$ za vsak $x \in X$ in vse $g, h \in G$.

Podobno lahko definiramo levo delovanje (glej [7]). Desno delovanje grupe G na množici X bomo krajše poimenovali kar delovanje grupe G na množici X.

Delovanje permutacije g na element x bomo v nadaljevanju označevali z $g(x)$ ali z x^g. Oznaki sta ekvivalentni.

Definicija 2.2.2 *Orbita elementa $x \in X$, pri delovanju grupe G na množici X, je množica:*

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

Ko bo grupa G delovala na množici X na naraven način, bomo $Orb_G(x)$ označevali kar z $Orb(x)$.

Trditev 2.2.3 *Za orbiti $Orb(x_1)$ in $Orb(x_2)$, pri delovanju grupe G na množici X, velja:*

$$Orb(x_1) \cap Orb(x_2) = \emptyset \quad ali \quad Orb(x_1) = Orb(x_2).$$

Dokaz. Naj imata orbiti $Orb(x_1)$ in $Orb(x_2)$ skupen element x'. To pomeni, da je $x' = x_i^{g_i}$ za nek $g_i \in G$, kjer je $i \in \{1, 2\}$. Zato je

$$\begin{aligned} Orb(x_i) &= \{x_i^g \mid g \in G\} \\ &= \{x_i^{g_i g_i^{-1} g} \mid g \in G\} \\ &= \{x'^{g_i^{-1} g} \mid g \in G\} \\ &= \{x'^g \mid g \in G\} = Orb(x'). \end{aligned}$$

■

Definicija 2.2.4 *Stabilizator elementa $x \in X$, pri delovanju grupe G na množici X, je množica:*

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

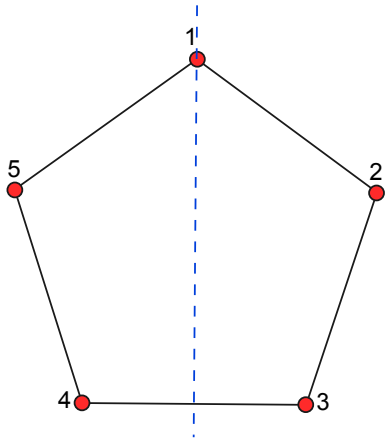
Primer 2.2.5 *Naj bo G podgrupa simetriče grupe S_5 generirana s permutacijama* (1 2 3 4) *in* (2 5)(4 3)*. Po kratkem razmisleku ugotovimo, da je grupa G izomorfna diedrski grupi D_{10}.*

V splošnem lahko diedrsko grupo D_{2n} predstavimo s pravilnim n-kotnikom, pri čemer element ρ predstavlja rotacije, element τ pa zrcaljenja pravilnega n-kotnika.

Za lažjo predstavo in razumevanje primerov bomo v bodoče bili površni in simetrično grupo G, ki je izomorfna diedrski grupi D_{2n}, kar enačili z D_{2n}.

Poiščimo orbito elementa 1*. Zanima nas, kam vse se ogliščе* 1 *preslika z elementi iz diedrske grupe D_{10}. Ker imamo na izbiro vse rotacije in zrcaljenja, hitro vidimo, da je orbita $Orb(1) = \{1, 2, 3, 4, 5\}$.*

Poiščimo še stabilizator elementa 1*. Poglejmo, kateri elementi fiksirajo ogliščе* 1*. Ker so rotacije generirane s* 5*-ciklom, se hitro prepričamo, da vsak element iz $\langle$(1 2 3 4 5)$\rangle$, razen identitete, preslika element* 1 *v enega od elementov iz množice $\{2, 3, 4, 5\}$. Preostanejo nam še zrcaljenja. Element, ki prezrcali petkotnik in fiksira* 1*, je en sam, in sicer* (2 5)(3 4) *(kot kaže slika 2.1). Torej množica stabilizatorjev elementa* 1 *je $G_1 = \{id, (2\ 5)(3\ 4)\}$.*



Slika 2.1: Modra premica je simetrijska os zrcaljenja, ki je predstavljena kot involucija (2 5)(3 4).

Trditev 2.2.6 *Stabilizator G_x, pri delovanju grupe G na množici X, je podgrupa grupe G.*

Dokaz. Po trditvi 2.1.4 moramo preveriti tri točke.

i) Naj bo id_G nevtralni element grupe G. Po definiciji delovanja stabilizatorja G_x sledi, da je $x^{id_G} = x$.

ii) Naj bosta $g_1, g_2 \in G_x$ in $x \in X$. Torej velja $x^{g_1} = x$ in $x^{g_2} = x$. Potem je:

$$x^{g_1 g_2} = (x^{g_1})^{g_2} = x^{g_2} = x.$$

Torej je $g_1 g_2 \in G_x$.

iii) Naj bo element $g \in G_x$ in element $x \in X$. Potem sledi:

$$\begin{aligned} x &= x^g \\ x^{g^{-1}} &= x^{gg^{-1}} \\ x^{g^{-1}} &= x. \end{aligned}$$

Sledi, da je g^{-1} vsebovan v stabilizatorju G_x.

■

Izrek 2.2.7 *(Lema 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

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

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

$$|\omega| \;=\; \sum_{g\in G} |\{x' \in Orb(x) \mid x^g = x'\}| \;= \sum_{g\in G} 1 = |G|. \qquad (2.1)$$

Drugič pa, da 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:

$$\sum_{x'\in Orb(x)} |\{g \in G \mid x^g = x'\}| \;= \sum_{x'\in Orb(x)} |G_x| \;= |Orb(X)| \cdot |G_x|. \qquad (2.2)$$

Dokaz izreka sledi iz točk (2.1) in (2.2). ■

Definicija 2.2.8 *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 (tj. $x^g = y$).*

Definicija 2.2.9 *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.

Naj bo B podmnožica G-prostora X in naj bo $g \in G$. Potem pišemo $B^g = \{x^g \mid x \in B\}$ in $G_{\{B\}}$ je podmnožica v G, ki je definirana na sledeči način: $G_{\{B\}} = \{g \in G \mid B^g = B\}$. Izkaže se, da je $G_{\{B\}}$ podgrupa v G.

Definicija 2.2.10 *Podmnožica B tranzitivnega G-prostora X je blok, če velja, da je $B^g = B$ ali $B^g \cap B = \emptyset$ za vsak $g \in G$.*

Naj bo X tranzitiven G-prostor. Hitro se prepričamo, da so množice $\{x\}$ za vsak $x \in X$ in cela množica X bloki. Imenujemo jih trivialni bloki.

Če je B blok, potem $|B|$ deli $|X|$ in velja, da vse podmnožice B^g za $g \in G$ tvorijo particijo množice X. To particijo imenujemo sistem blokov.

Definicija 2.2.11 *Grupa G deluje na množici X primitivno, če deluje tranzitivno in ima G-prostor X samo trivialne bloke.*

Trditev 2.2.12 *Če je B blok tranzitivnega G-prostora X in je $x \in B$, potem je $B \setminus \{x\} = O_1 \cup \ldots \cup O_n$, kjer so O_i orbite stabilizatorja G_x.*

Dokaz. $B \setminus \{x\} = O_1 \cup \ldots \cup O_n$ lahko zapišemo tudi kot $B = O_0 \cup O_1 \cup \ldots \cup O_n$, kjer je O_0 orbita z enim samim elementom, in sicer x. Dokazujemo s protislovjem. Recimo, da obstaja neka orbita z vsaj dvema elementoma, tako da je en element v enem bloku, drugi element pa v drugem bloku. Torej obstaja $\alpha \in G$, tako da $x^\alpha = x$ in $y^\alpha = z$, kjer $x, y \in B_1$ in $z \in B_2$. To nas vodi v protislovje, saj sta x in y iz istega bloka (vemo pa, da za blok B velja: $B^g = B$ ali $B^g \cap B = \emptyset$). ■

Primer 2.2.13 *Grupa D_{10} deluje na množici $X = \{1, 2, 3, 4, 5\}$ primitivno. Gledamo simetrije petkotnika. Zaradi rotacij se lahko hitro prepričamo, da je delovanje tranzitivno. Ker pa vemo, da moč blokov deli moč množice X in je 5 praštevilo, imamo le trivialne bloke.*

Primer, ko imamo netrivialne bloke, si bomo ogledali na koncu poglavja 3, saj bomo za razumevanje primera potrebovali še nekaj novih definicij.

Definicija 2.2.14 *Binarna relacija $\sim$ na G-prostoru X je G-invariantna, če velja:*

$$x_1 \sim x_2 \Longrightarrow x_1^g \sim x_2^g \text{ za vsak } x_1, x_2 \in X \text{ in } g \in G.$$

Binarno relacijo $\sim$ na tranzitivnem G-prostoru X imenujemo G-kongruenca, če je hkrati ekvivalenčna relacija in G-invariantna.

Trditev 2.2.15 *Particija Δ tranzitivnega G-prostora X je sistem blokov natanko tedaj, ko je pripadajoča relacija $\sim_\Delta$ G-kongruenca.*

Dokaz. Naj bo Δ poljubna particija množice X in naj $\sim_\Delta$ označi ekvivalenčno relacijo, ki pripada particiji Δ. Torej velja: $x_1 \sim_\Delta x_2 \Longleftrightarrow x_1$ in x_2 pripadata istemu razredu v Δ, kjer sta $x_1, x_2 \in X$.

Najprej predpostavimo, da je particija Δ sistem blokov G-prostora X. Naj bosta $x_1, x_2 \in X$ taka, da je $x_1 \sim_\Delta x_2$. Naj bo $g \in G$. Potem obstaja tak $B \in \Delta$, da $x_1, x_2 \in B$. Ker je Δ sistem blokov, dobimo, da je $B^g \in \Delta$. Iz tega sledi, da je $x_1^g \sim_\Delta x_2^g$. Po definiciji je relacija G-kongruenca.

Sedaj predpostavimo, da je relacija $\sim_\Delta$ G-kongruenca. Izberemo poljubno množico B iz Δ. Dovolj je pokazati, da je B blok G-prostora X. Naj bo $g \in G$ tak, da je $B \cap B^g \neq \emptyset$. To pomeni, da obstaja nek element $x_1 \in B$, da je $x_1^g \in B$. Naj bo zdaj x_2 poljuben element iz B. Ekvivalenca, $x_1 \sim_\Delta x_2 \Longleftrightarrow x_1$ in x_2 pripadata istemu razredu v Δ, pove, da je $x_1 \sim_\Delta x_2$. To implicira, da je $x_1^g \sim_\Delta x_2^g$. Torej sta x_1^g in x_2^g iz istega razreda v Δ. Ta razred pa mora biti B, saj je $x_1^g \in B$. Dobili smo, da je $B^g \subseteq B$. Enakost $B = B^g$ sledi iz tega, da je $|B| = |B^g|$. Po definiciji je B blok G-prostora X. Trditev je dokazana. ■

Podgrupi H in K grupe G sta konjugirani, če za nek element $g \in G$ velja, da je $H = g^{-1}Kg$. Kjer z $g^{-1}Kg$ označimo množico $\{g^{-1}kg \mid k \in K\}$.

Trditev 2.2.16 *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.

Dokaz. Po lemi orbita stabilizator (izrek 2.2.7) za vsak $x \in X$ velja naslednja enakost $|G| = |Orb(x)| \cdot |G_x|$. Ker pa je $Orb(x) = X$, saj G deluje tranzitivno na X, sledi točka (i). Poglejmo razred konjugiranosti podgrup v G, ki je definiran takole:

$$R = \{G_x^g = g^{-1}G_x g \mid g \in G\}.$$

Dokaz točke (ii) zaključimo tako, da pokažemo enakost:

$$R = \{G_z \mid z \in X\}. \tag{2.3}$$

Naj bo najprej G_x^g poljubna podgrupa iz R in pišimo y za element x^g. Potem za poljuben $g_1 \in G_x^g$ velja, da je $g_1 = g^{-1}g_2 g$ za nek element $g_2 \in G_x$. Sledi, da je $y^{g_1} = (x^g)^{g^{-1}g_2 g} = y$. To pomeni, da je G_x^g podgrupa v G_y. Zaradi tranzitivnosti je

$$|G_x^g| = |G_x| = \frac{|G|}{|X|} = |G_y|,$$

zato je $G_x^g = G_y$ in $R \subseteq \{G_z \mid z \in X\}$. Po drugi strani pa je stabilizator G_z, kjer je z poljuben element iz X, enak grupi $G_x^{g_3}$, kjer je g_3 izbran tako, da je $x^{g_3} = z$. Iz tega sledi, da je $\{G_z \mid z \in X\} \subseteq R$, kar dokazuje točko (2.3). ■

Lema 2.2.17 *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.*

Dokaz. Ker je G tranzitivna, je $y = x^g$ za nek $g \in G$. Iz točke (ii) trditve 2.2.16 sledi, da je $G_y = g^{-1}G_x g$. Naj bo O poljubna orbita stabilizatorja G_x,

$$O = Orb(z) = \{z^s \mid s \in G_x\}.$$

Permutacija g preslika O v $O^g = \{z^{sg} \mid s \in G_x\}$. To se piše kot

$$O^g = \{(z^g)^{g^{-1}sg} \mid s \in G_x\} = \{(z^g)^{s'} \mid s' \in g^{-1}G_x g\}.$$

Dobili smo, da je slika O^g enaka orbiti $Orb_{G_y}(z^g)$ pri delovanju stabilizatorja G_y. Da lahko razločimo orbite G_x od orbit G_y, pišemo $Orb_{G_x}(z)$ in

$Orb_{G_y}(z^g)$. Na tak način g definira preslikavo $\overline{g}$ iz množice orbit stabilizatorja G_x v množico orbit stabilizatorja G_y, torej

$$\overline{g} : Orb_{G_x}(z) \mapsto Orb_{G_y}(z^g).$$

Da dokončamo dokaz, pokažimo, da je preslikava $\overline{g}$ bijektivna. Surjektivnost sledi iz dejstva, da je g permutacija množice X. Naj bo $Orb_{G_y}(z_1^g) = Orb_{G_y}(z_2^g)$ za neka elementa $z_1, z_2 \in X$. To pomeni, da je $z_2^g = (z_1^g)^{s'}$ za nek $s' \in G_y$. Ker je $G_y = g^{-1}G_x g$, je $s' = g^{-1}sg$ za nek $s \in G_x$ in je $z_2^g = (z_1^g)^{s'} = (z_1^g)^{g^{-1}sg} = (z_1^s)^g$. Iz tega sledi, da je $z_2 = z_1^s$, zato je $Orb_{G_x}(z_1) = Orb_{G_x}(z_2)$. Dobili smo, da je $\overline{g}$ tudi injektivna, zato je bijektivna. ■

Definicija 2.2.18 *Rank tranzitivne permutacijske grupe $G \leq S_n$ je število orbit stabilizatorja G_x za nek element $x \in X$.*

Primer 2.2.19 *Rank simetrične grupe S_n je 2. O tem se prepričajmo takole: naj bo G simetrična grupa S_n in naj bo $n \neq 1$. Oglejmo si stabilizator G_1. Zanima nas število orbit tega stabilizatorja. Ker je G_1 stabilizator elementa 1, je $\{1\}$ ena orbita. Če pogledamo element 2, se lahko hitro prepričamo, da se z G_1 preslika v vsak drugi element razen v 1. Zato imamo dve orbiti, in sicer $\{1\}$ in $\{2, \ldots, n\}$.*

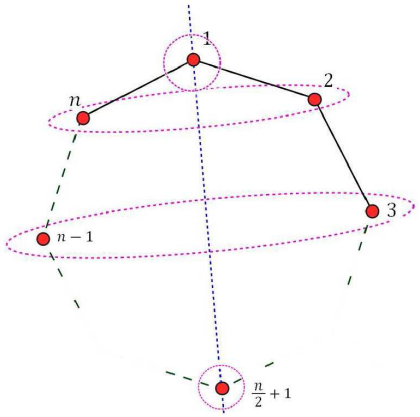
Primer 2.2.20 *Rank diedrske grupe D_{2n}, ko je n liho število, je $\frac{n-1}{2} + 1$, ko pa je n sodo, je $\frac{n-2}{2} + 2$. Da to drži, se prepričajmo takole:*

Naj bo n sodo število. Oglejmo si stabilizator elementa x. Brez škode za splošnost lahko vzamemo za $x = 1$. Vemo, da je D_{2n} generirana z rotacijami in zrcaljenji n-kotnika. Hitro se lahko prepričamo, da z nobeno rotacijo n-kotnika ne bomo fiksirali 1. Torej noben element rotacije ne bo vsebovan v stabilizatorju G_1.

Preverimo, katera zrcaljenja fiksirajo 1. Poznamo dve vrsti zrcaljen, in sicer skozi nasprotni si vozlišči n-kotnika ter skozi nasprotni stranici. Edino zrcaljenje, ki fiksira 1, je zrcaljenje skozi nasprotni si vozlišči, in sicer v našem primeru 1 in $(\frac{n}{2} + 1)$.

Od vseh n točk odštejemo 2, ki sta s tem zrcaljenjem fiksirani. Ker sta po dve točki v orbiti (kot kaže slika 2.2), delimo $n - 2$ z 2 in prištejemo 2, ker sta točki 1 in $(\frac{n}{2} + 1)$ vsaka v svoji orbiti.

Sledi: rank diedrske grupe D_{2n}, ko je n sodo število, je $\frac{n-2}{2} + 2$.



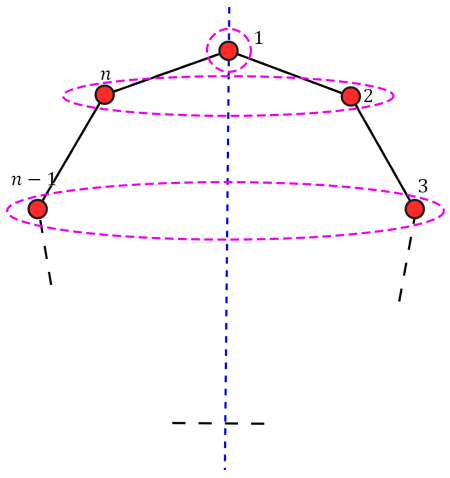
Slika 2.2: Pravilni n kotnik, kjer je n sodo število.

Naj bo n liho število. Oglejmo si stabilizator elementa x. Brez škode za splošnost lahko vzamemo za $x = 1$. Vemo, da je D_{2n} generirana z rotacijami in zrcaljenji n-kotnika. Kot smo se prepričali v zgornjem primeru, velja, da noben element rotacije ne bo vsebovan v stabilizatorju G_1.

V primeru, ko je n liho število, poznamo zrcaljenje skozi vozilšče in njemu nasprotno stranico. Torej če hočemo fiksirati vozlišče 1, zrcalimo n-kotnik prek simetrale, ki poteka skozi 1.

Od vseh n točk odštejemo 1, saj je ena točka fiksirana. Ker sta po dve točki v orbiti (kot kaže slika 2.3), delimo $n - 1$ z 2 in prištejemo 1, ker je fiksirana točka ena sama.

Sledi: rank diedrske grupe D_{2n}, ko je n liho število, je $\frac{n-1}{2} + 1$.



Slika 2.3: Pravilni n kotnik, kjer je n liho število.

Zapišimo še izrek iz [10], ki ga bomo potrebovali v poglavju 5, ko bomo dokazovali, da grupa sodega reda premore netrivialno sebizrcalno orbitalo.

Izrek 2.2.21 (Cauchyjev izrek) *Če praštevilo p deli moč končne grupe G, potem grupa G premore element reda p.*

Dokaz. Naj bo $n = |G|$. Bodi

$$X = \{(a_1, a_2, \ldots, a_p) \in G^p \mid \prod_{i=1}^{p} a_i = 1\}.$$

Očitno je $|X| = n^{p-1}$. Naj bo ciklična grupa $C = \langle c \rangle$ generirana z elementom c. Naj c deluje na množico X na sledeči način:

$$(a_1, a_2, \ldots, a_p)^c = (a_2, a_3, \ldots, a_p, a_1).$$

Po trditvi (2.2.7) so orbite delovanja grupe C na množico X dolžine p in 1. Naj bo r število orbit dolžine 1 in s število orbit dolžine p. Potem je $r + ps = n^{p-1}$. Ker p deli n, sledi, da p deli r. Poleg tega je $r > 0$, saj je element $(1, 1, \ldots, 1)$ sam v svoji orbiti, ker je $(1, 1, \ldots, 1)^c = (1, 1, \ldots, 1)$. Zato je $r \geqslant p > 1$ in posledično v grupi G obstaja element $a \in G$, tako da je $(a, a, \ldots, a) \in X$. Po definiciji množice X sledi, da je $a^p = 1$. ■

Poglavje 3

Osnovne lastnosti grafov

Da se lahko začnemo ukvarjati z grafi, moramo prvo le-te definirati in spoznati nekatere njihove lastnosti. Sledi nekaj novih pojmov in primerov. V mislih bomo imeli končne grafe.

Definicija 3.0.1 *Digraf je urejeni par* $\overrightarrow{\Gamma}= (V, E)$*, kjer je* V *neprazna množica. Elemente te množice imenujemo točke ali vozlišča.* E *je podmnožica množice* $V \times V$*. Elemente te množice imenujemo loki.*

Definicija 3.0.2 *Graf* (V, E) *je digraf, za katerega velja:*

i) za vsak $\alpha \in V$ *velja, da* $(\alpha, \alpha) \notin E$ *(nima zank),*

ii) za vsak $\alpha, \beta \in V$ *velja, če* $(\alpha, \beta) \in E \Longrightarrow (\beta, \alpha) \in E$*.*

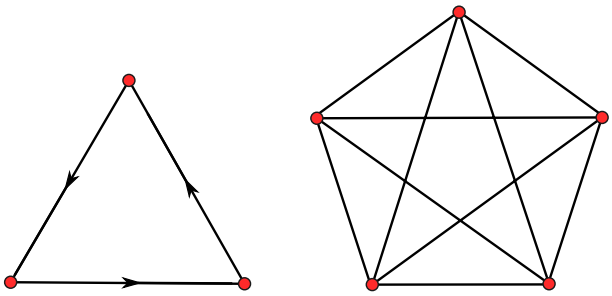
Točke digrafa $\overrightarrow{\Gamma}$ označujemo tudi z $V(\overrightarrow{\Gamma})$ in loke z $E(\overrightarrow{\Gamma})$. V grafu Γ je za vsak lok (α, β) tudi (β, α) lok. Zato par takšnih dveh lokov nadomestimo z neusmerjeno povezavo $\{\alpha, \beta\}$.

Definicija 3.0.3 *Stopnja točke* u *v grafu* Γ*, označimo jo z* $deg_\Gamma(u)$ *ali* $d_\Gamma(u)$*, je število povezav v grafu* Γ*, ki imajo točko* u *za svoje krajišče.*

Točkam stopnje 0 pravimo izolirane točke, točkam stopnje 1 pa listi. Najmanjšo stopnjo točke grafa Γ označimo z $\delta(\Gamma)$, največjo pa z $\Delta(\Gamma)$.

Definicija 3.0.4 *Graf* Γ *je regularen, če velja* $\delta(\Gamma) = \Delta(G)$*, in* $d-$*regularen, če velja* $d = \delta(G) = \Delta(G)$*.*

Primer 3.0.5 *Na sliki 3.1 vidimo digraf na treh točkah in* 4*-regularen graf na petih točkah.*



Slika 3.1: Digraf in graf

Definicija 3.0.6 *Naj bo Γ graf in u točka grafa Γ. Množici točk, s katerimi je u povezana, pravimo množica sosedov točke.*

Definicija 3.0.7 *Sprehod (dolžine k) je niz k povezav v grafu*

$$(u,x)(x,y)\dots(t,z)(z,w).$$

Temu sprehodu lahko rečemo tudi sprehod med točkama u in w. Povezave niso usmerjene, zato predstavlja niz

$$(w,z)(z,t)\dots(y,x)(x,u)$$

isti sprehod. Pogosto sprehod pišemo samo z zaporedjem točk na danem nizu povezav:

$$uxy\dots tzw.$$

Sprehod je enostaven, ko so vse vsebovane povezave v sprehodu različne. Enostaven sprehod je pot, ko so vse točke $v_0, v_1, \dots, v_k$ med seboj različne. Enostavni sprehod je cikel, ko so vse točke $v_0, v_1, \dots, v_{k-1}$ med seboj različne in je $v_0 = v_k$.

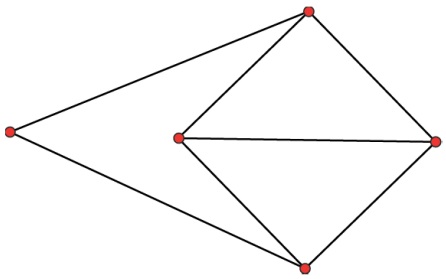
Definicija 3.0.8 *Izomorfizem iz grafa Γ v graf $\overline{\Gamma}$ je bijektivna preslikava $f : V(\Gamma) \to V(\overline{\Gamma})$, za katero velja:*

$$\forall u, v \in V(\Gamma) \text{ sledi, da: } \{u,v\} \in E(\Gamma) \iff \{f(u), f(v)\} \in E(\overline{\Gamma}).$$

Definicija 3.0.9 *Razdaljo $d_\Gamma(u,v)$ med točkama $u, v \in V(\Gamma)$ v grafu Γ definiramo kot dolžino najkrajše poti od u do v v Γ.*

Definicija 3.0.10 *Največji razdalji med parom poljubnih dveh točk pravimo diameter oz. premer grafa Γ:*

$$diam(\Gamma) = max\{d_\Gamma(u,v) \mid u, v \in V(\Gamma)\}.$$



Slika 3.2: Graf z diametrom 2 in obsegom 3

Definicija 3.0.11 *Obseg grafa je dolžina najkrajšega cikla v grafu.*

Primer 3.0.12 *Diameter grafa na sliki 3.2 je 2. Njegov obseg pa 3.*

Definicija 3.0.13 *Naj bo Γ graf. Grafu $\overline{\Gamma}$ z isto množico točk kot graf Γ, v katerem sta dve točki sosedni natanko tedaj, ko nista sosedni v grafu Γ, pravimo komplementarni graf (tudi komplement) grafa Γ.*

Definicija 3.0.14 *Avtomorfizem grafa Γ je permutacija $g \in S_{V(\Gamma)}$, za katero velja:*

$$\{v_1, v_2\} \in E(\Gamma) \Longleftrightarrow \{v_1^g, v_2^g\} \in E(\Gamma) \text{ za vsak } \{v_1, v_2\} \in E(\Gamma).$$

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

Sedaj imamo na voljo dovolj znanja, da pogledamo obljubljeni primer, ko pri delovanju grupe G na množico X G-prostor premore tudi netrivialne bloke. Ker si bomo za primer ogledali hiperkocko, jo pred tem še definirajmo.

Definicija 3.0.15 *Hiperkocka Q_n dimenzije n je graf, ki je definiran takole:*

i) $V(Q_n) = \{0,1\}^n = \mathbb{Z}_2^n$,

ii) $E(Q_n)$ *vsebuje tiste množice* $\{(a_i), (b_i)\}$, *kjer* $(a_i), (b_i) \in \{0,1\}^n$, *za katere velja, da je moč množice* $\{i \in \{1, \ldots, n\} \mid a_i \neq b_i\}$ *enaka 1.*

Primer 3.0.16 *Pišimo $V = V(Q_3)$ in $G = Aut(Q_3)$. Naj bo $\pi \in S_3$. Lahko je dokazati, da je preslikava $\overline{\pi}$,*

$$\overline{\pi} : V \longrightarrow V,\ (a_1, a_2, a_3) \longmapsto (a_{\pi(1)}, a_{\pi(2)}, a_{\pi(3)}) \text{ za vsak } (a_1, a_2, a_3) \in V,$$

permutacija množice V in je $\overline{\pi}$ tudi avtomorfizem grafa Q_3. Z uporabo permutacij π lahko dobimo, da so orbite stabilizatorja $G_{(0,0,0)}$:

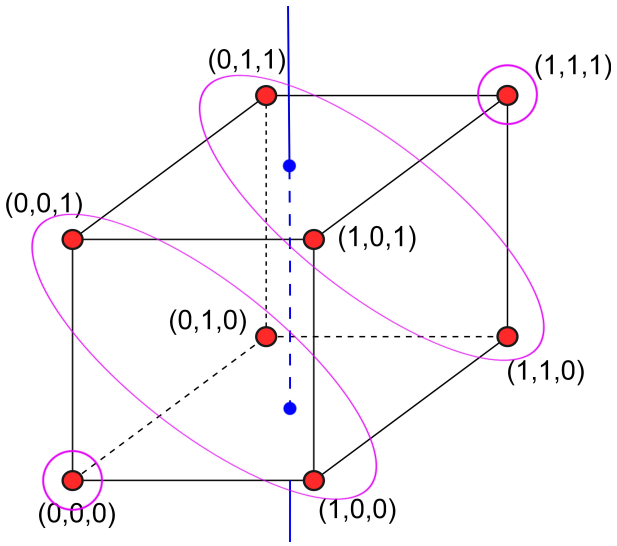
$V_1 = \{(0,0,0)\}$,
$V_2 = \{(1,0,0),(0,1,0),(0,0,1)\}$,
$V_3 = \{(1,1,0),(1,0,1),(1,1,0)\}$,
$V_4 = \{(1,1,1)\}$.

Naj bo B blok za permutacijsko grupo G, ki vsebuje $(0,0,0)$. Moč bloka B deli moč množice $V = \{0,1\}^3 = 8$. Iz 2.2.12 sledi, da je blok B unija nekaterih orbit stabilizatorja $G_{(0,0,0)}$. Iz tega sledi, da imamo naslednje možnosti: $B = V_1 \cup V_4$ ali $B = V_1 \cup V_2$ ali $B = V_1 \cup V_3$.

Hitro se lahko prepričamo, da $V_1 \cup V_2$ ni blok. Kocko zarotiramo za kot $\varphi = 90°$ skozi os, ki poteka skozi nasproti ležeči ploskvi (glej sliko 3.3). Tako dobimo, da $B \cap B^\varphi \neq \emptyset$ in hkrati $B \neq B^\varphi$. Torej B ne more biti blok.

Da je $V_1 \cup V_4$ res blok, lahko vidimo tako, da preverimo, da je relacija $\sim$ na V, ki je definirana takole: $(a_1,a_2,a_3) \sim (b_1,b_2,b_3)$ natanko tedaj, ko je moč množice $\{i \in \{1,2,3\} \mid a_i \neq b_i\}$ enaka 3 ali ko je $a_i = b_i$ $\forall i$, G-kongruenca. Množica $V_1 \cup V_4$ je razred pripadajoče particije.

Množica $V_1 \cup V_3$ je tudi blok, ker je razred particije, ki pripada G-kongruenci $\sim$, kjer je $\sim$ definirana takole: $(a_1,a_2,a_3) \sim (b_1,b_2,b_3)$ natanko tedaj, ko je moč množice $\{i \in \{1,2,3\} \mid a_i \neq b_i\}$ enaka 2 ali ko je $a_i = b_i$ $\forall i$.



Slika 3.3: Kocka

Za konec tega poglavja si poglejmo še definiciji induciranega podgrafa in razdaljno regularnega grafa, ki ju bomo potrebovali v poglavju 7.2.

Definicija 3.0.17 *Graf (V', E') je induciran podgraf grafa (V, E), če za poljuben par točk $u, v \in V'$ velja: $(u,v) \in E \Longrightarrow (u,v) \in E'$.*

Definicija 3.0.18 *Povezan graf* Γ *je razdaljno regularen, če je, za poljubni dve točki* $x, y \in \Gamma$ *in poljubni števili* $i, j \in \{0, 1, \ldots, d\}$ *(kjer je* d *diameter grafa), število točk na razdalji* i *od* x *in* j *od* y*, odvisno le od števil* i *in* j *ter od razdalje med točkama* x *in* y*, neodvisno pa od izbire* x *in* y*.*

Poglavje 4

Matrike in lastne vrednosti

Spoznajmo še, kaj so lastne vrednosti in lastni vektorji. Le-te bomo potrebovali v podpoglavjih 7.2 in 8.2. Za razumevanje spodnjih pojmov privzemimo, da že poznamo matrike in determinante.

Z J bomo označevali matriko, ki je sestavljena iz samih enic. Z I pa bomo označevali identično matriko, ki je sestavljena iz enic po diagonali (drugje se nahajajo ničle).

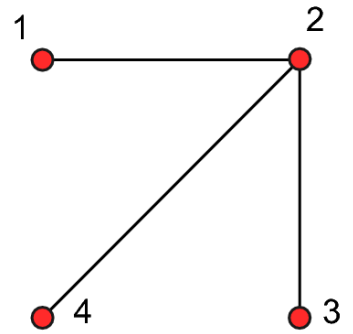
Definicija 4.0.1 *Matrika sosednosti grafa Γ s točkami iz množice $\{1, \ldots, n\}$ je kvadratna matrika $A(\Gamma) = [a_{ij}]$, kjer je $a_{ij} = 1$, če sta i in j povezana in $a_{ij} = 0$ sicer.*

Primer 4.0.2 *Na sliki 4.1 vidimo graf in pripadajočo matriko sosednosti.*

Definicija 4.0.3 *Naj bo $A \in \mathbb{R}^{n \times n}$ matrika velikosti $n \times n$. Potem vsoto $\sum_{i=1}^{n} a_{ii}$ vseh diagonalnih elementov matrike A imenujemo sled matrika A. Označimo jo s Sled(A).*

Že iz definicije matrike sosednosti sledi, da je sled matrike sosednosti enostavnega grafa enaka 0.

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



Slika 4.1: Matrika sosednosti danega grafa

Definicija 4.0.4 *Naj bo $A \in \mathbb{R}^{n\times n}$ matrika velikosti $n \times n$. Realno število λ je lastna vrednost matrike A, če za nek neničelni vektor $v \in \mathbb{R}^n$ velja: $Av = \lambda v$.*

Definicija 4.0.5 *Lastne vrednosti grafa Γ so lastne vrednosti njene matrike sosednosti $A(\Gamma)$.*

Opomba: Množici lastnih vrednosti grafa pravimo spekter grafa.

Definicija 4.0.6 *Karakteristični polinom grafa Γ je polinom $P_{A(\Gamma)}(x) = det(Ix - A(\Gamma))$.*

Definicija 4.0.7 *Naj bo Γ graf in λ neka lastna vrednost grafa Γ. Večkratnost lastne vrednosti λ je največje pozitivno število m, tako da $(x - \lambda)^m$ deli $P_{A(\Gamma)}(x)$.*

Trditev 4.0.8 *Naj bo A matrika velikosti $n \times n$. Vsota vseh večkratnosti lastnih vrednosti matrike A je enaka n.*

Dokaz si lahko preberete v [20].

Trditev 4.0.9 *Naj bo A matrika velikosti $n \times n$. Potem je $Sled(A)$ enaka vsoti lastnih vrednosti matrike A.*

Izreka ne bomo dokazali, saj bi za dokaz potrebovali tako imenovani Schurijev izrek [9].

Poglavje 5

Orbitale in rank 3 grupe

V tem poglavju se bomo počasi približali našemu glavnemu problemu. Spoznali bomo, kaj so to orbitale in kako orbitale določajo rank 3 grupo.

Definicija 5.0.1 *Naj bo G grupa, ki deluje na množici X. Potem definiramo delovanje grupe G na množici $X \times X$ na sledeči način:*

$$(x_1, x_2)^g := (x_1^g, x_2^g)\ \forall g \in G, \forall x_1, x_2 \in X.$$

Orbite grupe G na $X \times X$ imenujemo orbitale.

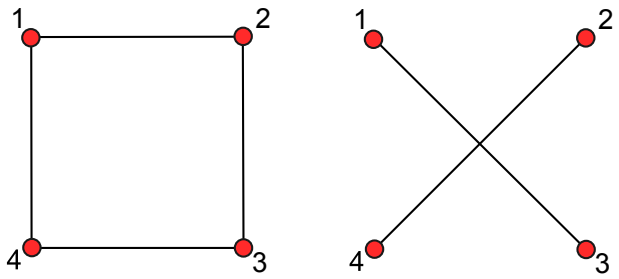
Orbitala $\{(x,x)|\ x \in X\}$ je trivialna orbitala. Če je $\Delta = \{(x,y)|\ x,y \in X\} \subseteq X \times X$ orbitala, potem je očitno tudi $\Delta^* = \{(y,x)|\ (x,y) \in \Delta\} \subseteq X \times X\}$ orbitala. Δ^* imenujemo zrcalna orbitala orbitale Δ. Orbitala Δ je sebizrcalna orbitala, če velja $\Delta = \Delta^*$. Pravimo ji tudi simetrična orbitala. Unijo G-orbital imenujemo posplošena orbitala.

Primer 5.0.2 *Naj bo G ciklična permutacijska grupa generirana s permutacijo* (1 2 3 4)*, ki na naraven način deluje na množici $X = \{1,2,3,4\}$. Pripadajoče orbitale so:*
$\Delta_0 = \{(1,1),(2,2),(3,3),(4,4)\}$ *(trivialna orbitala),*
$\Delta_1 = \{(1,2),(2,3),(3,4),(1,4),(4,1),(3,2),(2,1),(4,3)\}$,
$\Delta_2 = \{(1,3),(2,4),(3,1),(4,2)\}$.

Orbitali Δ_1 in Δ_2 sta sebizrcalni orbitali. Očitno je trivialna orbitala vedno sebizrcalna.

Definicija 5.0.3 *Orbitalni graf netrivialne sebizrcalne orbitale $\Delta \subseteq X \times X$ je graf, katerega točke so elementi množice X, povezave pa elementi orbitale Δ.*

Primer 5.0.4 *Slika 5.1 prikazuje grafa glede na sebizrcalni orbitali iz primera 5.0.2.*



Slika 5.1: Orbitalna grafa orbital Δ_1 in Δ_2 iz primera 5.0.2

Opomba: Če ne bi imeli sebizrcalne orbitale, bi dobili digraf.

Lema 5.0.5 *Naj grupa G deluje tranzitivno na množici X in naj bo $x \in X$. Potem obstaja bijekcija iz množice G-orbital na množico orbit stabilizatorja G_x na množici X.*

Dokaz. Naj bo preslikava φ definirana s predpisom $\varphi(\Delta) = \{y|(x,y) \in \Delta\}$, kjer je Δ neka G-orbitala. Najprej pokažimo, da je množica $\varphi(\Delta)$ invariantna za G_x.

Naj bo element $y \in \varphi(\Delta)$ in urejeni par $(x,y) \in \Delta$. Vzemimo poljuben $g \in G_x$ in preslikajmo par (x,y) na sledeči način:

$$(x,y)^g = (x^g, y^g) = (x, y^g).$$

Po definiciji stabilizatorja G_x sledi, da je $y^g \in \varphi(\Delta)$.

Naj bosta y_1 in y_2 poljubna elementa iz $\varphi(\Delta)$. Potem sta tudi para (x,y_1) in (x,y_2) elementa orbitale Δ. Ker je Δ orbitala, obstaja tak $g \in G$, da velja

$$(x,y_1)^g = (x,y_2).$$

Iz tega sledi, da je $x^g = x$ in ${y_1}^g = y_2$. To nas privede do dejstva, da je element $g \in G_x$ in da y_1 in y_2 pripadata isti G_x-orbiti. Pokazati moramo še, da je preslikava φ bijekcija iz množice G-orbital na množico orbit stabilizatorja G_x na X.

Najprej dokažimo surjektivnost: naj bo O orbita stabilizatorja G_x in element $y \in O$. Ker element y pripada neki G-orbitali, obstaja tak Δ, da je $(x,y) \in \Delta$. Torej Δ je iskana G-orbitala, ki se s preslikavo φ preslika v orbito O. Dokaz injektivnosti poteka takole: recimo, da sta Δ_1 in Δ_2 taki G-orbitali, da je $\varphi(\Delta_1) = \varphi(\Delta_2)$. Če je element y v preseku $\varphi(\Delta_1) \cap \varphi(\Delta_2)$, potem je par (x,y) vsebovan v Δ_1 in Δ_2. Ker pa sta Δ_1 in Δ_2 orbiti za

delovanje grupe G na množici $X \times X$, sta si bodisi disjunktni bodisi enaki. Ker pa obe vsebujeta element (x, y), sledi, da sta orbitali Δ_1 in Δ_2 enaki. ■

Definicija 5.0.6 *Naj bo G permutacijska grupa, ki deluje na množici X. Če je G tranzitivna na X in ima tri orbite na $X \times X$, potem jo imenujemo rank 3 grupa.*

Po lemi 5.0.5 sta definiciji 2.2.18 in 5.0.6 rank 3 grupe ekvivalentni.

Izrek 5.0.7 *Naj bo G tranzitivna permutacijska grupa na množici X. Grupa G je primitivna natanko tedaj, ko je vsak orbitalni digraf, ki pripada G-orbitali na X, povezan.*

Dokaz. Da dokažemo ekvivalenco, moramo dokazati obe implikaciji.
($\Longrightarrow$) Naj bo grupa G primitivna in naj bo $\Gamma = (X, E)$ orbitalni digraf, ki pripada G-orbitali E na X. Naj bo množica $\{\Delta_1, \ldots, \Delta_k\}$ particija množice X na množico točk povezanih komponent digrafa Γ. Torej $\omega_1, \omega_2 \in \Delta_i$ za nek i natanko tedaj, ko obstaja pot med ω_1 in ω_2. Pokazati moramo le, da je particija $\{\Delta_1, \ldots, \Delta_k\}$ G-invariantna.

Naj bo Δ_i element te particije in $\alpha \in \Delta_i$. Če je $\beta \in \Delta_i^g$, potem obstaja tak $\alpha' \in \Delta_i$, da velja $\beta = \alpha'^g$. Ker je $\alpha' \in \Delta_i$, potem obstaja pot $\alpha_0 = \alpha, \alpha_1, \ldots, \alpha_k = \alpha'$. Če preslikamo pot od α_0 do α' z elementom g, dobimo pot od α^g do $\alpha'^g = \beta$. Torej je Δ_i^g vsebovana v povezani komponenti od α^g. Podobno lahko pokažemo, da je tudi komponenta od α^g vsebovana v Δ_i^g. Torej je ${\Delta_i}^g$ povezana komponenta, ki vsebuje α^g. Iz tega sledi, da grupa G permutira elemente množice $\{\Delta_1, \ldots, \Delta_k\}$ in da je množica $\{\Delta_1, \ldots, \Delta_k\}$ G-invariantna particija množice X. Ker je Γ orbitalni graf, mora biti takšna povezana komponenta velikosti vsaj 2. Grupa G je primitivna, zato sledi, da je $k = 1$ in $\Delta_1 = X$. Torej je graf Γ povezan.
($\Longleftarrow$) Predpostavimo zdaj, da grupa G deluje tranzitivno na množici X in da je vsak orbitalni graf, ki pripada neki G-orbitali, povezan. Naj bo $\{\Delta_1, \ldots, \Delta_k\}$ taka G-invariantna particija množice X, da je moč množice Δ_1 vsaj 2 (posledično to velja za vsak Δ_i). Naj bosta elementa $\alpha, \beta \in \Delta_1$ in $E = (\alpha, \beta)^G$ orbita elementa $(\alpha, \beta) \in X \times X$ pri delovanju grupe G na $X \times X$. Potem je E G-orbitala. Naj bo $(\gamma, \delta) \in E$, tako da je $\gamma \in \Delta_1$.

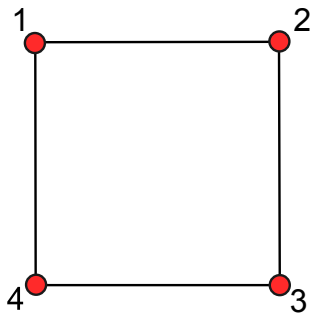
Ker grupa G deluje tranzitivno na orbiti E, obstaja tak element $g \in G$, da je $(\alpha, \beta)^g = (\gamma, \delta)$. Torej velja $\alpha^g = \gamma$ in $\beta^g = \delta$.

Vemo tudi, da je $\gamma = \alpha^g \in \Delta_1 \cap \Delta_1^g$, in ker je Δ_1 blok, vemo, da je $\Delta_1^g = \Delta_1$. Ker je $\beta \in \Delta_1$, to implicira, da je $\beta^g = \delta \in \Delta_1$. Torej, če je začetna točka nekega loka vsebovana v Δ_1, potem je tudi končna točka tega loka vsebovana v Δ_1. Podoben argument pokaže, da se nič ne spremeni, če zamenjamo vlogi začetne in končne točke. Zato Δ_1 vsebuje točke povezane kompomente grafa Γ.

Po predpostavki je Γ povezan, zato sledi, da je $\Delta_1 = X$, in torej je grupa G primitivna. ■

Primer 5.0.8 *Naj bo* $G = \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle$ *grupa izomorfna diedrski grupi reda* 8, *ki deluje na množici* $X = \{1, 2, 3, 4\}$. *Geometrijsko se tako grupo da predstaviti s pravilnim* 4*-kotnikom, kar nam bo pomagalo v nadaljevanju. Pripadajoče* G*-orbitale so:*
Δ_0 *(trivialna orbitala),*
$\Delta_1 = \{(1\ 2), (2\ 1), (2\ 3), (3\ 4), (4\ 1), (1\ 4), (4\ 3), (3\ 2)\}$,
$\Delta_2 = \{(1\ 3), (2\ 4), (3\ 1), (4\ 2)\}$.

Poglejmo si stabilizator elementa $1 \in X$*: na podoben način, kot smo poiskali stabilizator elementa v primeru 2.2.20, se prepričamo, da je stabilizator oglišča* 1 *enak* $G_1 = \{(2\ 4), id\}$. *Pri tem ugotovimo, da je pri delovanju grupe* G_1 *na* X *oglišče* 1 *v svoji orbiti, posledično tudi njemu najbolj oddaljeno oglišče* 3 *je v svoji orbiti, oglišči* 2 *in* 4 *pa sta v isti orbiti. Torej so* G_1*-orbite:* $\{1\}, \{3\}, \{2, 4\}$. *Naj bo* Γ *graf, ki ga dobimo na sledeči način:* $V(\Gamma) = X$, *točka* 1 *je povezana s točkami iz* G_1*-orbite* $\{2, 4\}$. *Za poljuben* $g \in G$ *točko* 1^g *povežemo z elementi iz* $\{2, 4\}^g$.



Slika 5.2: Graf Γ

Dobili smo graf (na sliki 5.2), ki je izomorfen grafu, ki pripada orbitali Δ_1.

Izrek 5.0.9 *Naj* G *deluje na množici* X *tranzitivno in naj bo* G *sodega reda. Potem obstaja vsaj ena netrivialna sebizrcalna orbita* Δ *na* $X \times X$.

Dokaz. Ker je G sodega reda, potem po izreku 2.2.21 G premore element g reda 2, ki zamenja nek par (x, y), kjer sta x in y različna. Naj bo Δ orbitala, ki vsebuje (x, y). Potem Δ vsebuje tudi (y, x), saj $(x, y)^g = (y, x)$. Ker pa je (x, y) element orbitale Δ, potem za poljuben $(x', y') \in \Delta$ obstaja tak $h \in G$, da velja $(x, y)^h = (x', y')$. Torej $x^h = x'$ in $y^h = y'$. Iz tega sledi: $((x, y)^g)^h = (y, x)^h = (y', x') \in \Delta$. Torej Δ je res sebizrcalna. ■

Poglavje 6

Rank 3 grafi

Še enkrat poglejmo zadnji izrek 5.0.9. Če G deluje na množici X tranzitivno in je sodega reda, obstaja netrivialna sebizrcalna orbita Δ na $X \times X$. V takem primeru lahko konstruiramo graf Γ, ki ima za točke elemente množice X in pare $\{p, q\}$, kjer sta (p, q) in (q, p) iz Δ, kot povezave. Imenujemo ga rank n graf, kjer je n rank grupe G.

Izrek 6.0.1 *Naj bo G tranzitivna permutacijska grupa ranka 3 in sodega reda, ki deluje na množici X. Potem obstaja rank 3 graf Γ, ki premore grupo G kot grupo avtomorfizmov.*

Dokaz. Grupa G ima le dve različni netrivialni orbiti glede na urejene pare (orbitali), in sicer Δ_1 in Δ_2.

Vemo, da je za vsako orbitalo Δ množica $\Delta^* = \{(y, x) | (x, y) \in \Delta\}$ tudi orbitala. Torej, ali ${\Delta_1}^* = \Delta_1$ ali ${\Delta_1}^* = \Delta_2$. Ker pa je G sodega reda, po 2.2.21, vsebuje element g reda 2. Ta element zamenja dve točki $x, y \in X$. Če je torej $(u, v) \in \Delta_i$, je $(u, v)^g = (v, u) \in {\Delta_i}^*$ za vsak $u, v \in X$. Po definiciji množice ${\Delta_i}^*$ torej sledi ${\Delta_i}^* = \Delta_i$. Torej imamo rank 3 graf.

Zdaj vzemimo graf Γ, katerega množica točk je X. Če sta x in y sosedna, potem $(x, y) \in \Delta_1$. Argumenti nam povedo, da je graf neusmerjen. Potem očitno premore grupo avtomorfizmov G ranka 3. ■

Primer prav takih grafov smo videli v primeru 5.0.4. Imenovali smo jih orbitalni grafi.

Izrek 6.0.2 *Naj bo G tranzitivna grupa na množici X ranka 3. Naj bo Δ_1 ($\neq \Delta_0$) sebizrcalna orbitala pri delovanju grupe G na množici X in Γ pripadajoči orbitalni graf. Potem velja:*

i) za poljubni sosedni točki grafa Γ obstaja konstantno število točk (npr. λ), ki so sosedne obema,

ii) za poljubni različni nesosedni točki grafa Γ obstaja konstantno število točk (npr. μ), ki so sosedne obema.

Dokaz. Ker imamo grupo ranka 3, imamo 3 orbitale. Naj bo Γ orbitalni graf glede na orbitalo Δ_1. Za poljubna dva elementa x, y iz X definiramo $N(x,y) = \{z \in X | (x,z) \in \Delta_1 \text{ in } (y,z) \in \Delta_1)\}$. Torej $N(x,y)$ je množica točk iz Γ, ki so sosedne obema x in y.

i) Če sta x in y sosedna, potem je $(x,y) \in \Delta_1$. Podobno, če sta x' in y' sosedna, imamo $(x',y') \in \Delta_1$. Ker pa je Δ_1 orbita, obstaja nek $g \in G$ tako, da velja $x^g = x'$ in $y^g = y'$. Preslikava iz $z \mapsto z^g$ je bijektivna preslikava iz $N(x,y)$ v $N(x',y')$, tako da velja $|N(x,y)| = |N(x',y')| = \lambda$.

ii) Če sta x in y poljubna različna nesosedna elementa, potem par (x,y) pripada netrivialni orbitali Δ_2. In za drugi dve poljubni različni nepovezani točki spet velja, da je par $(x',y') \in \Delta_2$. Podobno kot pri prvi točki obstaja nek $\overline{g} \in G$ tako, da $x^{\overline{g}} = x'$ in $y^{\overline{g}} = y'$. S podobno razlago kot zgoraj, le da zamenjamo g z $\overline{g}$ in dobimo $|N(x,y)| = |N(x',y')| = \mu$.

■

Poglavje 7

Krepko regularni grafi in njihove lastnosti

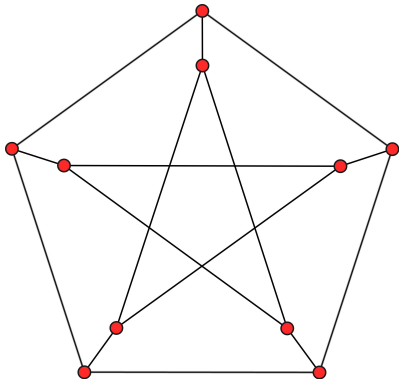
7.1 Krepko regularni grafi

Za lažje razumevanje nadaljnje vsebine zaključne projektne naloge bomo na primeru Petersenovega grafa predstavili nekaj novih pojmov. Kot je splošno znano, ima Petersenov graf veliko pomembnih značilnosti. Velikokrat ga lahko navedemo kot primer ali protiprimer k neki lastnosti.

Če na hitro osvežimo spomin in pogledamo sliko 7.1, vidimo, da ima Petersenov graf 10 točk, valenca vsake točke je 3, ima diameter 2 in obseg 5.

Seveda te značilnosti niso naključne in med seboj neodvisne. Po definiciji Mooreovih grafov [6], sledi, da ima graf s stopnjo 3, diametrom 2 in obsegom 5 vsaj 10 točk. Primer takega grafa je tudi Petersenov graf.

Če nekatere zgoraj naštete lastnosti zapišemo v zaporedje $(10, 3, 0, 1)$, pridemo do definicije krepko regularnega grafa.



Slika 7.1: Petersenov graf

Definicija 7.1.1 *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 iz grafa Γ velja, da imata natanko λ skupnih sosedov,

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

Poglejmo si nekaj primerov krepko regularnih grafov.

Primer 7.1.2 *Mrežni grafi.*

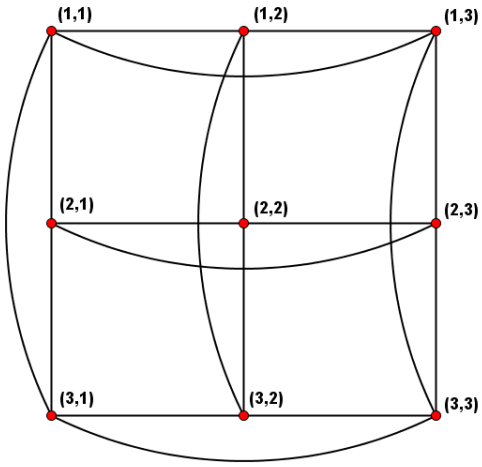
Naj bo $S = \{1, \ldots, n\}$, potem so točke grafa urejeni pari $(i, j) \in S \times S$. Točki (i, j) in (a, b) sta povezani, če velja $i = a$ ali $j = b$.

Naredimo premislek, da je tako nastali graf krepko regularen.

Graf ima n^2 točk in je $2n-2$ regularen. Dve točki sta povezani, če se nahajata v istem stolpcu ali isti vrstici, zato si delita ravno $n-2$ sosedov. Nepovezani točki pa imata natanko dva skupna soseda, in sicer robova kvadrata, ki ga nepovezani točki "tvorita".

Torej mrežni grafi so krepko regularni grafi s parametri $(n^2, 2n-2, n-2, 2)$.

Primer mrežnega grafa na 9 točkah je prikazan na sliki 7.2.



Slika 7.2: Mrežni graf

Primer 7.1.3 *Grafi, nastali iz latinskega kvadrata [3].*

Latinski kvadrat je $n \times n$ preglednica, ki vsebuje števila od 1 do n, tako da se nobeno ne pojavi dvakrat v isti vrstici oziroma stolpcu. Preprost primer vidimo na sliki 7.3.

Iz takega latinskega kvadrata definiramo graf, ki ima n^2 točk (vsaka za eno celico iz preglednice). Dve točki (i, j) in (a, b) sta povezani, če $i = a$ ali $j = b$ ali če sta vrednosti pri (i, j) in (a, b) enaki.

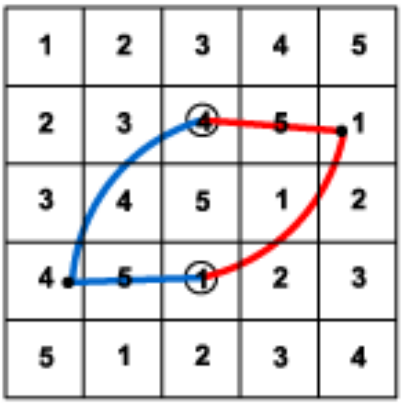
Naredimo premislek, da je tako nastali graf krepko regularen.

Že vemo, da ima graf n^2 točk. Je $3n-3$ regularen: poljubna točka je povezana s celo vrstico (razen sama s sabo), s celim stolpcem (razen sama s sabo) in z vsemi točkami, ki imajo enako vhodno vrednost (razen sama s sabo). Torej poljubna točka je povezana s $3(n-1)$ drugimi točkami.

Dve povezani točki (a_i, b_i) in (a_i, b_j), ki se nahajata v istem stolpcu, si delita ravno $n-2$ sosedov. Imata pa še dva skupna soseda: točko, ki se nahaja v isti vrstici kot (a_i, b_i) in ima vhodno vrednost enako kot (a_i, b_j) in obratno (glej sliko 7.3). Očitno velja enako za vrstice. Ni težko preveriti, da velja podobno tudi za povezani točki z enako vhodno vrednostjo. Torej imata dve povezani točki v takem grafu n skupnih sosedov.

Poglejmo si še dve poljubni nepovezani točki. Brez škode za splošnost vzemimo kar $(1, 1)$ in $(2, 2)$. Ti dve se nahajata v različnih stolpcih in različnih vrsticah in imata različni vhodni vrednosti (sicer bi bili povezani). V svoji vrstici ima točka $(1, 1)$ dva skupna soseda s točko $(2, 2)$: točko $(1, 2)$ in točko, ki ima enako vhodno vrednost kot $(2, 2)$. Podobno velja za stolpec. Na koncu pa lahko najdemo še dve skupni sosedi točke $(2, 2)$, ki se nahajata v različnih vrsticah in stolpcih. Pogledamo vrstico/stolpec točke $(2, 2)$ in v njej/njem najdemo točko z isto vhodno vrednostjo kot $(1, 1)$. Torej imata dve nepovezani točki v takem grafu natanko 6 skupnih sosedov.

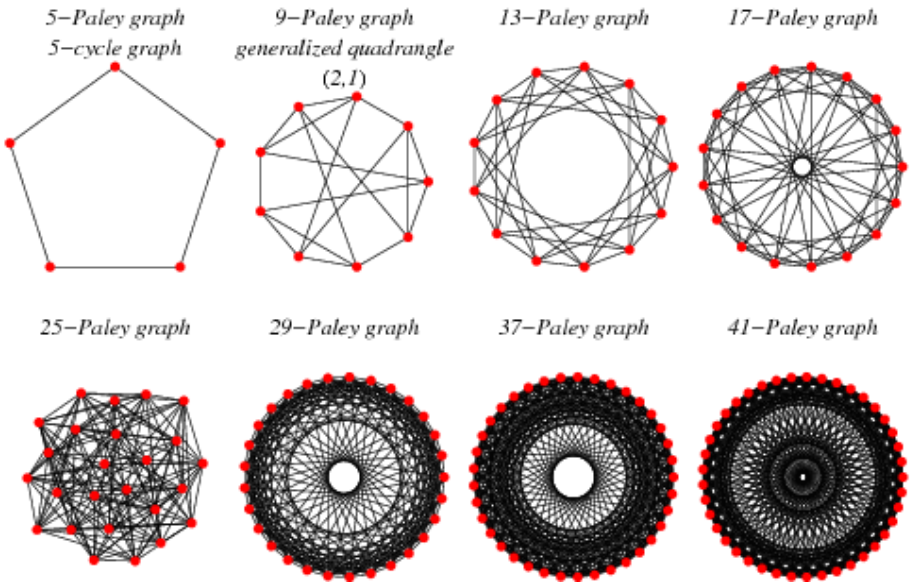
Iz tega sledi, da so to krepko regularni grafi s parametri $(n^2, 3n-3, n, 6)$.



Slika 7.3: Latinski kvadrat

Primer 7.1.4 *Paleyjevi grafi:*

Ker so krepko regularni grafi definirani na posebno lep način, so tudi njihove grafične predstavitve, torej slike, vredne ogleda. Poseben primer takih grafov so na primer Paleyjevi grafi (glej sliko 7.4).



Slika 7.4: Paleyjevi grafi [21]

Podrobneje bomo te grafe spoznali v poglavju 8.

Primer 7.1.5 *Točkovni in povezavni grafi:*

Da dobimo občutek, da so krepko regularni grafi res obsežna družina grafov, omenimo še tako imenovane točkovne in povezavne grafe. Oboji so krepko regularni. Ne bomo pa jih definirali, saj ne poznamo pojmov, kot sta parcialna geometrija in incidenčna struktura. S temi grafi se lahko seznanite v članku [17].

Med drugim obstaja še nekaj posplošitev ali "variant" krepko regularnih grafov, kot so na primer: razdaljno regularni grafi, asociativne sheme, po poteh regularni grafi, povezavno regularni grafi, Deza grafi in krepki grafi. Več o tem si lahko preberete v 7. poglavju Cameronovega članka [17].

7.2 Lastnosti krepko regularnih grafov

V tem podpoglavju se bomo osredotočili na lastnosti krepko regularnih grafov. V mislih bomo vedno imeli nepolne in neprazne grafe. Saj je očitno, da so vsi polni grafi K_n in prazni grafi nK_1 krepko regularni, pri katerih pa λ in μ nista definirana. Zato bomo odslej obravnavali le grafe, ki niso izomorfni ne K_n ne nK_1.

Trditev 7.2.1 *Naj bo Γ krepko regularen graf s parametri (n, k, λ, μ). Potem velja:*

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

Dokaz. Fiksirajmo točko x. Naj bo y poljuben sosed točke x. Kandidatov za takšno točko je k, saj je k stopnja točke x. Poglejmo zdaj, koliko povezav je med y in točkami, ki niso sosedne točki x. Točka y je sosedna k točkam, od tega odštejemo točke, ki so hkrati sosedne x in y, in točko x. Torej število povezav, ki povezujejo točke, ki so sosedne točki x, in točke, ki niso sosedne točki x, je enako $k(k - \lambda - 1)$.

Preštejmo število povezav v grafu Γ, ki povezujejo točke, ki so sosedne točki x, in točke, ki niso sosedne točki x še na drugi način. Naj bo zdaj z poljubna nesosedna točka točke x. Kandidati za takšno točko so vse točke brez k točk, s katerimi je povezana x in brez točke x. Torej jih je $(n-k-1)$. Po definiciji imata točki x in z μ skupnih sosedov. Torej je število povezav, ki povezujejo točke, ki so sosedne točki x, in točke, ki niso sosedne točki x, hkrati enako $(n - k - 1)\mu$. S tem smo dokazali enakost.

■

Primer 7.2.2 *Prepričajmo se, da enakost velja za Petersenov graf. Le-ta ima parametre $(10, 3, 0, 1)$. Torej, če v enakost $k(k - \lambda - 1) = (n - k - 1)\mu$ vstavimo vrednosti $n = 10$, $k = 3$, $\lambda = 0$ in $\mu = 1$, dobimo: $3(3 - 0 - 1) = (10 - 3 - 1)1$. Vidimo, da enakost drži.*

Izrek 7.2.3 *Če krepko regularen graf Γ s parametri (n, k, λ, μ) obstaja, potem velja ali*

i) $k = 2\mu$ *in* $\lambda = \mu - 1$ *ali*

ii) $(\lambda-\mu)^2+4(k-\mu)$ *je popoln kvadrat, recimo* s^2 *in izraz* $m = (k/2\mu s)((k-1+\mu-\lambda)(s+\mu-\lambda)-2\mu)$ *je pozitivno celo število.*

Dokaz izreka si lahko preberete v knjigi [13].
Sledeča trditev je povzeta po [2].

Trditev 7.2.4 *Naj bo Γ krepko regularen graf s parametri (n, k, λ, μ). Potem je komplement grafa Γ krepko regularen graf $\overline{\Gamma}$ s parametri $(n, l, l-k+\mu-1, l-k+\lambda+1)$, pri čemer je $l = n-k-1$.*

Dokaz. Označimo parametre grafa $\overline{\Gamma}$ takole: $(\overline{n}, \overline{k}, \overline{\lambda}, \overline{\mu})$.

- Število točk grafa $\overline{\Gamma}$ je enako številu točk grafa Γ, zato je $\overline{n} = n$.
- V grafu $\overline{\Gamma}$ so povezane ravno tiste točke, ki so v grafu $\overline{\Gamma}$ nepovezane in obratno, zato velja $\overline{k} = l$ in $\overline{l} = k$.
- Število skupnih sosedov dveh povezanih točk v grafu $\overline{\Gamma}$ je enako:

$$\overline{\lambda} = n - 2k + \mu - 2 = 1 + k + l - 2k + \mu - 2$$

$$\overline{\lambda} = l - k + \mu - 1.$$

- Število skupnih sosedov dveh nepovezanih točk v grafu $\overline{\Gamma}$ je enako:

$$\overline{\mu} = n - 2k + \lambda = 1 + k + l - 2k + \lambda$$

$$\overline{\mu} = l - k + \lambda + 1.$$

Torej so parametri krepko regularnega grafa $\overline{\Gamma}$ $(\overline{n}, \overline{k}, \overline{\lambda}, \overline{\mu})$ res enaki $(n, l, l-k+\mu-1, l-k+\lambda+1)$.

■

Izrek 7.2.5 *Krepko regularen graf Γ s parametri (n, k, λ, μ) je povezan natanko tedaj, ko $\mu \neq 0$.*

Dokaz. Da dokažemo ekvivalenco, moramo dokazati obe implikaciji.
($\Longrightarrow$) Recimo, da graf Γ ni povezan. Potem obstajata nepovezani točki x in y, ki seveda nimata skupnega soseda. Ker je Γ krepko regularen, to velja za vsako točko, ki ni povezana z x. Zato sledi, da je $\mu = 0$.
($\Longleftarrow$) Recimo, da je $\mu = 0$. Ker je Γ nepoln krepko regularen graf, mora biti sestavljen iz disjunktne unije polnih grafov iste velikosti. Torej je graf Γ nepovezan. ■

Trditev 7.2.6 *Povezan krepko regularen graf ima diameter* 2.

Dokaz. Pokazati želimo, da sta poljubni dve točki v grafu na oddaljenosti največ 2. Zato si poglejmo dve poljubni nepovezani točki. Po definiciji krepko regularnega grafa imata dve nepovezani točki μ sosedov. In ker je naš graf povezan, torej $\mu \neq 0$, vemo, da imata ti dve točki vsaj enega skupnega soseda. Zato je oddaljenost med tema dvema točkama ravno 2. ■

Spoznajmo še lastne vrednosti krepko regularnih grafov.

Trditev 7.2.7 *Naj bo* Γ k*-regularen graf na* n *točkah in* A *njegova matrika sosednosti. Potem je* k *lastna vrednost grafa* Γ.

Dokaz. Naj bo v vektor, ki je sestavljen iz samih enic. Ker je Γ $k-$regularen, velja $Av = kv$. Tako je k lastna vrednost grafa Γ. ■

Trditev 7.2.8 *Naj bo* Γ *povezan regularen graf stopnje* k *in* $\{v_1, \ldots, v_n\}$ *množica točk tega grafa. Potem je večkratnost lastne vrednosti* k *enaka* 1.

Dokaz. Naj bo A matrika sosednosti grafa Γ in naj bo $y = (y_1, \ldots, y_n)^T$ poljuben lastni vektor te matrike. Naj bo y_j komponenta vektorja y z največjo absolutno vrednostjo.

Ker je $(Ay)_j = ky_j$, je $\sum_{i=1}^{k} y_i = ky_j$, kjer vsota preteče i-je, za katere je točka v_i sosedna točki v_j. Zaradi maksimalnosti y_j sledi, da je $y_i = y_j$.

Ker je graf povezan, lahko na enak način postopek nadaljujemo z nekim y_i, kjer je v_i sosedna točka točke v_j.

Sledi, da so vse komponente vektorja y enake, zato je le-ta večkratnik vektorja v. Torej je večkratnost lastne vrednosti k res enaka 1. ■

Iz zgornjih trditev sledi, da je prva lastna vrednost krepko regularnega grafa enaka k in ima večkratnost 1.

Trditev 7.2.9 *Krepko regularen graf* Γ s *parametri* (n, k, λ, μ) *ima poleg* k *še dve lastni vrednosti:*

$$r = \frac{\lambda - \mu + \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}}{2} \text{ in } s = \frac{\lambda - \mu - \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}}{2}.$$

Dokaz. Za začetek razmislimo, da je mesto (u, v) matrike A^2 število skupnih sosedov točk u in v. Pri $u = v$ pa gre preprosto za stopnjo točke u. Zdaj pa uporabimo dejstvo, da lahko matriko A^2 zapišemo kot linearno kombinacijo matrik A, I in J. Ne smemo pozabiti, da lahko matriko sosednosti komplementa grafa Γ (graf, ki nima povezav, kjer jih je imel Γ) zapišemo kot $J - I - A$. Iz tega sledi

$$A^2 = \lambda A + \mu(J - I - A) + kI$$

$$A^2 = (\lambda - \mu)A + \mu J + (k - \mu)I.$$

Za vsak vektor v pravokoten na vektor samih enic, velja

$$A^2 v = (\lambda - \mu)Av + (k - \mu)v.$$

Torej vsaka lastna vrednost θ različna od k, zadošča

$$\theta^2 = (\lambda - \mu)\theta + k - \mu.$$

Rešitvi te kvadratne enačbe sta iskani lastni vrednosti, ki ju označimo z r in s:

$$r, s = \frac{\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}{2}.$$

■

V sledečem izreku bomo spoznali še, kakšne so večkratnosti teh dveh lastnih vrednosti.

Trditev 7.2.10 *Večkratnosti f in g lastnih vrednosti r in s iz trditve 7.2.9 sta enaki:*

$$f = \tfrac{(n-1)s+k}{s-r} \text{ in } g = \tfrac{(n-1)r+k}{r-s}.$$

Dokaz. Naj bodo 1, f in g večkratnosti lastnih vrednosti k, r in s. Iz izrekov 4.0.8 in 4.0.9 vemo, da mora veljati:

$$1 + f + g = n$$

in

$$Sled(A) = k + fr + gs = 0.$$

Iz zgornjih enačb izračunamo večkratnost lastne vrednosti f tako, da iz prve enačbe izrazimo $g = n - 1 - f$ in vstavimo v drugo:

$$k + fr + s(n - 1 - f) = 0$$

$$k + sn - s + f(r - s) = 0$$

$$k + s(n - 1) + f(r - s) = 0$$

$$k + s(n - 1) = -f(r - s)$$

$$f = \frac{(n - 1)s + k}{s - r}.$$

Podobno naredimo za večkratnost lastne vrednosti g. Izrazimo $f = n-1-g$ in izračunamo:

$$k + (n - 1 - g)r + gs = 0$$

$$k + nr - r + g(s - r) = 0$$

$$k + r(n-1) + g(s-r) = 0$$
$$k + r(n-1) = -g(s-r)$$
$$g = \frac{(n-1)r + k}{r-s}.$$

■

Krepko regularnemu grafu, ki ima enaki večkratnosti $f = g$ lastnih vrednosti r in s, pravimo konferenčni graf.

Za konec navedimo še nekaj dejstev, ki veljajo za krepko regularne grafe [8], [12], [17], [18].

i) Povezan regularen graf je krepko regularen natanko tedaj, ko ima tri različne lastne vrednosti.

ii) Povezani krepko regularni grafi so natanko razdaljno regularni grafi z diametrom 2.

iii) Vsak graf na n točkah je induciran podgraf krepko regularnega grafa na največ $4n^2$ točkah.

iv) Krepko regularen graf je konferenčni graf natanko tedaj, ko ima parametre $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-5), \frac{1}{4}(v-1))$.

Poglavje 8

Paleyjevi grafi in njihove lastnosti

8.1 Uvod v Paleyjeve grafe

V tem podpoglavju bomo spoznali nekaj definicij, ki jih bomo potrebovali za nadaljnje razumevanje Paleyjevih grafov in njihovih lastnosti.

Definicija 8.1.1 *Cayleyjev digraf* $\overrightarrow{\Gamma} = Cay(G, S)$ *grupe* G *glede na množico* S *je digraf, za katerega velja:*

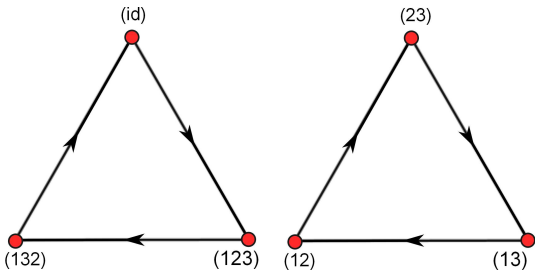
i) $V(\overrightarrow{\Gamma}) = G$,

ii) $(u, v) \in E \iff \exists s \in S : v = su$.

Za poljubno točko $u \in V(\overrightarrow{\Gamma})$ je število lokov, ki se začnejo v točki u enako $|S|$.

Primer 8.1.2 *Naj bo grupa* $G = S_3$ *in* $S = \{(123)\}$. *Slika 8.1 prikazuje Cayleyjev digraf* $Cay(G, S)$, *ki smo ga dobili s sledečimi izračuni:*

$$\begin{aligned} s * id &= (123), & s * (12) &= (23), \\ s * (123) &= (132), & s * (23) &= (13), \\ s * (132) &= id, & s * (13) &= (12). \end{aligned}$$



Slika 8.1: Cayleyjev graf

Trditev 8.1.3 *Naj bo G grupa in S njena podmnožica, potem je Cayleyjev digraf $Cay(G, S)$ graf natanko tedaj, ko velja:*

$$1 \notin S \ \ (nima\ zank) \tag{8.1}$$

$$S = S^{-1} \ \ oz.\ \check{c}e\ s \in S,\ potem\ tudi\ s^{-1} \in S. \tag{8.2}$$

Dokaz. Najprej predpostavimo, da je $\Gamma = \mathrm{Cay}(G, S)$ Cayleyjev graf. Potem Γ nima zank in zato za vsak $x \in G$ in vsak $s \in S$ velja, da je $x \neq sx$. Torej $1 \notin S$.

Naj bo (x, y) poljuben lok grafa Γ. Ker je Γ graf, je tudi (y, x) lok grafa Γ. Torej $(x, y), (y, x) \in E(\Gamma)$ in zato obstajata taka $s, s' \in S$, da je $y = sx$ in $x = s'y$. Odtod sledi, da je $y = sx = ss'y$. Če obe strani enačbe z leve pomnožimo z y^{-1} (z inverzom elementa y v grupi G), dobimo, da je $s' = s^{-1} \in S$.

Za dokaz obratne smeri predpostavimo, da za Cayleyjev digraf $\overrightarrow{\Gamma} = \mathrm{Cay}(G, S)$ veljata (8.1) in (8.2). Ker $1 \notin S$, $(x, 1 \cdot x) \notin E(X)$. Torej digraf $\overrightarrow{\Gamma}$ nima zank. Naj bo $(x, y) \in E(\overrightarrow{\Gamma})$ poljuben lok grafa $\overrightarrow{\Gamma}$. Potem obstaja tak $s \in S$, da je $y = sx$. Če to enakost z desne pomnožimo z elementom s^{-1}, dobimo $x = s^{-1}y$. Ker je po predpostavki $s^{-1} \in S$, odtod sledi, da je $(y, x) \in E(\overrightarrow{\Gamma})$.

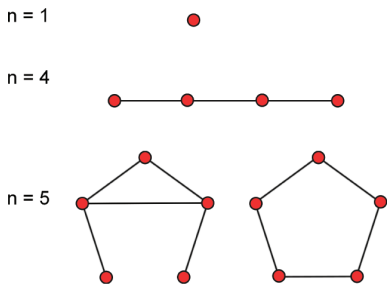
■

Izkaže se, da so Cayleyjevi grafi točkovno tranzitivni. Dokaz tega dejstva si lahko preberete v magisterskem delu [14].

Definicija 8.1.4 *Graf je ločno tranzitiven, če grupa avtomorfizmov deluje tranzitivno na množici lokov.*

Definicija 8.1.5 *Graf je sebikomplementaren, če je izomorfen svojemu komplementu.*

Primer 8.1.6 *Na sliki 8.2 vidimo tri enostavne primere sebikomplementarnih grafov.*



Slika 8.2: Primeri najbolj preprostih sebikomplementarnih grafov

Definicija 8.1.7 *$(R, +, *)$ je polje, če sta $(R, +)$ in $(R \setminus \{0\}, *)$ komutativni grupi in velja distributivnost.*

Polje $(R, +, *)$ reda n označujemo s $\mathbb{F}_n$.

Definicija 8.1.8 *Naj bo p poljubno praštevilo. Elementu ω, ki generira multiplikativno grupo neničelnih elementov končnega polja s p^n elementi, pravimo primitivni koren.*

Navedimo še dve ključni lastnosti [4], ki ju bomo potrebovali za razumevanje dokaza izreka 8.2.5 v naslednjem poglavju.

i) Za vsako praštevilo p obstaja število g, tako da za vsako število x med 1 in $p-1$ obstaja i med 1 in $p-1$, da velja $x \equiv g^i \bmod p$. V posebnem velja $g^{p-1} \equiv 1$.

ii) Če je p praštevilo, za katerega velja $p \equiv 1 \bmod 4$, potem je -1 kvadrat po modulu p.

8.2 Paleyjevi grafi

Naj bo q taka praštevilska potenca, da je $q \equiv 1 \bmod 4$ in naj bo $\mathbb{F}_q$ končno polje reda q s primitivnim korenom ω. Naj S označuje množico neničelnih kvadratov iz $\mathbb{F}_q$. Paleyjev graf reda q je Cayleyjev graf, ki ga konstruiramo na grupi $\mathbb{F}_q$ in uporabimo S kot množico povezav.

Element x v $\mathbb{F}_q$ je kvadrat, če obstaja tak element s v $\mathbb{F}_q$, da je $x = s^2 \bmod q$.

Oglejmo si formalno definicijo Paleyjevih grafov.

Definicija 8.2.1 *Naj bo q potenca praštevila, za katero velja $q \equiv 1 \bmod 4$. Paleyjev graf $P(q)$ dobimo tako, da za točke vzamemo elemente iz $\mathbb{F}_q$. Točka x je povezana s točko y, če je $(x - y) \in S$, kjer s S označimo neničelne kvadrate števil iz množice $\mathbb{F}_q$.*

Trditev 8.2.2 *Paleyjevi grafi $P(q)$ so ločno tranzitivni.*

Dokaz. Naj θ predstavlja permutacijo na $\mathbb{F}_q$, definirano na sledeči način θ: $x \longmapsto \omega^2 x$, kjer je ω primitivni koren polja $\mathbb{F}_q$. Spomnimo se, da je multiplikativna grupa S grupe $\mathbb{F}_q$ generirana z ω^2 in zato podgrupa permutacijske grupe generirane s θ deluje tranzitivno na S. Predpostavimo, da sta x in y povezani točki v $P(q)$, torej $x - y = \omega^{2i}$ za nek i. Vidimo, da velja

$$x - y = \omega^{2i} \iff \omega^2 x - \omega^2 y = \omega^{2(i+1)}.$$

Torej sta x in y sosedni natanko tedaj, ko sta $\theta(x)$ in $\theta(y)$ sosedni. Tako lahko vidimo, da je θ avtomorfizem grafa $P(q)$, ki fiksira 0, in da podgrupa generirana s θ deluje tranzitivno na sosede točke 0.

Z uporabo dejstva, da grupa avtomorfizmov Cayleyjevega grafa vedno deluje tranzitivno na njegove točke, zaključimo, da grupa avtomorfizmov deluje tranzitivno na loke grafa $P(q)$. ■

Trditev 8.2.3 *Paleyjevi grafi so sebikomplementarni.*

Dokaz. Naj bo ω primitivni koren polja $\mathbb{F}_q$. Naj σ označuje permutacijo na $\mathbb{Z}_q$, ki preslika x v ωx. Opazimo, da

$$x - y = \omega^{2i} \iff \sigma(x) - \sigma(y) = \omega^{2i+1}.$$

Spomnimo se, da je S multiplikativno generirana z ω^2, torej sta x in y sosedna v $P(q)$ natanko tedaj, ko $\sigma(x)$ in $\sigma(y)$ nista sosedna. Torej sledi, da je σ izomorfizem iz $P(q)$ na njegov komplement. ■

Lema 8.2.4 *Sebikomplementarni grafi, ki so hkrati ločno tranzitivni, so krepko regularni.*

Dokaz. Naj bo Γ sebikomplementaren ločno tranzitiven graf. Ločna tranzitivnost implicira točkovno tranzitivnost. Zato lahko brez škode za splošnost obravnavamo poljubno točko x grafa Γ. Vsaka točka ima isto stopnjo, torej je parameter k sebikomplementarnega grafa dobro definiran.

Naj bo točka y soseda točke x. Zaradi ločne tranzitivnosti obstaja avtomorfizem grafa Γ, ki fiksira x in y premakne v poljubnega soseda točke x. Torej je število skupnih sosedov točk x in y neodvisno od izbire točke y. To implicira, da je parameter λ dobro definiran.

Naj bo z točka, ki ni sosedna točki x v Γ in naj bo $\overline{\Gamma}$ komplement grafa Γ. Očitno je x sosedna z z v grafu $\overline{\Gamma}$. Ker je $\overline{\Gamma}$ ločno tranzitiven, je število točk, ki niso sosedne z x in niso sosedne z z, neodvisno od izbire točke z. Zato je število skupnih sosedov točke x in poljubne nesosedne točke v Γ konstantno. Sledi, da je tudi parameter μ dobro definiran. ■

Iz trditev 8.2.2, 8.2.3 in 8.2.4 sledi, da so Paleyjevi grafi krepko regularni.

Pokažimo še, da so krepko regularni s parametri $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$. Naslednja trditev pokaže krepko regularnost brez uporabe ločne tranzitivnosti in sebikomplementarnosti.

Trditev 8.2.5 *Paleyjev graf $P(q)$ je krepko regularen s parametri* $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

Dokaz. Za začetek povejmo, da so kvadrati grupe $\mathbb{F}_q$ ravno elementi g^i, kjer je i sodo število. Ker velja $g^i g^j = g^{i+j}$, dejstvo, da je -1 kvadrat, implicira, da je x kvadrat natanko tedaj, ko je tudi $-x$ kvadrat. Torej množica S vsebuje tudi vse inverze, zato je ta Cayleyjev graf dejansko graf. Če ne štejemo 0, imamo v grupi $\mathbb{F}_q$ ravno polovico kvadratov in polovico nekvadratov. Zato je $|S| = \frac{q-1}{2}$. In graf je regularen s $k = \frac{q-1}{2}$.

Preidimo na dokazovanje, da gre za krepko regularen graf. Naj bosta x in y poljubni točki. Ker iščemo število skupnih sosedov, nas zanima, koliko je elementov z, tako da sta hkrati $x - z$ in $y - z$ kvadrata. Namesto tega bomo izračunali, koliko elementov z je takih, da je $(x - z)(y - z)$ kvadrat. Ker poznamo valenci točk x in y, bomo lahko določili število skupnih sosedov teh dveh točk. Da vidimo to, definirajmo X kot množico sosedov točke x, Y kot množico sosedov točke y in Z kot množico točk $(X \cap Y) \cup (\overline{X} \cap \overline{Y})$. Tako dobimo

$$|Z| = |(X \cap Y) \cup (\overline{X} \cap \overline{Y})|$$
$$|Z| = |(X \cap Y)| + |\overline{X} \cap \overline{Y}|$$
$$|Z| = |(X \cap Y)| + q - |X \cup Y|$$
$$|Z| = |(X \cap Y)| + q - |X| - |Y| + |X \cap Y|$$
$$|Z| = 2|(X \cap Y)| + q - 2k$$
$$|Z| = 2|(X \cap Y)| + q - \frac{2(q-1)}{2}$$
$$|Z| = 2|X \cap Y| + 1.$$

Torej je

$$|Z| = \begin{cases} 2\lambda + 1, & \text{če sta } x \text{ in } y \text{ povezani} \\ 2\mu + 1, & \text{če } x \text{ in } y \text{ nista povezani} \end{cases}.$$

Zdaj bomo dokazali, da je

$$|Z| = \begin{cases} k - 1, & \text{če sta } x \text{ in } y \text{ povezani} \\ k + 1, & \text{če } x \text{ in } y \text{ nista povezani} \end{cases}.$$

Kar je enako kot

$$|Z| = \begin{cases} k-1, & \text{če je } x-y \text{ kvadrat} \\ k+1, & \text{če } x-y \text{ ni kvadrat} \end{cases}.$$

Da to dokažemo, definirajmo funkcijo

$$f(x) = \begin{cases} 0, & \text{če } x = 0 \\ 1, & \text{če je } x \text{ kvadrat modulo } q \\ -1, & \text{sicer} \end{cases}.$$

Pogledali si bomo dve možnosti.

1. Prvo poglejmo primer, ko sta x in y povezani točki. V tem primeru x in y nista v Z. Zato velja:

$$|Z| = \sum_{z \notin \{x,y\}} \frac{1}{2}(1 + f((x-z)(y-z)))$$

$$|Z| = \frac{1}{2} \sum_{z \notin \{x,y\}} 1 + \frac{1}{2}(\sum_{z \notin \{x,y\}} f((x-z)(y-z)))$$

$$|Z| = \frac{q-2}{2} + \frac{1}{2}(\sum_{z} f((x-z)(y-z))).$$

   Za $z \neq y$ lahko $f(y-z)$ zapišemo tudi kot $f(\frac{1}{y-z})$, saj če je $y-z$ kvadrat, je tudi $\frac{1}{y-z}$ kvadrat. Tako lahko izračunamo še iskano vsoto:

$$\sum_{z \notin \{x,y\}} f((x-z)(y-z)) = \sum_{z \notin \{x,y\}} f(\frac{x-z}{y-z})$$

$$\sum_{z \notin \{x,y\}} f((x-z)(y-z)) = \sum_{z \notin \{x,y\}} f(1 + \frac{x-y}{y-z}).$$

   Uvedemo novo spremenljivko w in naredimo sledečo zamenjavo

$$z = y - \frac{x-y}{w-1}.$$

   Ker z teče po vseh elementih različnih od x in y, sledi, da $w = 1 + \frac{x-y}{y-z}$ teče po vseh elementih različnih od 0 in 1. Zato iščemo naslednjo vsoto

$$\sum_{w \notin \{0,1\}} f(w).$$

Vemo, da nam funkcija f vrne 0, ko je $w = 0$, 1, ko imamo kvadrat in -1 ko imamo nekvadrat. V splošnem bi imeli $\frac{q-1}{2}$ kvadratov. Zdaj pa v vsoti ne zajamemo števila 1, zato imamo $\frac{q-1}{2} - 1 = \frac{q-3}{2}$ kvadratov. Nekvadratov pa je $q - 2 - \frac{q-3}{2} = \frac{q-1}{2}$. Opazimo, da je nekvadratov ravno za 1 več kot kvadratov, zato sledi:

$$\sum_{w \notin \{0,1\}} f(w) = -1.$$

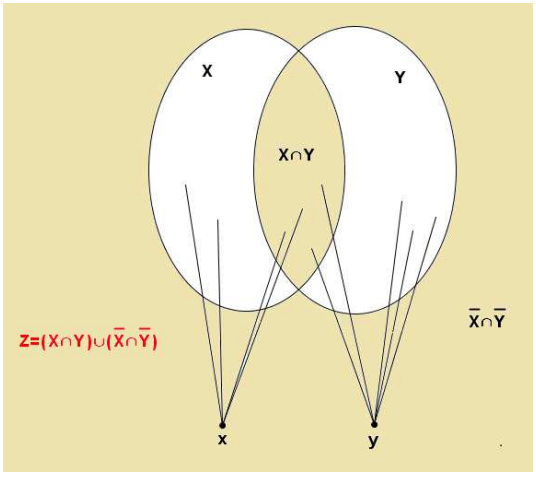
Zdaj smo dobili še zadnjo vsoto, zato lahko zapišemo

$$|Z| = \frac{q-2}{2} + \frac{1}{2} \sum_{w \notin \{0,1\}} f(w) = \frac{q-2}{2} - \frac{1}{2} = \frac{q-3}{2} = \frac{(2k+1)-3}{2} = k-1.$$

Zaključimo

$$|Z| = 2\lambda + 1$$
$$\lambda = \frac{|Z| - 1}{2}$$
$$\lambda = \frac{\frac{q-3}{2} - 1}{2}$$
$$\lambda = \frac{q-5}{4}.$$

2. Poglejmo še primer, ko x in y nista povezana. Ker je $x \in \overline{Y}$ in očitno $x \in \overline{X}$, sledi, da je $x \in \overline{X} \cap \overline{Y}$. Podobno pa velja tudi za y. Zato velja, da sta tako x kot y elementa množice Z (glej sliko 8.3).



Slika 8.3: Množica Z je obarvana z rumeno barvo.

V tem primeru je

$$|Z| = 2 + \sum_{z \notin \{x,y\}} \frac{1}{2}(1 + f((x-z)(y-z))) = 2 + (k-1) = k+1.$$

Tako dobimo

$$|Z| = 2\mu + 1$$
$$\mu = \frac{|Z| - 1}{2}$$
$$\mu = \frac{(k+1) - 1}{2}$$
$$\mu = \frac{k}{2}.$$

Zaključimo

$$\mu = \frac{\frac{q-1}{2}}{2}$$
$$\mu = \frac{q-1}{4}.$$

Tako smo torej prišli do sklepa, da je Paleyjev graf $P(q)$ res krepko regularen s parametri $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

■

Trditev 8.2.6 *Lastne vrednosti Paleyjevih grafov so $\frac{q-1}{2}$ z večkratnostjo 1 in $\frac{-1\pm\sqrt{q}}{2}$, obe z večkratnostjo $\frac{q-1}{2}$.*

Dokaz. Ker so Paleyjevi grafi krepko regularni, lahko njihove lastne vrednosti in njihove večkratnosti izračunamo po vzorcu lastnih vrednostih krepko regularnega grafa iz trditev 7.2.9 in 7.2.10.

Prva lastna vrednost krepko regularnega grafa s parametri (n, k, λ, μ) je k z večkratnostjo 1. Sledi, da je prva lastna vrednost za Paleyjev graf s parametri $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ enaka $\frac{q-1}{2}$ in ima večkratnost 1.

Druga lastna vrednost je sledeča:

$$r = \frac{\frac{q-5}{4} - \frac{q-1}{4} + \sqrt{(\frac{q-5}{4} - \frac{q-1}{4})^2 + 4(\frac{q-1}{2} - \frac{q-1}{4})}}{2}$$
$$r = \frac{-1 + \sqrt{(-1)^2 + 4\frac{q-1}{4}}}{2}$$
$$r = \frac{-1 + \sqrt{1 + q - 1}}{2}$$

$$r = \frac{-1+\sqrt{q}}{2}.$$

Tretjo lastno vrednost izračunamo na enak način:

$$s = \frac{\frac{q-5}{4} - \frac{q-1}{4} - \sqrt{(\frac{q-5}{4} - \frac{q-1}{4})^2 + 4(\frac{q-1}{2} - \frac{q-1}{4})}}{2}$$

$$s = \frac{-1-\sqrt{q}}{2}.$$

Sedaj lahko izračunamo še večkratnosti lastnih vrednosti r in s.
Večkratnost f lastne vrednosti r je enaka:

$$f = \frac{(q-1)\frac{-1-\sqrt{q}}{2} + \frac{q-1}{2}}{\frac{-1-\sqrt{q}}{2} - \frac{-1+\sqrt{q}}{2}}$$

$$f = \frac{\frac{-q+1-q\sqrt{q}+\sqrt{q}+q-1}{2}}{-\sqrt{q}}$$

$$f = \frac{-q\sqrt{q}+\sqrt{q}}{2} \cdot \frac{1}{-\sqrt{q}}$$

$$f = \frac{q-1}{2}.$$

Večkratnost g lastne vrednosti s je enaka:

$$g = \frac{(q-1)\frac{-1+\sqrt{q}}{2} + \frac{q-1}{2}}{\frac{-1+\sqrt{q}}{2} - \frac{-1-\sqrt{q}}{2}}$$

$$g = \frac{\frac{-q+1+q\sqrt{q}-\sqrt{q}+q-1}{2}}{\sqrt{q}}$$

$$g = \frac{q\sqrt{q}-\sqrt{q}}{2} \cdot \frac{1}{\sqrt{q}}$$

$$g = \frac{q-1}{2}.$$

■

Za konec navedimo še nekaj dejstev, ki veljajo za Paleyjeve grafe [12].

i) Paleyjevi grafi so konferenčni grafi.

ii) Paleyjevi grafi premorejo Hamiltonski cikel, to je cikel, ki poteka skozi vse točke v grafu.

iii) Če je $q = p^r$, je moč grupe avtomorfizmou Paleyjevega grafa enaka $\frac{rq(q-1)}{2}$.

Še kaj o konstrukciji Paleyjevih grafov pa si lahko preberete v članku [15].

Poglavje 9

Zaključek

V zaključni projektni nalogi smo raziskovali rank 3 grupe in krepko regularne grafe. Dokazali smo, da vsaka rank 3 grupa porodi krepko regularen graf. Spoznali smo, da obstaja zveza med parametri takega grafa in si ogledali še druge njegove lastnosti. Seznanili smo se z nekaj družinami teh grafov in podrobneje spoznali Paleyjeve grafe. Dokazali smo tudi, da so le-ti krepko regularni.

Prišli smo do zaključka, da je krepko regularnost tako zanimiva lastnost, da je raziskovana na različnih področjih. In krepko regularni grafi so še vedno plod zanimanja, saj je o njih še marsikaj neznanega. Morda še enkrat omenimo to, da so krepko regularni grafi na meji med točno določenimi in povsem naključnimi grafi. Razlog tiči v parametrih takega grafa. Očitno je, da ni vsak nabor parametrov primeren za konstrukcijo krepko regularnega grafa. Prav zato se raziskuje tudi v tej smeri – iskanje potrebnih pogojev za obstoj takih grafov. Znano je celo, da obstaja natanko en krepko regularen graf s parametri $(36, 10, 4, 2)$. Toda McKayjevi in Spencejevi izračuni kažejo, da pa je krepko regularnih grafov s parametri $(36, 15, 6, 6)$ ravno 32548 [1]. In vzorec se še nadaljuje. Vsak krepko regularen graf s parametri $(m^2, 2(m-1), m-2, 2)$ je enolično določen. Na drugi strani pa imamo več kot eksponentno mnogo krepko regularnih grafov s parametri $(m^2, 3(m-1), m, 6)$ [16]. Zato ostajajo krepko regularni grafi zanimiva iztočnica za nadaljnje študije.

Literatura

[1] B. D. McKay, E. Spence, Classification of regular two-graphs on 36 and 38 vertices, Australasian Journal of Combinatorics 24 (2001), 293-300.

[2] B. Frelih, Krepko regularni grafi, diplomsko delo, marec 2003.

[3] D. Spielman, Lecture 16, november 1996.

[4] D. Spielman, Strongly regular graphs, part 2, november 2009. Dostopno na: http://www.cs.yale.edu/homes/spielman/561/lect24-09.pdf, april 2011.

[5] I. Kovacs, Permutacijske grupe, 2011, študijsko gradivo.

[6] J. Fox, The Petersen graph and Moore graphs, lecture 19. Dostopno na: http://math.mit.edu/ fox/MAT307-lecture19.pdf, september 2011.

[7] J. B. Fraleigh, A first course in abstract algebra, Addison-Wesley, 7th edition (2002), 93-94.

[8] J. L. Gross, J. Yellen, Handbook of graph theory, Boca Raton, 2004.

[9] K. Kuttler, An introduction to linear algebra, 13. julij 2011.

[10] K. Kutnar, A. Malnič, D. Marušič, P. Šparl, Uvod v teorijo grup, 4. oktober 2009.

[11] M. Behbahani, On Strongly Regular Graphs, Concordia University, Montreal, Quebec, Canada, 2009.

[12] N. Biggs, Algebraic graph theory, Cambridge University Press 1974, 1993.

[13] N. L. Biggs, A. T. White, Permutation groups and combinatorial structures, Cambridge University Press 1979, 80-102.

[14] N. Mullin, Self-complementary arc-transitive graphs and their imposter, Waterloo, Ontario, Canada, 2009.

[15] P. J. Cameron, D. Stark, A prolific construction of strongly regular graphs with the n-e.c. property, Queen Mary, University of London.

[16] P. J. Cameron, Random strongly regular graphs?, Queen Mary, University of London.

[17] P. J. Cameron, Strongly regular graphs, Queen Mary, University of London, 2001.

[18] R. J. Elzinga, Strongly regular graphs: Values of λ and μ for which there are only finitely many feasible (v, k, λ, μ), 8. oktober 2003.

[19] R. Gera, J. Shen, Extension of Strongly Regular Graphs, Department of Mathematics Texas State University and Department of Applied Mathematics Naval Postgraduate School Monterey, 2008.

[20] T. Košir, Linearna algebra, 12. januar 2009.

[21] Paleyjevi grafi. Dostopno na: http://mathworld.wolfram.com/PaleyGraph.html, april 2011.

[22] Hoffman-Singletonov graf. Dostopno na: http://mathworld.wolfram.com/Hoffman-SingletonGraph.html, april 2011.