Sveučilište u Rijeci
Fakultet za matematiku

Sveučilišni diplomski izvanredni studij Matematika – smjer nastavnički

Martina Križanac

O p-rangu matrice susjedstva jako regularnog grafa

Diplomski rad

Rijeka, srpanj, 2022.

Sveučilište u Rijeci
Fakultet za matematiku

Sveučilišni diplomski izvanredni studij Matematika – smjer nastavnički

Martina Križanac

O p-rangu matrice susjedstva jako regularnog grafa

Mentor: dr. sc. Dean Crnković

Rijeka, srpanj, 2022.

SADRŽAJ

Sažetak

Ovaj rad temelji se na proučavanju p-ranga matrice susjedstva jako regularnog grafa. Za neke specifične slučaje izvest ćemo granice za takav rang. Istražit ćemo povezanost između p-rangova matrica susjedstva ekvivalentnih grafova s obzirom na switching

Ključne riječi

Jako regularan graf, matrica susjedstva, p-rang, Smithova normalna forma

1. UVOD

U ovom radu proučavat ćemo rang nad konačnim poljem od p elemenata, odnosno p-rang matrice susjedstva jako regularnih grafova. Takve matrice koriste se kao generatori p-arnih kodova. Kod tih je kodova p-rang matrice upravo dimenzija koda.

Za razne incidencijske strukture proučavaju se p-rangovi pridruženih $(0,1)$ matrica. Primjerice, proučavaju se kod kodova za ispravljanje grešaka. S druge strane, proučava se p-rang matrica incidencije. Kod samodualnih kodova asociranih sa simetričnim dizajnima pronalaze se novi rezultati o parametrima takvih dizajna. U svojim radovima Bagchi, Brouwer i Wilbrink i Brouwer i Haemers daju rezultate o p-rangu matrice susjedstva jako regularnih grafova.

Neka je A matrica susjedstva jako regularnog grafa. Nećemo se fokusirati samo na p-rang matrice A, već ćemo proučavati p–rang matrice $A + rI$, za r cijeli broj. Za većinu izbora p i r, p -rang od $A + rI$ je u potpunosti određen parametrima grafa. U preostalim slučajevima potrebno je proučiti strukturu grafa.

Linearna algebra, Teorija kodiranja i Teorija grupa igraju važnu ulogu pri proučavanju p -ranga matrice susjedstva jako regularnog grafa. U prvome poglavlju objasnit ćemo pojmove iz ovih područja koji se koriste u radu, odnosno prvo će poglavlje dati uvod u teoriju jako regularnih grafova. P-rang cjelobrojne matrice lako je izvesti iz Smithove normalne forme, čime se bavimo u drugome poglavlju. U trećem poglavlju promatramo cjelobrojne svojstvene vrijednosti p-ranga matrica susjedstva jako regularnih grafova. Izoliramo kombinacije brojeva p i r za koje određivanje p-ranga nije trivijalno i dajemo opću gornju granicu za ove slučajeve. Također, istražujemo povezanost između p-rangova matrica susjedstva ekvivalentnih grafova s obzirom na switching.

2. UVOD U TEORIJU JAKO REGULARNOG GRAFA

U ovom se radu koriste mnogi pojmovi iz različitih grana matematike, stoga ćemo u ovom poglavlju ponoviti pojmove koje smatramo bitnima za ovaj rad.

Uvodimo notaciju koju ćemo koristiti u ovom radu:

- slovo p označava prost broj, odnosno $p \in P$, gdje je P skup prostih brojeva
- F_q oznaka je za konačno polje sa q elemeata
- skup svih nxm matrica nad poljem F označavamo F^{nxm}
- vektor x uvijek označava retčani vektor
- I_n je jedinična matrica reda n, O_n matrica reda n čiji su svi elementi nule, a J_n matrica reda n čiji su svi elementi jedinice
- 1_n i 0_n su retčani vektori sa n elemenata. Indeks n se može izostaviti kada je jasno o kakvom se vektoru radi
- dijagonalnu matricu kojoj su elementi $\alpha_i, 1 \leq i \leq n$, označavamo sa $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)$
- $\mathrm{diag}({\alpha_1}^{m_1}, {\alpha_2}^{m_2}, \ldots)$ označava matricu koja najprije na dijagonali ima elemente α_1 (m_1 puta), zatim α_2 (m_2 puta) itd. Dakle, takva je matrica dimenzije $m_1 + m_2 + \cdots + m_n$
- blok-dijagonalna matrica sa n_1 blokova M_1, n_2 blokova M_2, itd., označava se sa $\mathrm{diag}({M_1}^{n_1}, {M_2}^{n_2}, \ldots)$
- sa V označavamo n −dimenzionalni vektorski prostor nad poljem F
- Neka su V_1 i V_2 potprostori od V. Suma potprostora V_1 i V_2 označava se sa $V_1 + V_2$. Ako je presjek trivijalan, onda je suma direktna i označava se s $V_1 \oplus V_2$.

2.1. Teorija matrica

U Linearnoj algebri dokazani su teoremi koje ćemo sada iskazati.

Neka je F polje i M kvadratna matrica reda n nad poljem F. Matrica M je regularna ako i samo ako je $detM \neq 0$. U suprotnom, matrica je singularna.

Karakteristični ili svojstveni polinom matrice M je polinom $p(z) = \det(M - zI)$, odnosno normirani polinom stupnja n oblika $z^n + \alpha_{n-1}z^{n-1} + \cdots + \alpha_1 z + \alpha_0$. Nul-točke polinoma $p(z)$ nazivamo svojstvenim vrijednostima matrice M.

Ako je λ svojstvena vrijednost matrice M, onda postoji vektor x različit od nul-vektora tako da vrijedi $xM = \lambda x$. Taj se vektor naziva svojstvenim vektorom matrice M (za svojstvenu vrijednost λ). Skup svih svojstvenih vrijednosti matrice M nazivamo spektrom od M. Algebarska kratnost svojstvene vrijednosti λ matrice M definira se kao kratnost nul-točke z karakterističnog polinoma $p(z)$. Geometrijska kratnost svojstvene vrijednosti λ definira se kao dimenzija pripadajućeg svojstvenog potprostora $V_\lambda = \{x \in V | xM = \lambda x\}$. Geometrijska je kratnost manja ili jednaka od algebarske kratnosti iste svojstvene vrijednosti. U slučaju jednakosti, vrijedi da je suma dimenzija potprostora svih svojstvenih vrijednosti jednaka upravo n, što je ekvivalentno tvrdnji da prostor V ima bazu koja se sastoji od svojstvenih vektora matrice M.

Kažemo da se matrica M može dijagonalizirati ako postoji regularna matrica $S \in F^{nxn}$ tako da je $S^{-1}MS$ dijagonalna matrica. Matrica se može dijagonalizirati samo ako vrijedi da je suma dimenzija potprostora svih svojstvenih vrijednosti matrice jednaka n. Ako se matrice M_1 i M_2 mogu dijagonalizirati i vrijedi da je $M_1 M_2 = M_2 M_1$, onda se dijagonaliziraju s istom matricom S.

Skup $\langle x_1 x_2, \dots, x_m \rangle := \{\sum_{i=1}^{m} \alpha_i x_i | \alpha_i \in F\}$ je vektorski prostor nad poljem F razapet vektorima $x_1 x_2, \dots, x_n$. $R_F(M)$ je prostor redaka od M nad F, odnosno vektorski prostor generiran redcima matrice M.

F-rang matrice M je dimenzija od $R_F(M)$ i označavamo ga sa $r_F(M)$. Ukoliko je $F = F_q$, oznake su $R_q(M)$ i $r_q(M)$.

Jezgru matrice M nad poljem F označavamo sa $N_F(M)$, a definiramo je kao

$$N_F(M) := \{x | xM = 0\}.$$

Vrijedi

$$\dim R_F(M) + \dim N_F(M) = n.$$

Ako je λ svojstvena vrijednost matrice M, tada je $V_\lambda = N_F(M - \lambda I)$.

Za matrice M i M' kažemo da su ekvivalentne ako postoji regularne matrice P i Q od F^{nxn} tako da vrijedi $M = PM'Q$. Zapisujemo: $M \sim M'$.

Za sljedeće operacije nad matricom kažemo da su ekvivalentne:

(i) zamjena dvaju redaka (stupaca);

(ii) množenje retka (stupca) skalarom različitim od nule;

(iii) dodavanje nekog retka (stupca) matrice nekom drugome retku (stupcu) te matrice.

Navedeno nazivamo elementarne transformacije nad matricom.

Ako su matrice M i M' ekvivalentne, onda jednu možemo dobiti iz druge elementarnim transformacijama nad redcima i stupcima.

Propozicija 2.1. *Ekvivalentne matrice imaju isti rang.*

Trag matrice M je zbroj svih elemenata koji se nalaze na dijagonali matrice. Označava se sa $\mathrm{tr}(M)$.

Vrijedi sljedeće:

$$\mathrm{tr}(MM') = \mathrm{tr}(M'M), \;\; M, M' \in F^{n\mathrm{x}n}.$$

Za skup Ω i $\Omega' \subset \Omega$, karakteristični vektor od Ω' je s koordinatama indeksiranim elementima od Ω tako da vrijedi

$$c_\omega = \begin{cases} 1, & \omega \in \Omega \\ 0, & \text{inače.} \end{cases}$$

Permutacijska matrica je kvadratna matrica koja ima točno jednu 1 u svakom stupcu i retku, a svi su ostali elementi 0.

2.2. Teorija grafova

2.2.1. Opći pojmovi

Definicija 2.1. *Graf je konačna incidencijska struktura* $\Gamma = (V, E, I)$ *gdje je* V *neprazni konačni skup čije elemente nazivamo vrhovima,* E *je konačni skup dvočlanih podskupova skupa* V *i njegove elemente nazivamo bridovima, a binarna relacija* $I \subseteq V \times E$ *relacija incidencije.*

Dva vrha su susjedna ako su incidentna s istim bridom. Dva brida su susjedna ako su incidentna s istim vrhom. Brid koji je incidentan samo s jednim vrhom zove se *petlja*.

Graf je jednostavan ako ne sadrži petlju i višestruke bridove.

Definicija 2.2. $\Delta = (V', E', I')$ *je podgraf od* $\Gamma = (V, E, I)$ $(\Delta \subseteq \Gamma)$ *ako je*

- $V' \subseteq V$,
- $E' \subseteq E$,
- $I|_{V' \times E'} = I'$.

Ako je $\Delta \subseteq \Gamma$ *i* $\Delta \neq \Gamma$ *pišemo* $\Delta \subset \Gamma$ *i nazivamo ga pravi podgraf.*

Broj vrhova od Γ naziva se redom od Γ i označava se s v.

Ako je $e = \{x, y\}$ brid grafa Γ, tada za vrhove x i y kažemo da su susjedni vrhovi, a brid e je incidentan s vrhovima x i y. Za $x \epsilon V$ stupanj vrha x definira se kao broj bridova incidentnih sa x. Vrh stupnja 0 naziva se izolirani vrh.

Graf Γ je k-regularan ako je stupanj svakog vrha jednak k. Graf Γ je regularan ako je k-regularan za neki k.

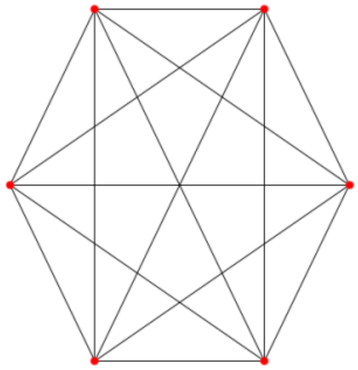
Ako je V_1 bilo koji podskup vrhova od Γ, tada je podgraf induciran s V_1 podgraf od Γ dobiven uzimanjem vrhova iz V_1 i spajanjem onih parova vrhova iz V_1 koji su spojeni u Γ. Inducirani podgraf od Γ je podgraf induciran nekim podskupom V_1 od V.

Definicija 2.3. *Neka je* $\Gamma = (V, E, I)$. *Njemu komplementaran graf* Γ^c *je graf* (V, E, I') *gdje je* $I' = V \times E - I$ *tako da vrijedi:*

$(v, e) \in I' \Leftrightarrow (v, e) \notin I.$

Dakle, dva su vrha susjedna u Γ^c ako i samo ako nisu susjedni u Γ.

Graf koji se sastoji od v izoliranih vrhova naziva se nulgraf ili *koklika* (*coclique)* veličine v. Jednostavni graf u kojem su svaka dva vrha susjedna zove se *potpun graf* ili klika.



Slika 1. Potpun graf sa 6 vrhova

Definicija 2.4. *Grafovi* $\Gamma = (V, E, I)$ *i* $\Gamma' = (V', E', I')$ *su izomorfni ako i samo ako postoji bijekcija* $f : V \times E \to V' \times E'$ *tako da vrijedi:*

1) *f preslika* V *na* V', E *na* E'
2) $(v, e) \in I \Leftrightarrow \big(f(v), f(e)\big) \in I',\ \forall v \in V,\ \forall e \in E$

Automorfizam grafa Γ je bijektivno preslikavanje ϕ iz V na samog sebe tako da za su $\phi(x)$ i $\phi(y)$ susjedni vrhovi ako i samo ako su x i y susjedni vrhovi. Automorfizmi od Γ čine grupu koju nazivamo grupa automorfizama grafa Γ. Ta je grupa tranzitivna ako sadrži preslikavanja svakog vrha grafa u svaki drugi vrh tog grafa.

Graf možemo opisati $(0,1)$ matricom susjedstva A dimenzije vxv.

Definicija 2.5. *Matrica susjedstva grafa* Γ *je* vxv *matrica* $A(\Gamma) = [a_{ij}]$, *pri čemu* a_{ij} *označava broj bridova incidentnih s vrhovima* x_i *i* x_j.

Svojstvene vrijednosti grafa Γ su svojstvene vrijednosti matrice A. Svojstvene vrijednosti grafa ne ovise o promjeni oznaka vrhova grafa. Kako je matrica A simetrična, njezine su svojstvene vrijednosti realne.

Grafovi sa istim spektrom nazivaju se *kospektralni* grafovi. Kospektralni grafovi nisu nužno izomorfni.

Neka je Γ graf i Γ' njegov komplement. Neka je B matrica susjedstva grafa Γ'. Tada vrijedi

$$I_v + A + B = J_v.$$

Matricu susjedstva grafa Γ označavat ćemo s A_Γ, a ukoliko nije dvosmisleno, označavat ćemo je samo s A.

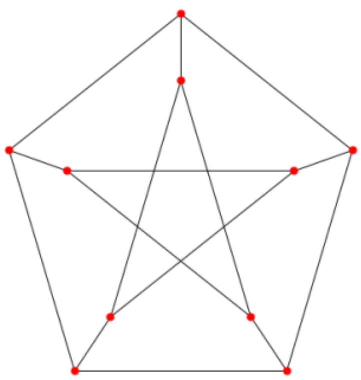
2.2.2. Jako regularni grafovi

Definicija 2.6. *Jako regularan graf s parametrima* (v, k, λ, μ) *je jednostavan* k*-regularan graf* Γ *s* v *vrhova koji nije potpun graf ili nulgraf. Nadalje, za svaka dva vrha* x *i* y *grafa* Γ *vrijedi da je broj njihovih zajedničkih susjeda jednak:*

1. λ, *ako su* x *i* y *susjedni vrhovi,*
2. μ, *ako su* x *i* y *nesusjedni vrhovi.*

Parametri jako regularnog grafa nisu nezavisni.

Primjer 2.1. *Petersenov graf je jednostavan* 3*-regularan graf s* 10 *vrhova i* 15 *bridova. Nazvan je po Juliusu Petersenu koji ga je otkrio 1898. godine. Petersenov graf je jako regularan s parametrima* $(10, 3, 0, 1)$.



Slika 2. Petersonov graf

Propozicija 2.2. *Ako postoji jako regularan graf s parametrima* (v, k, λ, μ), *onda je njegov komplement jako regularan s parametrima* $(v,\ v-k-1,\ v-2k+\ \mu-2,\ v-2k+\lambda)$.

Dokaz. Neka je Γ jako regularan graf s parametrima (v, k, λ, μ) i neka je Γ^c njegov komplement. Kako je svaki vrh u grafu Γ stupnja k, iz definicije komplementa grafa zaključujemo da je svaki vrh u grafu Γ^c stupnja $v-k-1$, tj. graf Γ^c je regularan stupnja $k' = v-k-1$. Nadalje, neka su x i y susjedni vrhovi grafa Γ^c. Iz definicije komplementa grafa zaključujemo da vrhovi x i y nisu susjedni u grafu Γ. Sada želimo prebrojiti zajedničke susjede u komplementu, tj. vrhove u grafu Γ koji nisu susjedi niti od x niti od y. Znamo da u grafu Γ x ima k susjeda, y ima k susjeda, a zajedničkih susjeda imaju μ. Primjenom formule uključivanja-isključivanja (FUI) na njihove susjede, zaključujemo da unija zajedničkih susjeda vrhova x i y ima ukupno $2k-\mu$ elemenata. Kako mi tražimo vrhove u grafu Γ koji nisu susjedi niti od x niti od y, trebamo ovu uniju komplementirati. Dobivamo da je:

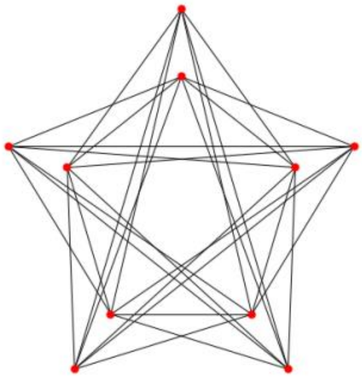
$$\lambda' = (v\ -\ 2) - 2k + \mu = v - 2k + \mu - 2.$$

Neka su sada x i y nesusjedni vrhovi grafa Γ^c. Iz definicije komplementa grafa zaključujemo da su vrhovi x i y susjedni u grafu Γ. Sada opet želimo prebrojiti zajedničke susjede u komplementu, tj. vrhove u grafu Γ koji nisu susjedi niti od x niti od y. Znamo da u grafu Γ x ima k susjeda, y ima k susjeda, a zajedničkih susjeda imaju λ. Primjenom formule uključivanja-isključivanja zaključujemo da unija ima $2k\ -\lambda$ elemenata. Komplementiranjem dobivamo da je:

$$\mu' = v - 2k + \lambda.$$

□

Primjer 2.2. *Graf* $T(5)$, *komplement Petersonovog grafa, jako regularan graf sa parametrima* (10,6,3,4)



Slika 3. Graf T(5)

Nepovezane grafove i njihove komponente nećemo razmatrati.

Neka je A matrica susjedstva grafa Γ. Vrijedi:

$$AJ = kJ,$$
$$A^2 = kI + \lambda A + \mu(J - I - A).$$

(1.1)

Vidimo da je retčani vektor koji ima samo jedinice svojstveni vektor matrice A sa svojstvenom vrijednošću k. Matrica A ima još dvije svojstvene vrijednosti r i s $(r > s)$ koje su rješenja jednadžbe $x^2 + (\mu - \lambda)x + ((\mu - k) = 0$. Njihove kratnosti f i g zadovoljavaju

$$f + g = v - 1$$
$$k + fr + gs = 0.$$

Očito je da f i g možemo izraziti preko v, k, λ i μ. Dolazimo do nužnog uvjeta za parametre jako regularnih grafova.

Ako je $f = g$ (tzv. poluslučaj), imamo

$$v = 4\mu + 1,$$
$$k = 2\mu,$$
$$\lambda = \mu - 1\ ,$$

i graf ima iste parametre kao njegov komplement. Inače, svojstvene vrijednosti r i s $(r > s)$ su cijeli brojevi.

Spomenimo i odnose između parametara k, λ, μ, r i s:

$$\lambda - \mu = r + s, \quad \mu = k + rs. \tag{1.2}$$

Ovi odnosi direktno slijede iz jednadžbe $x^2 + (\mu - \lambda)x + (\mu - k) = (x - r)(x - s)$.

Neka je A vektorski prostor nad $\mathbb{R}$ razapet sa $\{I, A, B\}$, gdje B označava matricu susjedstva od Γ^c. Vektorski prostor A zatvoren je s obzirom na standardno množenje matrica i naziva se algebra susjedstva ili Bose-Mesnerova algebra od Γ. Budući da su matrice u A simetrične i međusobno komutiraju, mogu se istovremeno dijagonalizirati. Stoga A dopušta (jedinstvenu) bazu minimalnih idempotenti $\{E_0, E_1, E_2\}$ zadovoljavajući

$$\sum_{i=0}^{2} E_i = j,$$

$$E_i E_j = \delta_{i_j} E_i, \tag{1.3}$$

Gdje je δ_{i_j} Kroneckerov simbol. U tablicama su zapisane idemponente kao linearne kombinacije baze $\{I, A, B\}$ i obrnuto.

	I	A	B
vE_0	1	1	1
vE_1	f	$f\frac{r}{k}$	$-f\frac{r+1}{l}$
vE_2	g	$g\frac{s}{k}$	$-g\frac{s+1}{l}$

	E_0	E_1	E_2
I	1	1	1
A	k	r	s
B	l	$-r-1$	$-s-1$

Iz desne tablice i (1.3) dobivamo da je $AE_1 = rE_1$ i $AE_2 = sE_2$. Stupci E_i razapinju svojstvene prostore svih matrica od vektorskog prostora A. Stoga je rang matrice E_i jednak dimenziji i-tog svojstvenog prostora. Iz toga slijedi da je $r(E_1) = f$ i $(E_2) = g$, gdje $r(M)$ označava $\mathbb{R}$-rang od M.

Posljednji ovdje razmotreni koncept je zamjena (*switching*).

Definicija 2.7. *Neka je* $\Gamma = (V, E)$ *(ne nužno jako regularan) graf i neka je* V_1 *neprazan pravi podskup od* V. *Za skup* V_2 *uzmimo* $V_2 \coloneqq V \backslash V_1$. *Konstruiramo novi graf* $\Gamma' = (V, E')$ *na sljedeći način:*

$$ako\ v_1, v_1' \in V_1, \qquad onda\ \{v_1, v_1'\} \in E'\ akko\ \{v_1, v_1'\} \in E\ ;$$
$$ako\ v_2, v_2' \in V_2, \qquad onda\ \{v_2, v_2'\} \in E'\ akko\ \{v_2, v_2'\} \in E;$$
$$ako\ v_1 \in V_1, v_2, \in V_2, \qquad onda\ \{v_1, v_2\} \in E'\ akko\ \{v_1, v_2\} \notin E\ .$$

Grafovi Γ *i* Γ' *su ekvivalentni s obzirom na switching (switching equivalent).* V_1 *se naziva skup zamjene.*

Može se dokazati da za Γ jako regularan, ako njegovi parametri zadovoljavaju

$$v + 4rs + 2r + 2s = 0,$$

i graf Γ' je regularan. Tada je Γ' opet jako regularan graf, s različitim parametrima, ili s istim parametrima. Graf Γ'može i ne mora biti izomorfan sa Γ. Ako je $V_1 = \{y | x{\sim}y\}$ za proizvoljan vrh x od Γ, onda je Γ' disjunktna unija vrha x i jako regularnog grafa s $k = 2\mu$.

2.3. Grupe

U ovom ćemo dijelu navesti nekoliko elementarnih pojmova iz Teorije grupa.

Definicija 2.8. *Uređeni par* $(G,\cdot)$, *koji se sastoji od nepraznog skupa* G *i binarne operacije*

$$\cdot : G \times G \to G$$

nazivamo grupa ako su ispunjeni ovi uvjeti:

(1) binarna operacija je asocijativna, tj. vrijedi

$$(ab)c = a(bc), \qquad za\ sve\ a, b, c \in G\ ;$$

(2) za binarnu operaciju postoji i jednoznačno je određen neutralni element, tj. $e \in G$ *sa svojstvom*

$$ea = ae = a, \qquad za\ svaki\ a \in G\ ;$$

(3) svaki je element invertibilan, tj. Za svaki $a \in G$ postoji i jednoznačno je određen $a^{-1} \in G$ sa svojstvom

$$aa^{-1} = a^{-1}a = e.$$

Kardinalni broj skupa G nazivamo red grupe i označavamo sa $|G|$.

Neka je $g \in G$. Najmanji prirodni broj n sa svojstvom da $g^n = e$, zovemo red elementa g. Skup $\{g^{-1}g_1 g | g \in G\}$ naziva se klasa konjugiranosti elementa g_1.

Neka je H podgrupa od G. H je normalna podgrupa grupe G ako vrijedi

$$H^g \coloneqq \{g^{-1}hg | h \in H\} = H, \text{ za svaki g} \in G.$$

Neka je H je normalna podgrupa grupe G. Tada kvocijentnu (faktorsku) grupu G/H nazivamo grupom suskupova $gH \coloneqq \{gh | h \in H\}$ uz množenje $(g_1 H)(g_2 H) \coloneqq (g_1 g_2 H)$. Indeks od H u G je red grupe G/H.

Neka su G i G' grupe. Funkcija $f: G \to G'$ naziva se homomorfizam iz G u G' ako vrijedi

$$f(g_1)f(g_2) = f(g_1 g_2), \text{ za svaki } g_1, g_2 \in G .$$

Ako je f bijekcija onda je f izomorfizam grupa. U tom slučaju kažemo da su grupe G i G' izomorfne i pišemo $G \cong G'$.

Definicija 2.9. *Neka je G grupa, a S skup. Djelovanje grupe G na skup S je preslikavanje*

$$G \times S \to S,$$

čiju vrijednost na uređenom paru $(g, x) \in G \times S$ označavamo sa $g.x$, te koje zadovoljava uvjete

(D1) $e.x = x$ za svaki $x \in S$, gdje je e neutralni element grupe G,

(D2) $g_1.(g_2.x) = (g_1 g_2).x$ za sve $g_1, g_2 \in G$ i svaki $x \in S$.

Orbita je podskup skupa X koji se dobije djelovanjem svih elemenata grupe na jedan izabrani i fiksirani element skupa X. Ako je $x \in X$ taj fiksirani element, onda se orbita koja se dobije pomoću njega zove orbita elementa x i označava $\bar{x}$. Orbita elementa x definira se kao

$$\bar{x} = \{g.x | g \in G\}.$$

Ako grupa G djeluje na skup X, onda djelovanje gledamo zdesna. Dakle, ako je $x \in X$ i $g \in G$, onda se slika elementa x pod g označava sa $x.g$.

Ako je cijeli skup X jedna orbita, tada se G naziva tranzitivna grupa.

Definicija 2.10. *Uređenu trojku* $(P, +.\cdot)$, *koja se sastoji od nepraznog skupa* P *i dviju binarnih operacija definiranih na tom skupu (prvu označavamo aditivno, drugu multiplikativno), nazivamo prsten, ako su ispunjeni ovi uvjeti:*

(1) skup P je u odnosu na zbrajanje komutativna grupa

(2) skup P je u odnosu na množenje polugrupa

(3) dvije su operacije povezane zakonom distribucije, tj. Vrijedi

$$a(b+c) = ab + ac,$$
$$(a+b)c = ac + bc,$$

za svaki izbor $a, b, c \in P$.

Grupu $(P, +)$ nazivamo aditivna grupa prstena P, a polugrupu $(P,\cdot)$ multiplikativna polugrupa prstena P.

Definicija 2.11. *U komutativnom prstenu P za element* $a \in P$ *kažemo da je invertibilan ako postoji element* $b \in P$ *takav da vrijedi:* $a \cdot b \ = b \cdot a = 1$.

Definicija 2.12. *Kažemo da je prsten P tijelo, ili prsten s dijeljenjem, ako je svaki element različit od nule u P invertibilan.*

Komutativno tijelo naziva se polje.

Definicija 2.13. *Kažemo da je F polje, ako je F komutativni prsten koji zadovoljava dodatna dva svojstva.*

(1) Svaki element iz F različit od nule je invertibilan

(2) F ima barem dva elementa (netrivijalno polje).

Definicija 2.14. *Neka je* $(V,+)$ *Abelova grupa, a* F *polje. Ako je zadano preslikavanje*

$\cdot\ \ F\times V\rightarrow V$ *koje zadovoljava sljedeća svojstva:*

(1) $\alpha\cdot(\beta\cdot a)=(\alpha\beta)\cdot a$, *za sve* $\alpha,\beta\in F,\ a\in V$, *(kvaziasocijativnost)*

(2) $(\alpha+\beta)\cdot a=\alpha\cdot a+\beta\cdot a$, *za sve* $\alpha,\beta\in F,\ a\in V$,

(distributivnost operacije · u odnosu na zbrajanje u F)

(3) $\alpha\cdot(a+b)=\alpha\cdot a+\alpha\cdot b$, *za sve* $\alpha\in F,\ a,b\in V$,

(distributivnost operacije · u odnosu na zbrajanje u V)

(4) $1\cdot a=a$, *za sve* $a\in V$,

tada se uređena trojka $(V,+,\cdot)$ *naziva vektorski ili linearni prostor nad poljem* F.

Ako je $F=R$ onda govorimo o realnom vektorskom prostoru, a ako je $F=C$ onda o kompleksnom vektorskom prostoru.

Elemente skupa V zovemo vektorima, a elemente polja F skalarima. Neutralni element (nulu) Abelove grupe $(V,+)$ zovemo nulvektor. Operaciju $\cdot$ nazivamo množenje vektora skalarom i umjesto $\alpha\cdot a$ često pišemo αa. Skup koji se sastoji samo od nulvektora također je vektorski prostor, a nazivamo ga trivijalni prostor.

Definicija 2.15. *Neka je* F *polje i* V *vektorski prostor nad* F. *Ako vrijedi*

$(cu)v=c(uv)=u(cv)$, *za sve* $c\in F$ *i* $u,v\in V$,

tada se V *naziva* F*-algebra.*

2.4. Kodovi

Ovdje ćemo navesti neke osnovne pojmove iz Teorije kodiranja

Linearni [n,k] kod poljem Fp, odnosno p-arni linearni kod C duljine n i dimenzije k, je k-dimenzionalni podprostor n-dimenzionalnog vektorskog prostora nad poljem Fp. Elemente od C nazivamo kodnim riječima. Treći parametar koda je minimalna udaljenost d, koju definiramo kao

$$d \coloneqq \min\{d(c_1, c_2) | c_1, c_2 \in C, c_1 \neq c_2\},$$

gdje je Hammingova udaljenost $d(x, y)$ između dvije riječi x i y označava broj koordinata na kojima se x i y razlikuju. Ako C ima minimalnu udaljenost d, onda je gornja granica broja pogreška koje možemo ispraviti $\left\lceil \frac{d-1}{2} \right\rceil$.

Neka je C linearni $[\mathrm{n}, \mathrm{k}]$ kod. Generirajuća matrica koda C je $\mathrm{k} \times \mathrm{n}$ matrica čiji redci su vektori baze prostora C.

Dualni kod koda C definiran je kao

$$C^{\perp} \coloneqq \left\{x \in {F_p}^n | (c, x) = 0, \qquad \forall c \in C\right\},$$

Gdje $(\cdot,\cdot)$ označava standardni skalarni produkt. Dimenzija koda $C^{\perp}$ je $n - k$.

Kod C je samoortogonalni kod ako je $C \subset C^{\perp}$. U slučaju da vrijedi $C = C^{\perp}$, kod se naziva samodualni kod.

3. SMITHOVA NORMALNA FORMA

Neka je M kvadratna matrica reda n s realnim rangom r.

Smithova normalna forma matrice M je dijagonalna matrica dobivena iz M nizom elementarnih transformacija redaka i stupaca nad $\mathbb{Z}$, iz kojih se lako izvodi p-rang od M za sve proste brojeve p.

Najprije ćemo definirati osnovne pojmove i dokazati neke opće rezultate. U drugom ćemo dijelu računati Smithovu normalnu formu matrice susjedstva triangularnih grafova i grafova rešetki.

3.1. Definicije i rezultati

Definicija 3.1. Matrica M se zove *unimodularna* matrica ako je $|\det(M)| = 1$.

Kažemo da su dvije cjelobrojne matrice M i N unimodularno ekvivalentne ($M \sim N$) ako postoje unimodularne matrice P i Q takve da je $M = PNQ$.

Teorem 3.1. *Matrica M je unimodularno ekvivalentna dijagonalnoj matrici $S = diag(s_1, \dots, s_r, 0, \dots, 0)$, gdje r označava $\mathbb{R}$- rang od M i $s_i | s_{i+1}$, $1 \leq i \leq r-1$.*

Dokaz. Ako je M nul-matrica, tada se nema što dokazati. Stoga pretpostavimo da M sadrži element različit od nule koji se prikladnim izmjenama redaka i stupaca može dovesti u poziciju $(1,1)$. Primjenjujući Euklidov algoritam, taj element može biti zamijenjen najvećim zajedničkim djeliteljem elemenata prvog retka i stupca. Sada odgovarajućim operacijama na pozicijama svih elementa prvog retka i stupca, osim pozicije $(1,1)$, možemo dobiti nule. Novu matricu označimo sa $\widetilde{\mathrm{M}}$. Očito je $\mathrm{M} \sim \widetilde{\mathrm{M}}$. Pretpostavimo da $\widetilde{\mathrm{M}}$ sadrži element $\widetilde{\mathrm{m}}_{\mathrm{ij}}$ koji nije djeljiv sa elementom $\widetilde{\mathrm{m}}_{11}$. Dodamo li i-ti redak prvome retku i nastavimo li opisani postupak, dolazimo do matrice u kojoj element na poziciji $(1,1)$ dijeli svaki element matrice, a svi drugi elementi u prvom retku i prvom stupcu su jednaki nuli. Taj postupak ponavljamo koristeći matricu koju dobijemo brisanjem prvog retka i prvog stupca matrice $\widetilde{\mathrm{M}}$. Budući da unimodularno ekvivalentne matrice imaju isti rang, na kraju dobivamo dijagonalnu matricu sa traženim svojstvima.

$\square$

Teorem 3.2. *Dijagonalni elementi matrice S koji su opisani teoremom 3.1 jedinstveni su do na predznak.*

Za dokaz ovog teorema uvodimo koncept determinantnih djelitelja od M, $d_i(M), 1 \leq i \leq n$. Ti su djelitelji definirani kao najveći zajednički djelitelj svih determinanti od $i \times i$ podmatrica matrice M.

Dokaz. Iz činjenice da unimodularno ekvivalentne matrice imaju iste determinantne djelitelje (Newman, M., *Integral Matrices*, Academic Press, London, 1972.), proizlazi da

$$d_i(M) = \prod_{j=1}^{i} s_j, \ \ 1 \leq i \leq r.$$

Dakle, $s_1 = d_1(M)$ i $s_i = d_i(M)/d_{i-1}(M), \ 2 \leq i \leq r$. Budući da su determinantni djelitelji određeni do na predznak, dokaz je gotov.

□

Matrica S se naziva *Smithova normalna forma* (SNF) matrice M. Koristit ćemo oznaku $S(M)$. Elementi s_i nazivaju se invarijantni faktori od M.

Iz $S(M)$ lakše se dolazi do p- ranga matrice M.

Neka je $S(M) = \text{diag}(s_1, \dots, s_r, 0, \dots, 0)$. Tada $r_p(M) = r_p(S(M)) = r^*$, gdje r^* zadovoljava da p ne dijeli s_{r^*} i $p|s_{r^*+1}$. Očito je $r_p(M) \leq r$, rangu od M nad poljem $\mathbb{R}$.

Primjer 3.1. *Odredimo Smithovu normalnu formu za danu matricu*

$$A = \begin{pmatrix} 2 & 4 & 4 \\ -6 & 6 & 12 \\ 10 & -4 & -16 \end{pmatrix}.$$

Vrijedi: $\begin{pmatrix} 2 & 4 & 4 \\ -6 & 6 & 12 \\ 10 & -4 & -16 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 4 \\ 0 & 18 & 24 \\ 0 & -24 & -36 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & 24 \\ 0 & -24 & -36 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & 24 \\ 0 & -6 & -12 \end{pmatrix} \sim$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 12 \\ 0 & 18 & 24 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 12 \\ 0 & 0 & -12 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \end{pmatrix}.$$

Dakle, $S(A) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \end{pmatrix}$.

Primjer 3.2. *Odredimo Smithovu normalnu formu za matricu $J_4 - I_4$, matricu susjedstva potpunog grafa s 4 vrha.*

$$J_4 - I_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Slijedi:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Dakle,

$$S(J_4 - I_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Primjer 3.3. *Odredimo Smithovu normalnu formu za matricu $J_n - I_n$, matricu susjedstva potpunog grafa s n vrhova.*

$$J_n - I_n = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -1 \end{pmatrix} \sim \mathbf{diag}(1^{n-1}, n-1).$$

Vrijedi:

$$r_p(J_n - I_n) = \begin{cases} n-1, & ako\ p|(n-1), \\ n & inače. \end{cases}$$

Općenito, $S(J_n - I_n) = \mathrm{diag}(1, r^{n-2}, r(r+n)), r \in \mathbb{Z}$.

Ako je za M poznata unimodularno ekvivalentna dijagonalna matrica, tada se $S(M)$ lako određuje. Neka je $S(M) = \text{diag}(s_1, \dots, , s_r, 0, \dots, 0)$ i neka je $\{p_1, \dots, p_k\}$ potpuni skup prostih brojeva koji se javljaju kao djelitelji od s_i. Za odgovarajuće nenegativne cijele brojeve imamo e_{ij} imamo

$$s_1 = {p_1}^{e_{11}} {p_2}^{e_{12}} \cdots {p_k}^{e_{1k}},$$

$$\vdots$$

$$s_r = {p_1}^{e_{r1}} {p_2}^{e_{r2}} \cdots {p_k}^{e_{rk}}.$$

Kako $s_i | s_{i+1}, 1 \leq i \leq r-1$, za e_{ij} vrijedi

$$0 \leq e_{1j} \leq e_{21} \leq \cdots \leq e_{rj}, \qquad 1 \leq j \leq k.$$

Skup prostih potencija ${p_j}^{e_{ij}}, 1 \leq i \leq r, 1 \leq j \leq k$, uključujući ponovljene vrijednosti, naziva se skupom elementarnih djelitelja. Obzirom na ovaj skup, invarijantni djelitelji mogu se jednostavno rekonstruirati.

Ako

$$e_j \coloneqq \max_{1 \leq i \leq r} e_{ij}, 1 \leq j \leq k,$$

Tada $s_r = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k}$. Brisanjem ovih prostih brojeva iz skupa elementarnih djelitelja, određujemo s_{r-1} na isti način i postupak nastavljamo. Dolazimo do sljedećeg teorema:

Teorem 3.3. *Ako je* $M \sim \Lambda = \text{diag}(\lambda_1, \dots, \lambda_r, 0, \dots, 0)$, *onda je skup potencija prostih faktora od* $\lambda_i, 1 \leq i \leq r$, *jednak skupu elementarnih djelitelja matrice* $S(M)$.

Dokaz. Najprije, iz Teorema 3.2 slijedi da je *je* $S(M) = S(\Lambda)$. Neka je p bilo koji prost broj koji dijeli neke $\lambda_i, 1 \leq i \leq r$. Poredajmo λ_i prema rastućim potencijama od p:

$$\lambda_{i1} = p^{e_1} \mu_1, \qquad (p, \mu_1) = 1,$$

$$\vdots$$

$$\lambda_{ir} = p^{e_r} \mu_r, \qquad (p, \mu_r) = 1,$$

Dakle $0 \leq e_1 \leq \cdots \leq e_r$. Tada d_i, i-ti determinantni djelitelj od Λ, zadovoljava

$$d_i = p^{e_1 \cdots e_i} \mu, \qquad (p, \mu) = 1.$$

Stoga, ako s_i označava i-ti invarijatni faktor od od Λ, pa i od $S(M)$, tada

$$s_1 = d_1,$$

$$s_i = d_i / d_{i-1} = p^{e_i} \bar{\mu}, \qquad (p, \bar{\mu}) = 1.$$

Dakle, p^{e_i} je elementarni djelitelj, $1 \leq i \leq r$. Primjenom istog argumenta za sve proste brojeve p koji dijele neki λ_i, dobivamo rezultat.

$\square$

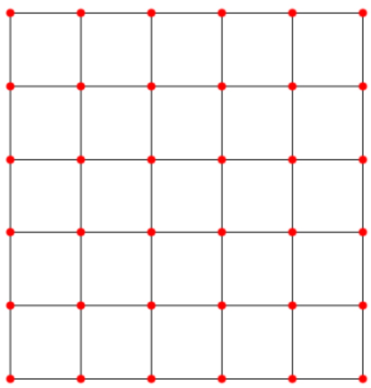
3.2. **Primjene** Smithove normalne forme

Matrice susjedstva grafova rešetki i triangularnih grafova imaju vrlo jednostavnu strukturu, što nam omogućuje ručno izračunavanje njihove Smithove normalne forme.

Primjer 3.4. *Graf kvadratne rešetke* $L_2(n)$ *sastoji se od vrhova skupa* $S \times S$, *gdje je* S *skup kardinaliteta* n; *dva različita vrha su susjedna ako se podudaraju u jednoj koordinati. Graf* $L_2(n)$ *je jako regularan s parametrima*

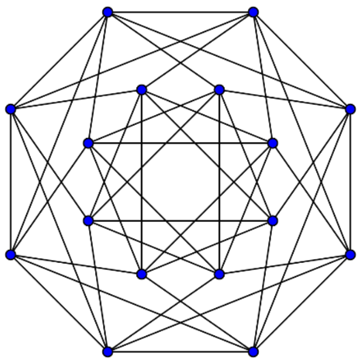
$$(v, k, \lambda, \mu) = (n^2, 2(n-1), n-2, 2).$$

Parametar v *lako dobijemo jer koordinatu* x *iz uređenog para* (x, y) *skupa* $S \times S$ *možemo izabrati na* n *načina. Analogno radimo za koordinatu* y *i ukupno dobivamo* n^2 *vrhova. Nadalje, neka je* (x, y) *jedan vrh našeg grafa. Postoji* $n-1$ *uređenih parova koji kao prvu koordinatu sadrže element* x *uz uvjet da druga koordinata nije* y. *Analogno ponavljamo postupak za koordinatu* y *i zaključujemo da je* $k = 2\,(n-1)$. *Nadalje, neka su* $\{x, y\}$ *i* $\{x, z\}$ *dva susjedna vrha grafa. Njihovi zajednički susjedi su svi oni vrhovi koji sadrže koordinatu* x *kao prvu koordinatu, a ne sadrže koordinate* y *i* z *kao drugu koordinatu. Slijedi da je* $\lambda = n - 2$. *Neka su sada* $\{x, y\}$ *i* $\{z, w\}$ *dva nesusjedna vrha grafa. Svi njihovi zajednički susjedi su vrhovi* $\{x, w\}$ *i* $\{z, y\}$. *Slijedi da je* $\mu = 2$.



Slika 4. Graf $L_2(6)$

Za $n \neq 4$, $L_2(n)$ je jedinstven, odnosno svaki jako regularan graf s istim parametrima je izomorfan grafu $L_2(n)$. Za $n = 4$ postoji točno jedan neizomorfan kospektralni graf, Shrikhande graf.



Slika 5. Shrikhande graf

Sljedeću ćemo propoziciju iskazati, a dokaz se može pronaći u diplomskom radu C.A. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, Eindhoven University of Technology, 1991.

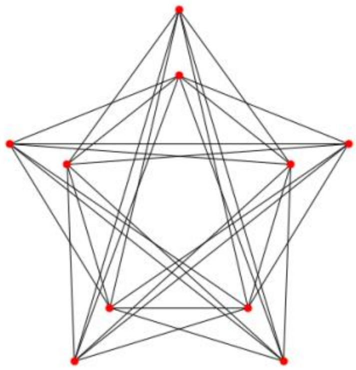
Propozicija 3.1. *SNF grafa rešetke $L_2(n)$ jednaka je*

$$diag\left(1^{2n-2}, 2^{(n-2)^2}, \{2(n-2)\}^{2n-3}, 2(n-1)(n-2)\right).$$

Primjer 3.5. *Neka je zadan skup $S = \{1, \dots, n\}$, pri čemu je $n \geq 4$. Neka je skup vrhova V jednak skupu dvočlanih podskupova skupa S, odnosno skupa kardinalnosti n. Triangularni graf $T(n)$ $(n \geq 4)$, uz definiciju da su dva vrha susjedna ako nisu disjunktna, je jako regularan, s parametrima*

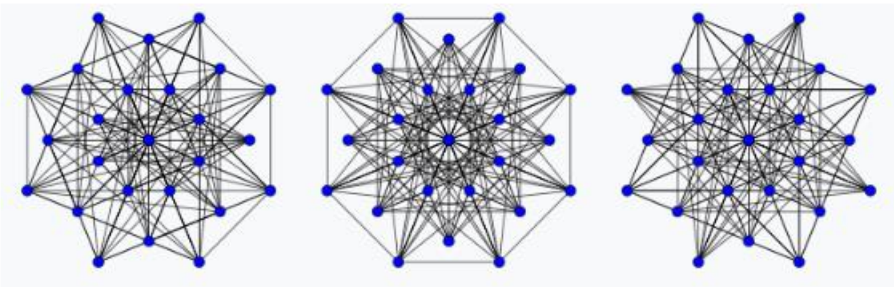
$$(v, k, \lambda, \mu) = \left(\frac{1}{2}n(n-1), 2(n-2), n-2, 4\right).$$

Parametar v lako dobijemo jer je to upravo broj dvočlanih podskupova n-članog skupa. Nadalje, neka je $\{x, y\}$ jedan vrh našeg grafa. Postoje $n-2$ dvočlana podskupa koji sadrže element x uz uvjet da drugi element u tom podskupu nije y. Analogno ponavljamo postupak za element y i zaključujemo da je $k = 2(n-2)$. Nadalje, neka su $\{x, y\}$ i $\{y, z\}$ dva susjedna vrha grafa. Njihovi zajednički susjedi su svi oni vrhovi koji sadrže element y, a ne sadrže elemente x i z uz specijalan slučaj $\{x, z\}$. Slijedi da je $\lambda = (n-1) - 1 - 1 + 1$ iz čega *zaključujemo da je $\lambda = n - 2$. Neka su sada $\{x, y\}$ i $\{z, w\}$ dva nesusjedna vrha grafa. Svi njihovi zajednički susjedi su vrhovi $\{x, z\}$, $\{x, w\}$, $\{y, z\}$ i $\{y, w\}$. Slijedi da je* $\mu = 4$.



Slika 6. Graf T(5)

$T(n)$ je jedinstveni jako regularan graf s parametrima $\left(\frac{1}{2}n(n-1), 2(n-2), n-2, 4\right)$, osim za $n = 8$. U tom slučaju postoje tri neizomorfna grafa, Changovi grafovi.



Slika 7. Changovi grafovi

Propozicija 3.2. SNF triangularnog grafa $T(n)$ jednaka je

$$\operatorname{diag}\left(1^{n-2}, 2^{\frac{1}{2}(n-2)(n-3)}, \{2(n-4)\}^{n-2}, (n-2)(n-4)\right) \text{ ako } 2|n,$$

$$\operatorname{diag}\left(1^{n-2}, 2^{\frac{1}{2}(n-1)(n-4)}, \{2(n-4)\}^{n-2}, 2(n-2)(n-4)\right) \text{ ako } 2|n \text{ inače.}$$

Dokaz propozicije se može pronaći u diplomskom radu C.A. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, Eindhoven University of Technology, 1991.

Sjetimo se da ako je $r_p(M) = r$, tada se M može svesti na dijagonalnu matricu nad poljem F_p $\text{diag}(1^r, 0^{n-r})$, takozvani kanonski oblik. Općenito, postojat će samo nekoliko prostih brojeva p za koje $r_p(M) < n$, budući da je $r_p(M) = n$, osim ako je p djelitelj od $\det(M)$. Stoga u praksi neće biti puno učinkovitije izračunati SNF od M od određivanja kanonskog oblika za one proste brojeve p koji dijele $\det(M)$.

U sljedećem ćemo poglavlju pokušati odrediti p-rang nekolicine (klasa) jako regularnih grafova, bez korištenja do sada spomenutih metoda. Za neke proste brojeve rang se može izračunati na prilično jednostavan način, dok za ostale brojeve možemo izvesti samo granice. U dokazima će se često koristiti sljedeća lema.

Lema 3.1. *Neka je M regularna matrica i pretpostavimo da $p^k || det(M)$. Tada je $r_p(M) \geq n - k$. (Pod $p^k||a, a \in \mathbb{Z}$, mislimo da $p^k|a$, ali da p^{k+1} nije djelitelj od a.)*

Dokaz. Budući da je $\det(S(M)) = \det(M) \neq 0$, dijagonalni elementi s_i matrice $S(M)$ različiti su od nule za $1 \leq i \leq n$. Nadalje, zbog $s_i|s_{i+1}, 1 \leq i \leq n-1$, najviše k invarijantnih faktora djeljivo je s p.

□

4. O p -RANGU MATRICA JAKO REGULARNIH GRAFOVA S CJELOBROJNIM SVOJSTVENIM VRIJEDNOSTIMA

Neka je Γ jako regularan graf sa v vrhova sa cjelobrojnim svojstvenim vrijednostima k, r i s. U ovome ćemo poglavlju pokazati da je p-rang matrice A u potpunosti određen parametrima grafa Γ, u slučaju kada p ne dijeli i r i s. Za preostale proste brojeve p izvest ćemo gornju granicu za $r_p(A)$. Sličan rezultat dobiven je za p-rang matrice $A + rI, r \in \mathbb{Z}$. Ispitat ćemo kako su povezani p-rangovi grafova ekvivalentnih s obzorom na switching.

4.1. Uvodne leme

Iskazat ćemo nekoliko elementarnih, ali korisnih lema iz teorije matrica. Leme nećemo dokazivati, a dokazi se mogu pronaći u nekom od udžbenika iz teorije matrica, primjerice Marcus, M. and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities*, Allyn and Bacon, Boston, 1964.

Neka su M, M_1 i M_2 kvadratne matrice reda n nad poljem F.

Lema 4.1 *Neka je $M = M_1 + M_2$. Tada vrijedi:*

$$|r_F(M_1) - r_F(M_2)| \leq r_F(M) \leq r_F(M_1) + r_F(M_2).$$

Posebno, $|r_F(M) - r_F(J_n - M)| \leq 1$.

Lema 4.2 *Neka je $M = M_1 M_2$. Tada vrijedi:*

$$r_F(M_1) + r_F(M_2) - n \leq r_F(M) \leq min\big(r_F(M_1), r_F(M_2)\big).$$

Ova se lema uglavnom koristi u jednom od sljedećih oblika:

(a) Ako je $M_1 M_2 = O_n$, onda $r_F(M_1) + r_F(M_2) \leq n$;

(b) Ako je $M_1 M_2 = J_n$, onda $r_F(M_1) + r_F(M_2) \leq n + 1$.

Lema 4.3 *Neka je* $\lambda_1 \dots, \lambda_k,\ \lambda_i \in F, \lambda_i \neq \lambda_j$ *za* $i \neq j$ *potpuni skup svojstvenih vrijednosti od* M*. Ekvivalentno je:*

1. $\Pi_{i=1}^{k}(M - \lambda_i I) = 0_n$
2. $\Sigma_{i=1}^{k}\dim (N_F((M - \lambda_i I)) = n.$

4.2. Opći teoremi

U ovome odjeljku neka je A matrica susjedstva jako regularnog grafa Γ sa parametrima (v, k, λ, μ) tako da su njene cjelobrojne svojstvene vrijednosti k, r, s kratnosti $1, f, g$, redom. Označimo rang matrice A nad $\mathbb{R}$ sa $r(A)$.

Teorem 4.1. *Neka je* $a_0 \coloneqq k(mod\, p), a_1 \coloneqq r(mod\, p), a_2 \coloneqq s(mod\, p)$. *Tada vrijedi* sljedeće:

(i) $ako\ je\ točno\ jedna\ od\ vrijednosti\ a_0, a_1, a_2\ jednaka\ nuli, a\ recimo\ a_i\ kratnosti\ m_i,$ $onda\ vrijedi\ r_p(A) = v - m_i;$

(ii) $ako\ a_0 = 0, a_1 = 0\ i\ a_2 \neq 0, onda\ r_p(A) = g;$

(iii) $ako\ a_0 = 0, a_1 \neq 0\ i\ a_2 = 0, onda\ r_p(A) = f;$

(iv) $ako\ a_1 = 0\ i\ a_2 = 0\ i\ a_2 = 0, onda\ r_p(A) \leq \min(f, g) + 1.$

Dokaz teorema može se pronaći u diplomskom radu C.A. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, Eindhoven University of Technology, 1991.

Dakle, jedini prosti brojevi p za koje je određivanje $r_p(A)$ netrivijalno su brojevi koji su djelitelji od r i od s.

Dolazi do pitanja je li gornja granica u slučaju (iv) dobra. Prema rezultatima u diplomskom radu *On the p-rank of the adjacency matrices of strongly regular graphs*, mogli bismo zaključiti kako je granica često prilično dobra. Međutim, za većinu ispitanih grafova su f i g mali (< 25), stoga općenito ne možemo zaključiti mnogo. Ponekad se nešto bolja granica iz slučaja (iv) može dobiti na način koji slijedi. Bez smanjenja općenitosti, možemo pretpostaviti da je $f < g$. Tada prema Teoremu 4.1 vrijedi da je $r_p(A) \leq f + 1$. Promotrimo minimalnu idempotentu E_i za koju vrijedi $r(E_i) = f$. Neka je c_1 najmanji cijeli broj takav da je $c_1 E_1$ cjelobrojna matrica, primjerice

$$c_1 E_1 = c_{10} I + c_{11} A + c_{12} B, \qquad c_{1i} \in \mathbb{Z}.$$

Pretpostavimo da $p|c_{10}$, $p|c_{12}$ i $p \nmid c_{11}$. Tada je $r_p(A) = r_p(c_1 E_1) \leq r(c_1 E_1) = f$.

Sljedeći je teorem generalizacija Teorema 4.1 za $A + rI, r \in \mathbb{Z}$. Ovdje je spektar $(k+r)^1, (r+r)^f, (s+r)^g$, gdje su kratnosti zapisane kao eksponenti.

Teorem 4.2. *Neka je* $a_0 \coloneqq (k+r)(mod\, p), a_1 \coloneqq (r+r)(mod\, p), a_2 \coloneqq (s+r)(mod\, p)$. *Tada vrijedi sljedeće:*

(i) $ako\ je\ točno\ jedna\ od\ vrijednosti\ a_0, a_1, a_2\ jednaka\ nuli, a\ recimo\ a_i\ kratnosti\ m_i,$ $onda\ vrijedi\ r_p(A + rI) = v - m_i;$

(ii) $ako\ a_0 = 0, a_1 = 0\ i\ a_2 \neq 0, onda\ r_p(A + rI) = g + \varepsilon, gdje\ je\ \varepsilon = 0\ ako\ p|\mu,$ $inače\ \varepsilon = 1;$

(iii) $ako\ a_0 = 0, a_1 \neq 0\ i\ a_2 = 0, onda\ r_p(A + rI) = f + \varepsilon, gdje\ je\ \varepsilon = 0\ ko\ p|\mu,$ $inače\ \varepsilon = 1;$

(iv) $ako\ a_1 = 0\ i\ a_2 = 0\ i\ a_2 = 0, onda\ r_p(A + rI) \leq min(f, g) + 1.$

Dokaz. Dokazat ćemo samo tvrdnju *(ii)*.

$$\begin{aligned} (A + rI)(A - sI) &= (k - \mu - rs)I + (\lambda - \mu + r - s)A + \mu J \\ &= -s(r+r)I + (r+r)A + \mu J \\ &\equiv \mu J (\mathrm{mod}\, p). \end{aligned}$$

Iz *(i)* slijedi da je $r_p(A - sI) = f + 1$ pod pretpostavkom da vrijedi tvrdnja *(ii)*. Zamijenimo li A sa $A + rI$, prema Teoremu 4.1 i Lemi 4.2,

$$g \leq r_p(A + rI) \leq g + r_p(\mu J).$$

Prema tvrdnji Leme 4.3, $r_p(A + rI) = g$ ako i samo ako

$$(A + rI)(A - sI) \equiv 0 (\mathrm{mod}\, p).$$

Dakle, zaključak vrijedi.

□

Tako se kod proučavanja p-ranga matrice $A+rI$ za dani jako regularni graf Γ sa cjelobrojnim svojstvenim vrijednostima k, r i s možemo ograničiti na vrijednosti p i r za koje je $r+r$ i $s+r$ djeljivo sa p. Ne postoji opća strategija za određivanje (granica) p-ranga matrice $A+rI$. Slijedi nekoliko lema koje bi mogle biti korisne kod određivanja granica, pogotovo za male f ili g. Često je lako dobiti donju granicu iz induciranog grafa, što ćemo pokazati u primjerima koji slijede.

4.3. Granice za p-rang pomoću podgrafa i primjeri

Neka je Γ jako regularan graf, ne nužno sa cjelobrojnim svojstvenim vrijednostima, i neka je $r \in \mathbb{Z}$. Pretpostavimo da Γ sadrži inducirani podgraf Γ' sa v' vrhova. Neka je A' matrica susjedstva grafa Γ'. Tada je očito $r_p(A+rI_v) \geq r_p(A'+rI_{v'})$. Vrijedi sljedeća lema.

Lema 4.4. *Ako graf Γ sadrži kliku veličine n i $r \not\equiv 1 (mod\ p)$, onda*

$$r_p(A+rI) \geq \begin{cases} n-1 & ako\ p|(n+r-1), \\ n & inače. \end{cases}$$

Dokaz. Ako Γ sadrži kliku veličine n, onda je $J_n+(r-1)I_n$ podmatrica od $A+rI_v$. U primjeru 3.3 je izvedeno da $S(J_n+(r-1)I_n) = \mathrm{diag}(1, (r-1)^{n-2}, (r-1)(n+r-1))$, iz čega slijedi rezultat.

□

Ako Γ sadrži kokliku veličine n, tada je n donja granica za $r_p(A+rI)$ ako r nije djeljiv sa p. S druge strane, Teorem 4.2 daje gornju granicu za kokliku u jako regularnom grafu sa cjelobrojnim svojstvenim vrijednostima.

Propozicija 4.1. *Veličina koklike u jako regularnom grafu sa cjelobrojnim svojstvenim vrijednostima je najviše jednaka* $\min(f,g)+1$.

Dokaz. Neka je C koklika u jako regularnom grafu Γ i neka je $n := |C|$. Neka su p_1 i p_2 dva (ne nužno različita) prosta broja tako da vrijedi $p_1|(r+1)$ i $p_2|(s-1)$ (takvi prosti brojevi postoje jer su i r i s različiti on nule). Tada, pod pretpostavkom da su sve svojstvene vrijednosti od Γ cijeli brojevi, iz Teorema 4.2 slijedi:

$$n \leq r_{p1}(A + I) \leq g + 1,$$

$$n \leq r_{p2}(A - I) \leq f + 1.$$

Dakle, propozicija je dokazana.

□

Ovime smo gotovo dokazali Cvetkovićevu granicu za jako regularne grafove sa cjelobrojnim svojstvenim vrijednostima. Ta granica podrazumijeva da veličina koklike C u grafu Γ ne može premašiti broj nenegativnih (nepozitivnih) svojstvenih vrijednosti od Γ (Cvetković, D.M., M. Doob and H. Sachs, *Spectra of Graphs: Theory and Application*. Academic Press, New York, 1980.). Za jako regularne grafove iz toga vrijedi $|C| \leq \min(f + 1, g)$.

Naš je problem povezan s drugim problemom Teorije grafova, odnosno određivanjem kromatskog broja od Γ. Kromatski se broj obično označava sa $\chi(\Gamma)$. Definira se kao najmanji broj različitih boja potrebnih za pravilno bojenje grafa Γ, odnosno bojenje svih vrhova od Γ tako da su susjedni vrhovi obojani međusobno različitim bojama. Ako je $\chi(\Gamma) = \chi$, tada postoji jedna koklika veličine najmanje $\lceil v/\chi \rceil$ koja je sadržana u Γ. Stoga gornja granica za $\chi(\Gamma)$ daje donju granicu za $r_p(A + rI)$ kada $p \nmid r$ i obratno. Opća gornja granica za $\chi(\Gamma)$ ipak ne daje korisne informacije za donju granicu za $r_p(A + rI)$.

Kada proučavamo p-rang danog grafa, promatrat ćemo $r_p(A + rI)$ i $r_p(J - A - rI)$. Odnos između navedena dva ranga možemo izraziti na sljedeći način:

$$\dim\big(R_p(A + rI) + \langle \underline{1} \rangle\big) = \dim\big(R_p(J - A - rI) + \langle \underline{1} \rangle\big) \qquad (4.1)$$

S obzirom na navedeno, sljedeća lema može biti korisna.

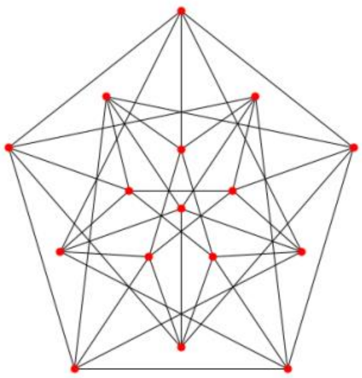
Lema 4.5. *Ako* $p \nmid v$, $p|k$, *onda* $r_p(J - A) = r_p(A) + 1$.

Dokaz. Imamo $\underline{1}(J - A) = (v - k)\underline{1} \not\equiv \underline{0} (\mathrm{mod}\, p)$, tako da $\underline{1} \in R_p(J - A)$. Promotrimo A kao generirajuću matricu p-arnog linearnog koda C. Budući da $(r, \underline{1}) = k \equiv 0 (\mathrm{mod}\, p)$ vrijedi za svaki redak $\underline{r}$ matrice A, dualni kod $C^{\perp}$ sadrži $\underline{1}$. Kako $(\underline{1}, \underline{1} = v \not\equiv 0 (\mathrm{mod}\, p)$, vektor čije su sve koordinate jedinice nije sadržan u $R_p(A)$. Zaključak sada slijedi iz (4.1).

□

Lema 4.6. 2-*rang matrice susjedstva bilo kojeg grafa je paran*.

Primjer 4.1. *Clebschov graf je graf koji ima za vrhove sve podskupove skupa* $\{1, 2, 3, 4, 5\}$ *koji su parne kardinalnosti. Dva vrha su susjedna ako im simetrična razlika ima kardinalnost* 4. *To je jako regularan graf s parametrima* $(16, 5, 0, 2)$. *Komplement Clebschova grafa je također jako regularan graf, s parametrima* $(16, 10, 6, 6)$.



Slika 8. Clebschov graf

Spektar Clebschovog grafa je $5^1, 1^{10}, (-3)^5$. *Sada trebamo odrediti* 2-*rang od* $A + I$ *i* $B \coloneqq J - A - I$. *Prema Teoremu 4.2, imamo* $r_2(A + I) \leq 6$. *Sada promotrimo podgraf sa 5 vrhova kardinalnosti 4 i vrhom* $\{1,2\}$. *Neka je* A' *odgovarajuća podmatrica od* A. *Tada*

$$A' + I_6 = \left(\begin{array}{c|c} I_5 & \underline{x}^T \\ \hline \underline{x} & 1 \end{array} \right),$$

gdje $\underline{x} = (00011)$.

Kako je $r_2(A + I_{16}) \geq r_2(A' + I_6) = 6$, *zaključujemo da* $r_2(A + I) = 6$.

Nadalje, $|r_2(A + I) - r_2(B)| \leq 1$ *(prema Lemi 4.1) i* $r_2(B)$ *je paran (Lema 4.6), dakle* $r_2(B) = 6$.

4.4. Grafovi ekvivalentni s obzirom na switching

U drugome je poglavlju pokazano da je p-rang jako regularnog grafa s cjelobrojnim svojstvenim vrijednostima potpuno određen svojim spektrom onda kada p nije djelitelj oba od brojeva r i s. Stoga kospektralni grafovi imaju isti p-rang za proste brojeve p koji zadovoljavaju ovaj uvjet. Međutim, ako $p|r$ i $p|s$, ovo nužno ne mora vrijediti. Primjerice, triangularni graf $T(8)$ i Changovi grafovi imaju različite 2-rangove. Jasno, izomorfni grafovi imaju isti rang nad bilo kojim poljem F_p jer označavanje redaka i stupaca na drugačiji način ne mijenja rang matrice.

Grafovi ekvivalentni s obzirom na switching ne moraju biti izomorfni ili kospektralni, ali kada je p-rang jednog od njih poznat, postoji samo nekoliko mogućih vrijednosti za p-rang drugog grafa ili ostalih grafova.

Lema 4.7. *Ako su grafovi Γ_1 i Γ_2 ekvivalentni s obzirom na switching, vrijedi*

$$|r_p(\mathrm{A}_1) - r_p(\mathrm{A}_2)| \leq 2.$$

Naravno, ova lema vrijedi i kada matrice A_1 i A_2 zamijenimo sa $\mathrm{A}_1 + rI$ i $\mathrm{A}_2 + rI$, za $r \in \mathbb{Z}$.

Lema 4.8. *Neka je Γ jako regularan graf sa v vrhova koji je ekvivalentan s obzirom na switching disjunktnoj uniji vrha i jako regularnog grafa Γ' sa $v-1$ vrhom. Svojstvene vrijednosti od Γ označimo sa k, r i s.*

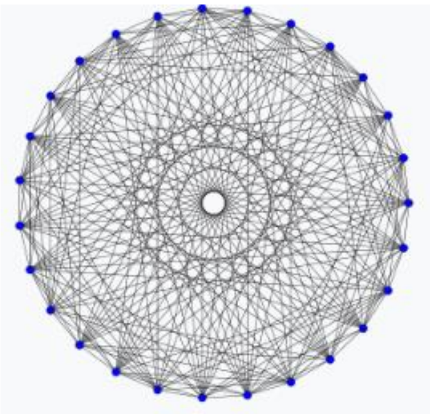
(a) Ako $2|r$ i $2|s$, onda $r_2(A_\Gamma) = r_2(A_{\Gamma'}) + \varepsilon$, gdje $\varepsilon = 2$ ako $\underline{1} \in R_2(A_\Gamma)$, inače $\varepsilon = 0$.

(b) Ako $2|(r+1)$ i $2|(s+1)$, onda $|r_2(A_\Gamma + I_v) - r_2(A_{\Gamma'} + I_{v-1})| \leq 1$.

Kako bismo objasnili navedeno, izračunat ćemo 2-rang Schläfli grafa i Changovog grafa, koje možemo dobiti zamjenom iz grafa $T(8)$.

Primjer 4.1. *Triangularne grafove smo opisali u prošlom poglavlju. Skupu vrhova grafa $T(8)$ pripadaju dvočlani podskupovi skupa $\{1, \dots, 8\}$. Dva su vrha susjeda ako nisu disjunktni. Graf $T(8)$ ima parametre $(v, k, \lambda, \mu) = (28, 12, 6, 4)$, spektar $12^1, 4^7, (-2)^{20}$ i njegov 2-rang je 6.*

Schläfli graf Γ_s dobiva se iz grafa $T(8)$ izoliranjem jednog vrha kroz zamjenu(switching) i onda ga uklanjajući. Njegovi su parametri $(v, k, \lambda, \mu) = (27, 16, 10, 8)$, spektar $27^1, 4^6, (-2)^{20}$. Može se pokazati da je Schläfli graf jedinstven, odnosno svaki jako regularan graf s istim parametrima je izomorfan ovom grafu.



Slika 9. Schläfli graf

Neka je A_s matrica susjedstva grafa Γ_s. Sada promatramo matricu susjedstva A_8. Za prvi redak uzmimo karakteristični vektor skupa zamjene, odnosno zamjena se izvodi s obzirom na skup $\{\{1, x\}, \{2, x\} | 3 \leq x \leq 8\}$ i vrh $\{1,2\}$ je izoliran. Tada se prvih šest redaka matrice A_s može zapisati na sljedeći način:

$$\left(\begin{array}{c|c|c|c|c|c} J_6 - I_6 & I_6 & \begin{matrix} 0_5^1 \\ J_5 - I_5 \end{matrix} & \cdots & \begin{matrix} 1_2^3 \\ 0_2^1 \\ J_2 - I_2 \end{matrix} & \begin{matrix} 1_1^4 \\ 0 \\ 0 \end{matrix} \end{array}\right).$$

Vidimo kako je I_6 podmatrica matrice A_s. Stoga $r_2(A_s) \geq 6$ i jednakost vrijedi zbog Leme 4.8 i činjenice da je $r_2(A_8) = 6$.

Changovi grafovi dobiveni su iz grafa $T(8)$ zamjenom tako da je skup zamjene:

(C_1) $\{\{1,2\}, \{3,4\}, \{5,6\}, \{7,8\}\}$;

(C_2) $\{\{1,2\}, \{2,3\}, \{3,4\}, \{4,5\}, \{5,6\}, \{6,7\} \{7,8\}, \{1,8\}\}$;

(C_3) $\{\{1,2\}, \{2,3\}, \{1,3\}, \{4,5\}, \{5,6\}, \{6,7\} \{7,8\}, \{4,8\}\}$.

Svi Changovi grafovi imaju iste parametre kao graf $T(8)$. Ne postoji niti jedan drugi jako regularan graf sa istim parametrima.

Za svaki i, $1 \leq i \leq 3$, jednostavno je naći podmatricu A'_C matrice A_C, čiji 2-rang iznosi 8. Te su podmatrice formirane od redaka i stupaca označenih sa $\{\{1,2\}, \dots, \{1,8\}, \{x, y\}\}$, gdje $\{x, y\} = \{3,5\}$ za graf C_1 i $\{x, y\} = \{2,4\}$ za grafove C_2 i C_3.

$$A'_{C_1} = \left(\begin{array}{c|c|c} & & 1 \\ \hline & J_6 - I_6 & \underline{v}_1^T \\ \hline 1 & \underline{v}_1 & \end{array}\right), A'_{C_2} = \left(\begin{array}{c|c|c|c} & & 1 & \\ \hline & J_5 - I_5 & & \underline{v}_2^T \\ \hline 1 & & & 1 \\ \hline & \underline{v}_2 & 1 & \end{array}\right), A'_{C_3} = \left(\begin{array}{c|c|c|c} & 1 & & \\ \hline 1 & & & 1 \\ \hline & & J_5 - I_5 & \underline{v}_3^T \\ \hline & 1 & \underline{v}_3 & \end{array}\right),$$

Gdje $\underline{v_1} = (101000), \underline{v_2} = (01000)$ i $\underline{v_3} = (10000)$.

Stoga $8 \leq r_2(A_{C_i}) \leq r_2(A_8) + 2 = 8$ za $1 \leq i \leq 3$, gdje desna nejednakost slijedi iz Leme 4.7. Naravno, gornja granica je također dobivena iz Teorema 4.1.

Neka $\underline{c}_1$ označava karakteristični vektor skupa zamjene grafova $T(8)$ i C_1. Iz Leme 4.8 slijedi da $\underline{1} \notin R_2(A_8)$. Sada se može dobiti:

$$8 \geq \dim\left(R_2(A_8) + \langle \underline{c}_1 \rangle\right) + 1 = \dim\left(R_2(A_{C_1}) + \langle \underline{c}_1, \underline{1} \rangle\right) \geq 8,$$

što je moguće jedino ako $\langle \underline{c}_1, \underline{1} \rangle \subset R_2(A_{C_1})$ i $\underline{c}_1 \notin R_2(A_8)$. Iz A'_{C_1} možemo vidjeti da $\sum_{i \in \{2,4,6,7,8\}} \underline{r}_{\{1,i\}} + \underline{r}_{\{3,5\}} \equiv \underline{1} \pmod 2$ mora postojati. Budući da se $\underline{1}$ može zapisati kao suma parnih brojeva redaka od A_{C_1}, ovaj vektor je također sadržan u $R_2(J_{28} - A_{C_1})$. Stoga $r_2(J_{28} - A_{C_1}) = R_2(A_{C_1}) = 8$. Isti argumenti se mogu upotrijebiti za pokazati da je $r_2(J_{28} - A_{C_2}) = r_2(J_{28} - A_{C_3}) = 8$.

Lema 4.5 daje da $r_2(J_{27} - A_S) = 7$. Konačno, budući da je I_7 podmatrica od $J_{28} - A_8$ i $|J_{28} - A_8| - r_2(A_8)| \leq 1$, zaključujemo da je $r_2(J_{28} - A_8) = 7$.

5. ZAKLJUČAK

U ovome smo seminaru mogli vidjeti kako p-rang matrice susjedstva jako regularnog grafa nije moguće u potpunosti odrediti. Ipak, za neke smo specifične slučajeve pokazali donje i gornje granice za vrijednosti p-ranga. Ispitujući strukturu grafa, mogli bismo što preciznije odrediti p-rang. Pokazali smo kako je p-rang matrice sa cjelobrojnim koeficijentima lako izvesti iz Smithove normalne forme. Također, pokazali smo povezanost p-ranga za međusobno izomorfne grafove i grafove ekvivalentne s obzirom na switching.

POPIS SLIKA

LITERATURA

1. Brouwer, Andries E., van Eijl, Cleola A., On the p-rank of the adjacency matrices of strongly regular graphs, J. Algebraic Combin. 1 (1992), 329-346.
2. Crnoja, Luka, *Jako regularni grafovi,* diplomski rad, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, 2018.
3. Grbac, Neven, Mikulić Crnković, Vedrana, *Algebarske strukture,* skripta, Odjel za matematiku, Sveučilište u Rijeci, 2011.
4. Franušić, Zrinka, Šiftar, Juraj, *Linearna algebra 1,* skripta za nastavničke studije na PMF-MO
5. Horvatić, Krešimir, *Linearna algebra,* Golden marketing - Tehnička knjiga, Zagreb, 2004.
6. Van Eijl, Cleola A, On the p-rank of the adjacency matrices of strongly regular graphs, MSc thesis, Eindhoven University of Technology, 1991..