Slučajni Cayleyevi grafovi

Mihovilić, Lugo

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lugo Mihovilić

SLUČAJNI CAYLEYEVI GRAFOVI

Diplomski rad

Voditelji rada:
dr. sc. Nina Kamčev,
doc. dr. sc. Rudi Mrazović

Zagreb, kolovoz, 2023.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

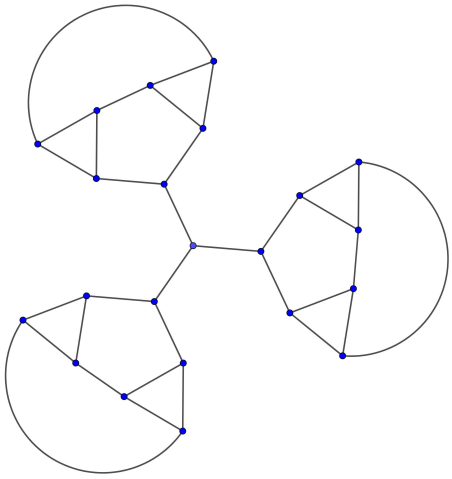
1. _____
2. _____
3. _____

Prije svega želio bih zahvaliti mentorici dr. sc. Nini Kamčev. Njeno znanje, strpljenje i mnogi savjeti uvelike su obogatili kvaliteti ovog rada. Također, izražavam zahvalnost doc. dr. sc. Rudiju Mrazoviću na preciznom uočavanju detalja čiji su ispravci pridonijeli finalnom oblikovanju rada. Neizmjerno sam zahvalan obitelji, prijateljima i djevojci za podršku tijekom studija. Dodatno, želim istaknuti da sam svoj interes prema matematici i njezinim izazovima prepoznao zahvaljujući profesorici Zlati Hržini iz srednje škole.

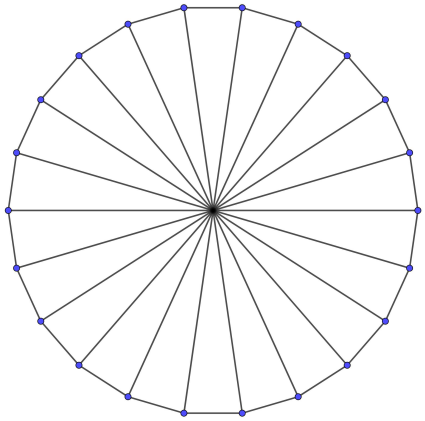
Sadržaj

Uvod

Promotrimo situaciju u kojoj grafom predstavljamo računala povezana „vezama”, odnosno mrežnim kablovima te neka poruke prolaze jednaku količinu vremena kroz svaku vezu. Dva računala mogu direktno komunicirati ako i samo samo ako su povezana vezom, u suprotnom se poruka od početnog računala šalje putem kroz mrežu do konačnog računala. Što ako mreža treba sadržavati velik broj računala koja međusobno šalju i primaju poruke, a pritom nam je postavljanje veza izuzetno skupo, kakvim grafom je najbolje opisati mrežu?
U situaciji kada u mreži imamo 22 računala te je svako računalo direktnom vezom povezano s točno 3 druga računala, koji je od iduća dva grafa arhitekture mreže „bolji”?



Graf X



Graf Y

Iako još ne znamo precizno po čemu bi jedna mreža bila „bolja” od druge, proučimo svojstva spomenutih grafova i pokušajmo zaključiti koja svojstva bi „dobra” mreža trebala zadovoljavati.
Vidimo da u oba grafa možemo iz jednog vrha doći u proizvoljan drugi vrh u najviše

šest koraka, stoga se čini da obje mreže jednako brzo provode informacije. Uočavamo i da uklanjanjem neke od veza središnjeg vrha grafa X, pripadni graf postaje nepovezan. Usprkos tome, uklanjanjem bilo koja dva brida grafa Y, on i dalje ostaje povezan. Dolazimo do zaključka da bi najveća udaljenost dvaju čvorova u grafu i minimalan broj veza koje bismo morali ukloniti da graf ostane nepovezan kandidati za svojstva „dobre" mreže.
Prethodna dva svojstva možemo pokušati objediniti tako što zahtijevamo od našeg grafa da je svaki podskup njegovih vrhova povezan s velikim brojem vrhova komplementa tog podskupa. Osim toga, nema nam previše smisla promatrati podskupove s više od pola ukupnog broja vrhova jer nam tada ponestaje vrhova s kojima bi oni mogli biti povezani. S obzirom na to da prethodno spomenutu, neformalnu definiciju **ekspander grafova**, graf Y ipak nije tako dobro rješenje našeg problema. Da bismo se uvjerili u to, uzmimo bilo kojih 5 uzastopnih vrhova grafa Y te njihovih 5 dijametralnih susjeda. Sada promatranih 10 vrhova ima samo 4 susjeda među vrhovima u ostatku grafa.
Slijedi formalna definicija ekspander grafa.

Definicija. *U grafu $G = (V, E)$ za $W \subseteq V$ definiramo **skup susjeda** skupa W kao*

$$N(W) := \{u \in V \mid \exists v \in W : (u, v) \in E\}. \tag{1}$$

*Za graf $G = (V, E)$ kažemo da je (n, d, ϵ)-**ekspander** ako ima n vrhova, najveći stupanj nekog vrha u grafu je d te $\epsilon > 0$ i za svaki $W \subseteq V$ takav da je $|W| \leq \frac{n}{2}$ vrijedi*

$$|N(W) \setminus W| \geq \epsilon |W|. \tag{2}$$

Kao što smo vidjeli iz primjera, ekspander grafovi čine se kao izuzetno zanimljiva skupina grafova. Ne samo to, nego bi bilo vrlo korisno kada bismo poznavali familije takvih grafova u kojima je svaki vrh grafa ima neki fiksan, mali broj veza, dok broj vrhova može biti proizvoljno velik. Postojanje takvih grafova dokazao je prvi puta Pinsker u [17], tada je vjerojatnosnom metodom dokazao „samo" njihovu egzistenciju. Problem eksplicitnih konstrukcija takvih „korisnih" grafova i dan danas nije u potpunosti riješen. Primjer ekspandera je graf čiji skup čvorova čine ostaci pri dijeljenju s p osim 0, za neki prost broj $p > 3$, a dva su ostatka $x, y \in F_p \setminus \{0\}$ povezani ako i samo ako je $x \equiv y + 1 \mod p$ ili $y \equiv x + 1 \mod p$ ili $xy \equiv 1 \mod p$. Prethodnu činjenicu dokazao je Alexander Lubotzky kao Teorem 4.4.2 svoje knjige „Discrete groups, expanding graphs and invariant measures"([12]). Već sada počinjemo uviđati ekspandere kao poveznicu kombinatorike, računarstva, vjerojatnosti, teorije brojeva pa i teorije grupa. Upravo zbog toga su i nama glavna tema ovog rada. Osim ekspandera, proučit ćemo slučajne **Cayleyeve grafove** i njihova svojstva te pokazati da su oni „najčešće" i ekspanderi. Navedimo njihovu definiciju.

Definicija. *Neka je G konačna grupa i $S \subset G$. Za G i S definiramo Cayleyev graf $Cay(G, S) = (V, E)$ gdje je skup vrhova V jednak G, a za skup bridova vrijedi*

$$E = \{(a, b) \mid a, b \in V,\ \exists s \in S, a = sb\}.$$

Kako smo već napomenuli, konstrukcija ekspandera je kompleksan problem, zato će naš cilj biti čitatelju iznijeti i dokazati **Alon-Roichmanov teorem**. Taj teorem će dat će nam veliku sigurnost u činjenicu da su odgovarajući slučajni Cayleyevi grafovi ujedno i ekspanderi, odnosno pružit će nam alat za konstrukciju ekspandera.

Teorem ([Alon-Roichman [3]). *Za svaki* $\epsilon > 0$ *postoji* $k = k(D) = \left(\frac{2}{\epsilon^2} + o(1)\right) \log D$ *takva da za sve konačne grupe G vrijedi*

$$\mathbf{E}\left[\frac{\lambda(Cay(G,S))}{2k}\right] \leq \epsilon.$$

Pri čemu su $s_1, ..., s_k$ *nezavisne slučajne varijable, uniformno distribuirane na G, a S je skup* $\{s_1, ..., s_k\}$ *i* $D = \sum_{\rho \in \hat{G}} d_\rho$.

U prvom poglavlju rada prisjetit ćemo se glavnih pojmova teorije grafova te uvesti i dokazati sve potrebne tvrdnje za razumijevanje daljnjih rezultata. Kroz drugo poglavlje bavit ćemo se teorijom reprezentacije, granom matematike koja povezuje linearnu algebru i teoriju grupa, a čiji rezultati omogućuju kratak dokaz glavnog teorema u radu. Iduće poglavlje posvetit ćemo samo dokazu Alon-Roichmanovog teorema i glavne ograde korištene u njemu dok ćemo u zadnjem poglavlju proučiti slučajnu šetnju i pomoću slučajne šetnje pokazati osnovnu primjenu ekspander grafova.

Poglavlje 1

Teorija grafova

1.1 Matrica susjedstva

U ovom dijelu iznosimo neke poznate i korisne tvrdnje iz teorije grafova. Započnimo s osnovnim definicijama.

Definicija 1.1.1. *1. **Graf** je uređeni par (V, E), gdje je V skup elemenata koji nazivamo vrhovi i E skup bridova. Ovisno o skupu E, razlikujemo dvije vrste grafova:*

- *Ako je $E \subseteq V \times V$, tada graf nazivamo **usmjerenim**.*
- *Kada je $E \subseteq \{\{u, v\} : u, v \in V\}$, kažemo da je graf **neusmjeren**.*

U oba slučaja ćemo za brid koji povezuje $u, v \in V$ pisati $(u, v) \in E$, gdje u slučaju usmjerenog grafa kažemo da brid izlazi iz u i ulazi u v.

2. *Za neusmjeren graf $G = (V, E)$ kažemo da je **jednostavan** ukoliko E ne sadrži bridove oblika (v, v) za $v \in V$.*

3. *U grafu $G = (V, E)$ definiramo stupanj vrha $v \in V$ kao broj bridova koji sadrži v te ga označavamo sa $deg(v)$.*

4. *Za graf G definiramo **matricu susjedstva** $A(G) = [a_{i,j}] \in M_n(\mathbb{R})$ kao*

$$a_{i,j} = \begin{cases} 1, & \text{ako je } (i, j) \in E \\ 0, & \text{ako } (i, j \notin E. \end{cases}$$

5. *Ako je dan graf $G = (V, E)$, **šetnja** u grafu je niz vrhova u kojemu je svaki vrh (osim prvog) susjedan sa svojim prethodnikom u nizu.*

6. ***Ciklus*** *je niz vrhova u kojemu su svaka dva uzastopna vrha povezana i svi osim prvog i zadnjeg vrha su različiti.*

7. ***Put*** *je šetnja koja ne sadrži ciklus kao podskup.*

8. *U grafu $G = (V, E)$ pod pojmom* ***udaljenost*** *vrhova $u, v \in V$ mislimo na broj bridova na najkraćem putu između u i v, ako takav put postoji, a u suprotnom je njihova udaljenost beskonačno. Udaljenost između dva vrha u i v označavamo kao $d(u, v)$.*

9. ***Promjer*** *grafa G je broj bridova najduljeg puta u grafu,đ. Označavamo ga sa $diam(G)$.*

Ako nije rečeno drugačije, kada u radu kažemo da nam je dan graf G sa n vrhova, pretpostavljamo da je on jednostavan te $V = \{1, ..., n\}$.
Matrica A u slučaju neusmjerenog grafa uvijek je simetrična, iz osnova linearne algebre sada slijedi da postoji ortogonalna baza $v_1, ..., v_n$ prostora $\mathbb{R}^n$ te pripadne svojstvene vrijednosti $\lambda_1, ..., \lambda_n$, takve da vrijedi $Av_i = \lambda_i v_i$ za $i = 1, ..., n$. Ako nije drugačije rečeno, u ostatku rada pretpostavljat ćemo da su prethodno spomenute svojstvene vrijednosti poredane padajući prema apsolutnoj vrijednosti.
Primijetimo da za A vrijedi

$$A\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}deg(1)\\ \vdots \\ deg(n)\end{pmatrix}$$

pa u slučaju d-regularnog grafa vrijedi da je d jedna od svojstvenih vrijednosti matrice susjedstva.
Promotrimo sada općenitu ogradu za najveću svojstvenu vrijednost matrice susjedstva.

Propozicija 1.1.2. *Neka je dan graf G s pripadnom matricom susjedstva $A = [a_{i,j}]$ i neka je λ_1 njegova svojstvena vrijednost s najvećom apsolutnom vrijednošću. Ako su $deg(i)$, deg_{max} i deg_{avg} redom, stupanj vrha i, maksimalni stupanj vrha u grafu, prosječni stupanj vrha u grafu, tada vrijedi $deg_{avg} \leq \lambda_1 \leq deg_{max}$.*

Dokaz. Neka je v_1 svojstveni vektor koji pripada λ_1 i $v_1(i)$ njegova koordinata s najvećom apsolutnom vrijednošću. Bez smanjenja općenitosti pretpostavimo da ona nije 0. Za $j \in V$ označimo sa e_j j-ti vektor standardne baze prostora $\mathbb{R}^n$. Neka je $e = e_1 + ... + e_n$. Sada vrijedi

$$\lambda_1 = \frac{Av_1e_i}{v_1^Te_i} = \frac{\sum\limits_{j:(i,j)\in E} v_1(j)}{v_1(i)} \leq deg(i) \leq deg_{max}.$$

Za prvu nejednakost iskoristimo Rayleighev kvocijent koji nam za najveću svojstvenu vrijednost simetrične matrice daje prvu jednakost

$$\lambda_1 = \max_{x \in \mathbb{R}^n} \frac{x^T A x}{x^T x} \geq \frac{e^T A e}{e^T e} = \frac{\sum\limits_{i,j \in V} a_{i,j}}{n} = deg_{avg}.$$

□

Sada dobivamo i posebnu tvrdnju u slučaju da je početni graf regularan.

Korolar 1.1.3. *Ako je $G = (V, E)$ d-regularan graf s matricom susjedstva A, tada vrijedi $\lambda_1 = d$.*

Dokaz. Po prethodno dokazanoj propoziciji imamo

$$d = deg_{avg} \leq \lambda_1 \leq deg_{max} = d.$$

□

Dokažimo rezultat koji povezuje udaljenost dvaju vrha i minimalni polinom matrice susjedstva.

Lema 1.1.4. *Ako je A matrica susjedstva grafa $G = (V, E)$ te za neka dva vrha $i, j \in V$ vrijedi $d(i, j) = m$, tada je minimalni polinom matrice susjedstva barem stupnja $m + 1$.*

Dokaz. Pretpostavimo suprotno, tada postoji polinom $p(A) = \sum\limits_{k=1}^{m} c_k A^k$ stupnja m, koji poništava A. Označimo sa 0 nuloperator, tada vrijedi

$$p(A) = \sum_{k=1}^{m} c_k A^k = 0.$$

S obzirom na to da matrica A^k na mjestu i, j ima element jednak 0 za $k = 0, 1, ..., m - 1$, a u slučaju $k = m$ taj je element jednak m, slijedi $c_m = 0$.
Analogno iz jednadžbe $A^i p(A) = 0$ za svaki $i = 1, ..., m$ zaključujemo $c_{m-i} = 0$. □

Iz navedene Leme slijedi sljedeća tvrdnja o minimalnom polinomu matrice susjedstva.

Korolar 1.1.5. *Ako je A matrica susjedstva grafa $G = (V, E)$, tada je minimalni polinom matrice susjedstva barem stupnja $diam(G) + 1$.*

Dokaz. Primjenom prethodne Leme na vrhove i i j, takve da $d(i, j) = diam(G)$ slijedi tvrdnja. □

Za graf $G = (V, E)$ uvedimo još i oznaku $\lambda(G) = \max\{|\lambda_2|, ..., |\lambda_n|\}$. Ako je iz konteksta jasno o kojem grafu se radi, pisat ćemo jednostavno λ.

Definicija 1.1.6. *Za graf $G = (V, E)$ i $S, T \subseteq V$ definiramo **skup mostova** između S i T kao $E(S, T) := \{(u, v) \in E \mid u \in S, v \in T\}$.*

Lema 1.1.7. *Neka je $G = (V, E)$ d-regularan graf s matricom susjedstva A i $\lambda(G) = \lambda$. Za sve $S, T \subseteq V$ vrijedi*

$$\left||E(S,T)| - \frac{d|S||T|}{n}\right| \leq \lambda\sqrt{|S||T|}.$$

Ukoliko S i T čine particiju skupa V, tada vrijedi i

$$E(S,T) \geq \frac{d-\lambda}{n}|S||T|.$$

Dokaz. Neka su e_S i e_T karakteristični vektori skupova S i T (e_S ima 1 na i-tom mjestu ako je i-ti vrh u S, a u suprotnom ima 0 na i-tom mjestu).
S obzirom na to da $v_1, ..., v_n$ čine ortonormiranu bazu prostora $\mathbb{R}^n$, pri čemu je $v_1 = \frac{e_1+...+e_n}{\sqrt{n}}$, označimo sa $e_S = \sum_{i=1}^{n} \alpha_i v_i$ i $e_T = \sum_{i=1}^{n} \beta_i v_i$ prikaze naših karakterističnih vektora u danoj bazi, sada vrijedi

$$|E(S,T)| = 1_S A 1_T = (\sum_{i=1}^{n} \alpha_i v_i) A (\sum_{i=1}^{n} \beta_i v_i) = \sum_{i=1}^{n} \alpha_i \beta_i \lambda_i.$$

Dakle, zbog $\lambda_1 = d$, $\alpha_1 = \langle 1_S, \frac{e_1+...+e_n}{\sqrt{n}}\rangle = \frac{|S|}{\sqrt{n}}$ i $\beta_1 = \langle 1_T, \frac{e_1+...+e_n}{\sqrt{n}}\rangle = \frac{|T|}{\sqrt{n}}$ slijedi

$$|E(S,T)| = \frac{d|S||T|}{n} + \sum_{i=2}^{n} \alpha_i \beta_i \lambda_i. \tag{1.1}$$

Odnosno

$$\left||E(S,T)| - \frac{d|S||T|}{n}\right| = \left|\sum_{i=2}^{n} \alpha_i \beta_i \lambda_i\right| \leq \lambda \sum_{i=2}^{n} |\alpha_i \beta_i|.$$

Zbog Cauchy-Schwarzove nejednakosti dobivamo

$$\left||E(S,T)| - \frac{d|S||T|}{n}\right| \leq \lambda\sqrt{||\alpha||_2 ||\beta||_2} = \lambda\sqrt{|S||T|}$$

pa smo dokazali prvu nejednakost.
Ako S i T čine particiju od V, tada vrijedi $1_T = \sqrt{n} \cdot v_1 - 1_S$ iz čega slijedi

$$\beta_i = -\alpha_i \text{ za } i = 2, ..., n.$$

Primijetimo još i

$$\sum_{i=2}^{n} \alpha_i^2 = \|1_S\| - \alpha_1^2 = |S|^2 - \frac{|S|^2}{n} = \frac{|S||T|}{n}$$

Vratimo se sada na (1.1), koristeći prethodne tvrdnje dobiva se

$$\begin{aligned} |E(S,T)| &= \frac{d|S||T|}{n} + \sum_{i=2}^{n} \alpha_i \beta_i \lambda_i \\ &= \frac{d|S||T|}{n} - \sum_{i=2}^{n} \alpha_i^2 \lambda_i \\ &\geq \frac{d|S||T|}{n} - \lambda \sum_{i=2}^{n} \alpha_i^2 \\ &= \frac{d|S||T|}{n} - \lambda \frac{|S||T|}{n}. \end{aligned}$$

□

Iz prethodne propozicije možemo vidjeti da stvaran broj bridova između dva proizvoljna podskupa vrhova, tj. $E(S,T)$, nije daleko od očekivanog broja bridova među njima u slučajnom d-regularnom grafu, odnosno $\frac{d|S||T|}{n}$. To možemo protumačiti kao jednoliku raspodjelu bridova u d-regularnom grafu.

Definicija 1.1.8. *Ako je $G = (V,E)$ i $S \subseteq V$, kažemo da je S nezavisan, ako vrijedi*

$$E(S,S) = \emptyset.$$

Lema 1.1.7 povlači da grafovi s malom drugom najvećom svojstvenom vrijednosti matrice susjedstva nemaju velike skupove s relativno malim ili velikim brojem bridova. Navedimo tu tvrdnju i kao našu iduću propoziciju.

Korolar 1.1.9. *Neka $G = (V,E)$ d-regularan graf sa n vrhova i $\lambda(G) = \lambda$, tada svaki nezavisan skup u grafu ima najviše $\frac{\lambda}{d}n$ elemenata.*

Dokaz. Neka je S neki nezavisan skup, uzimanjem $T = S$ u Lemi 1.1.7 slijedi tvrdnja. □

Prethodna nejednakost govori nam kako mala druga svojstvena vrijednost grafa uzrokuje homogeniju raspodjelu bridova u grafu G. Međutim, idući rezultat govori nam kako druga svojstvena vrijednost ne može biti proizvoljno mala.

Propozicija 1.1.10. *Neka je $G = (V,E)$ d-regularan graf s matricom susjedstva A i $\lambda(G) = \lambda$, tada vrijedi*

$$\lambda \geq \sqrt{\frac{(n-d)d}{(n-1)}}.$$

Dokaz. Primjenom činjenice da je $\mathrm{Tr}(A)$ jednak sumi svojstvenih vrijednosti matrice A za matricu A^2 i toga da je $\mathrm{Tr}(A^2)$ jednak sumi elemenata na dijagonali, odnosno broju ciklusa duljine 2 u grafu, dobivamo

$$\begin{aligned} nd = \mathrm{Tr}(A^2) &= \sum_{i=1}^{n} \lambda_i^2 \\ \implies nd &\leq d^2 + (n-1)\lambda^2 \\ \implies \lambda &\geq \sqrt{\frac{(n-d)d}{(n-1)}}. \end{aligned}$$

□

Vidimo kako za situacije u kojima je $d << n$, donja ograda na $\lambda(G)$ približno je jednaka $\sqrt{d}$.

Sljedeći teorem iskazujemo bez dokaza.

Teorem 1.1.11. *[16] Neka je G d-regularan graf sa n vrhova i $diam(G) \geq 4$, tada vrijedi*

$$\lambda_2 \geq 2\sqrt{d-1} - \frac{2\sqrt{d-1}-1}{\left\lfloor \frac{diam(G)}{2} \right\rfloor}.$$

Iz prethodnog teorema vidimo da nužno slijedi $\lambda(G) \geq 2\sqrt{d-1} - \frac{2\sqrt{d-1}-1}{\left\lfloor \frac{diam(G)}{2} \right\rfloor}$. Motivirani navedenom ogradom, definiramo Ramanujanove grafove.

Definicija 1.1.12. *Neka je $G = (V, E)$ d-regularan graf, takav da za $\lambda(G)$ vrijedi*

$$\lambda(G) \leq 2\sqrt{d-1}.$$

*Takav graf zovemo **Ramanujanov graf**.*

Ramanujanovi grafovi interesantni su jer njihova po apsolutnoj vrijednosti druga najveća svojstvena vrijednost ima „skoro" minimalnu vrijednosti. Prvu konstrukciju Ramanujanovih grafova dali su A. Lubotzky, R. Phillips i P. Sarnak ([13]).
Na kraju, u radu sa d-regularnim grafovima često ćemo koristiti u dokazima „skaliranu" verziju matrice susjedstva.

Definicija 1.1.13. *Neka je dan d-regularan graf G, tada definiramo **normaliziranu matricu susjedstva** kao*

$$N(G) = \frac{1}{d}A \in M_n(\mathbb{R}).$$

Uočimo, ako su $\lambda_1, ..., \lambda_n$ svojstvene vrijednosti matrice A poredane padajući po apsolutnoj vrijednosti, tada su svojstvene vrijednosti matrice N jednake $\frac{\lambda_1}{d}, ..., \frac{\lambda_n}{d}$ te su one također poredane padajući.

1.2 Ekspander grafovi

Kao što smo najavili u uvodu, od interesa su nam posebni, „dobro povezani" grafovi koje nazivamo **ekspanderi**. Postoji nekoliko međusobno sličnih ili ekvivalentnih definicija ekspandera, no bavit ćemo se onom najčešćom.

Definicija 1.2.1. *U grafu $G = (V, E)$ za $W \subseteq V$ definiramo **skup susjeda** skupa W kao*

$$N(W) := \{u \in V \mid \exists v \in W : (u, v) \in E\}. \tag{1.2}$$

Definicija 1.2.2. *Za graf $G = (V, E)$ kažemo da je (n, d, ϵ)-**ekspander** ako ima n vrhova, najveći stupanj nekog vrha u grafu je d te $\epsilon > 0$ i za svaki $W \subseteq V$ takav da je $|W| \leq \frac{n}{2}$ vrijedi*

$$|N(W) \setminus W| \geq \epsilon |W|. \tag{1.3}$$

*Broj ϵ zovemo **koeficijent ekspanzije** grafa G.*

Sljedeća propozicija daje nam vezu između spektra i ekspanzije grafa.

Propozicija 1.2.3. *Za d-regularan graf $G = (V, E)$ sa n vrhova, matricom susjedstva A i svojstvenim vrijednostima $\lambda_1, ..., \lambda_n$ vrijedi da je (n, d, c)-**ekspander**, pri čemu je $c = \frac{d-\lambda}{2d}$ i $\lambda(G) = \lambda$.*

Dokaz. Neka je W skup sa najviše $\frac{n}{2}$ vrhova, prema Lemi 1.1.7 slijedi

$$E(W, V \setminus W) \geq \frac{(d-\lambda)|W|(n-|W|)}{2} \geq \frac{d-\lambda}{2}|W|.$$

S obzirom na to da je svaki vrh u komplementu od W sadržan u najviše na najviše d bridova iz $E(W, V \setminus W)$, mora vrijediti

$$|N(W) \setminus W| \geq \frac{d-\lambda}{2d}|W|.$$

□

Iz prethodne propozicije možemo vidjeti da su grafovi za koje je druga svojstvena vrijednost po apsolutnoj vrijednosti mala, dobri ekspanderi. Promotrimo nekoliko primjera ekspandera.

Primjer 1.2.4. *Najosnovniji primjer ekspander grafa je potpun graf sa n vrhova. Naime, budući da je svaki vrh povezan sa svim ostalim vrhovima u grafu, ako je S proizvoljan podskup vrhova grafa s najviše $\frac{n}{2}$ vrhova, tada imamo*

$$|N(S) \setminus S| = n - |S| \geq \frac{n}{2} \geq |S|.$$

Slijedi da je graf $(n, n-1, 1)$-ekspander.

Propozicija 1.2.5. *Neka je graf G (n, d, ϵ)-ekspander te $\epsilon > 0$, tada je G povezan.*

Dokaz. Pretpostavimo suprotno. Tada postoji povezana komponenta sa skupom vrhova S, za koji vrijedi $|S| \leq \frac{n}{2}$.
Jasno je da tada vrijedi $N(S) \setminus S = \emptyset$ pa G ne može biti ekspander. $\Rightarrow\Leftarrow$ □

Od posebnog interesa su nam „rijetki ekspanderi", oni malog maksimalnog stupnja, a velikog broja vrhova. Najčešće promatramo d-regularne ekspandere, i to familije d-regularnih grafova $\{G_i\}_{i\in\mathbb{N}}$ koji su (n_i, d, ϵ) ekspanderi, gdje su d i ϵ fiksni, a n_i teži u beskonačnost.
Prirodno je pitati se postoje li uopće takve familije. Odgovor na to pitanje dugo nije bio poznat. Njihovu egzistenciju dokazao je Mark Semenovich Pinsker tek 1973. ([17]) godine. Tvrdnja je dokazana modernim pristupom koji se počeo koristiti u 20. stoljeću, većinom u problemima koji nisu „opipljivi", tzv. vjerojatnosnom metodom. Velik dio dobro poznatih dokaza vjerojatnosnom metodom djelo su matematičara Paula Erdősa, iako on nije bio prvi koji ju je koristio.

Teorem 1.2.6. *[21] Za svaki $0 < \epsilon < 1$ i dovoljno velik $d \in \mathbb{N}$ za svaki paran $n \in \mathbb{N}$ postoji d-regularan graf $G = (V, E)$, u kojem dozvoljavamo višestruke bridove i bridove oblika (v, v) za $v \in V$, koji je (n, d, ϵ) ekspander.*

Dokaz. Pokazat ćemo da za dovoljno velik d, slučajni d-regularni graf sa n vrhova (n paran) (n, d, ϵ) ekspander s pozitivnom vjerojatnošću.
Odaberimo slučajan d-regularan graf sa n vrhova tako da promatramo uniju d savršenih uparivanja koji su skupovi disjunktnih $\frac{n}{2}$ bridova. Kao što smo već rekli, dopustit ćemo višestruke bridove među dva vrha i bridove koji spajaju čvor sa samim sobom.
Za svaki podskup S sa $k \leq \frac{n}{2}$ vrhova i svaki podskup T od $\lfloor \epsilon k \rfloor$ vrhova ograničit ćemo vjerojatnost da je $N(S) \setminus S \subset T$ odnosno $N(S) \subset T \cup S$ za nasumično savršeno uparivanje (to će biti dovoljno jer $\epsilon k \geq \lfloor \epsilon k \rfloor > \lfloor \epsilon k \rfloor - 1$).
Savršeno uparivanje možemo konstruirati tako da odabiremo redom vrhove iz S, te prvi još neupareni vrh uparimo s nasumičnim neuparenim vrhom iz grafa.
Označimo sa E_i događaj da je i-ti vrh iz S povezan s nekim vrhom iz T ili S u proizvoljnom savršenom uparivanju. E_i je sigurno dobro definiran za $i \leq \frac{k}{2}$ jer je moguće da su nakon $\frac{k}{2}$ koraka svi vrhovi iz S upareni međusobno.
Koristeći formulu uvjetne vjerojatnosti i $\lfloor \epsilon k \rfloor \leq \epsilon k$ da vrijedi

$$\mathbf{P}\left(E_1 \cap ... \cap E_{\lfloor \frac{k}{2} \rfloor}\right) = \prod_{i=1}^{\lfloor \frac{k}{2} \rfloor} \mathbf{P}(E_i | E_{i-1} \cap ... \cap E_1) \leq \left(\frac{(1+\epsilon)k}{n}\right)^{k/2}.$$

Uz prethodnu nejednakost i činjenicu da su susjedi od S dobiveni kao rezultat d nezavisnih savršenih sparivanja dobiva se

$$\mathbf{P}(N(S) \subset T \cup S) \leq \mathbf{P}\left(\text{svi susjedi prvih } \lfloor \frac{k}{2} \rfloor \text{ vrhova iz S nalaze se u } S \cup T\right)$$
$$= \left(\mathbf{P}\left(E_1 \cap ... \cap E_{\lfloor \frac{k}{2} \rfloor}\right)\right)^d \leq \left(\frac{(1+\epsilon)k}{n}\right)^{dk/2}.$$

S obzirom na to da skup S možemo odabrati na $\binom{n}{k}$ načina i podskupova veličine $\lfloor \epsilon k \rfloor$ ima $\binom{n}{\lfloor \epsilon k \rfloor}$ pa koristeći poznatu ogradu $\binom{n}{k} \leq \left(\frac{en}{k}\right)^k$, gdje je desna strana rastuća za $k < \frac{n}{2}$, dobivamo da za događaj da skup susjeda nekog skupa veličine k ima manje od ϵk elemenata vrijedi da je njegova vjerojatnost manja ili jednaka

$$\begin{aligned}
\binom{n}{k}\binom{n}{\lfloor \epsilon k \rfloor}\left(\frac{(1+\epsilon)k}{n}\right)^{dk/2} &\leq \left(\frac{en}{k}\right)^k \left(\frac{en}{\epsilon k}\right)^{\epsilon k} \left(\frac{(1+\epsilon)k}{n}\right)^{dk/2} \\
&\leq \left(\frac{en}{k}\right)^k \left(\frac{en}{(1+\epsilon)k}\right)^{(1+\epsilon)k} \left(\frac{(1+\epsilon)k}{n}\right)^{dk/2} \\
&\leq \left(\frac{en}{k}\right)^{(2+\epsilon)k} \left(\frac{(1+\epsilon)k}{n}\right)^{dk/2} \\
&= ((1+\epsilon)e)^{(2+\epsilon)k} \left(\frac{(1+\epsilon)k}{n}\right)^{dk/2-(2+\epsilon)k}.
\end{aligned}$$

Prethodni izraz je za dovoljno velik d strogo manji od 4^{-k} zbog $\frac{(1+\epsilon)k}{n} \leq \frac{(1+\epsilon)}{2} < 1$. Sada zbog subaditivnosti vjerojatnosti dobivamo da je vjerojatnost događaja da naš nasumični graf nije ekspander strogo manja od

$$\sum_{k=1}^{\frac{n}{2}} 4^{-k} < \frac{1}{2}.$$

□

Primijetimo, uvjet parnosti broja n ne može se izbjeći jer inače ne bismo mogli konstruirati savršeno uparivanje grafa sa n vrhova.
Navest ćemo primjer prve eksplicitno definirane familije ekspandera konstantnog stupnja, no bez potvrde da zadovoljava definiciju ekspander. Definirao ju je Margulis ([14]). Pripadni dokaz da su opisani grafovi zaista ekspanderi nije dao eksplicitnu ogradu za konstantu ϵ ekspanzije, kasnije su znanstvenici Gabber i Galil ([5]) koristeći harmonijsku analizu dokazali odgovarajuću ogradu na koeficijent ekspanzije.

Primjer 1.2.7. *Za $m \in N$, neka je G_m 8-regularan graf sa skupom vrhova $V_m = Z_m \times Z_m$. vrh $(x, y) \in V_m$ povežimo sa $(x+y, y)$, $(x-y, y)$, $(x, y+x)$, $(x, y-x)$, $(x+y+1, y)$, $(x-y+1, y)$, $(x, y + x + 1)$ i $(x, y - x + 1)$ gdje su operacije zbrajanja i oduzimanja rađene modulo m.*

Definicija 1.2.8. *Za graf $G = (V, E)$ definiramo **kromatski broj** grafa kao najmanji $k \in \mathbb{N}$ takav da postoji surjekcija $f : V \to \{1, ..., k\}$ za koju vrijedi*

$$(u, v) \in E \implies f(u) \neq f(v).$$

*Općenito, funkciju $f : V \to \{1, ..., k\}$ nazivamo **bojenje** grafa.*

Korolar 1.2.9. *Ako je $G = (V, E)$ d-regularan graf sa n vrhova i $\lambda(G) = \lambda$, tada za kromatski broj $\chi(G)$ vrijedi $\chi(G) \geq \frac{d}{\lambda}$.*

Dokaz. Neka je $f : V \to \{1, ..., m\}$ bojenje našeg grafa, tada je za svaki $k \in \{1, ..., m\}$ skup $f^{-1}(k)$ nezavisan skup našeg grafa pa prema Korolaru 1.1.9 imamo

$$n = \sum_{i=1}^{m} f^{-1}(i) \leq \frac{md}{\lambda} n,$$

odakle slijedi tvrdnja. □

Definicija 1.2.10. *Za funkcije $f, g : A \to R$ pišemo $f(a) = O(g(a))$ ako postoji $c \in \mathbb{R}$ $c > 0$ i za sve $a \in A$ vrijedi $f(a) \leq cg(a)$.*

Teorem 1.2.11. *Za promjer (n, d, ϵ)-grafa vrijedi $diam(G) \leq 2\left\lceil \frac{\log n - 1}{\log(1+\epsilon)} \right\rceil + 1 \leq 3 \log n$, odnosno $diam(G) = O(\log n)$.*

Dokaz. Neka je dan graf $G = (V; E)$ koji je (n, d, ϵ)-ekspander. Za proizvoljan $S \subseteq V$, uvedimo oznaku $N^0(S) = S$ i $N^k(S) = N(N^{k-1})$ za $k \geq 1$.
Sada za $v \in V$ zbog

$$\left|N^k(S)\right| \geq (1 + \epsilon) \left|N^{k-1}(S)\right|$$

laganom indukcijom dobivamo

$$\left|N^k(\{v\})\right| \geq \min\left\{\frac{n}{2}, (1 + \epsilon)^k\right\}.$$

Lako vidimo da ako su $u, v \in V$ i $k = \left\lceil \log_{1+\epsilon} \frac{n}{2} \right\rceil = \left\lceil \frac{\log n - 1}{log(1+\epsilon)} \right\rceil$ tada

$$\left|N^k(\{u\})\right| \geq \frac{n}{2}$$

i

$$\left|N^k(\{v\})\right| \geq \frac{n}{2}.$$

Prema Dirichletovom principu ili su $N^k(u)$ i $N^k(v)$ disjunktni ili zbog svojstva ekspanzije postoji brid koji ih povezuje, stoga je udaljenost između u i v manja ili jednaka

$$2k + 1 = 2\left\lceil \frac{\log n - 1}{log(1+\epsilon)} \right\rceil + 1.$$

Zbog $1 + \epsilon > 0$ i $\lceil x \rceil \leq x + 1$ slijedi

$$2\left\lceil \frac{\log n - 1}{log(1+\epsilon)} \right\rceil + 1 \leq 2\log n + 1 \leq 3\log n$$

□

Budući da smo sada upoznati s osnovnim svojstvima ekspander grafova, promotrimo poznati primjer grafa i utvrdimo zadovoljava li barem neka od svojstva ekspandera.

Primjer 1.2.12. *Neka je C_n ciklički graf sa n vrhova. Već smo dokazali da kod ekspandera očekujemo „male" nezavisne skupove, lako vidimo da u slučaju grafa C_n možemo uzeti svaki drugi vrh ciklusa te tako dobiti nezavisan skup sa $\left\lfloor \frac{n}{2} \right\rfloor$ elemenata.*
Uočimo još da je promjer grafa C_n jednak $\left\lfloor \frac{n+1}{2} \right\rfloor$ pa promjer grafa C_n nije $O(\log n)$.
Pokušajmo odgonetnuti još i svojstvene vrijednosti matrice susjedstva A. Neka je $B = [b_{i,j}]$, pri čemu je

$$b_{i,j} = \begin{cases} 1, & \text{ako je } j = i + 1 \\ 0, & \text{u suprotnom} \end{cases}$$

Jasno je da vrijedi $A = B + B^T$. Neka je sada $\omega = e^{\frac{2\pi i}{n}}$. Direktnom provjerom vidimo kako za $v_k = (1, \omega^k, \omega^{2k}, ..., \omega^{(n-1)k})$ vrijedi $Bv_k = \omega^k v_k$, stoga su svojstvene vrijednosti matrice B jednake $\omega^0, ..., \omega^{n-1}$.
Također možemo provjeriti da vrijedi $B^T v_k = \overline{\omega^k} v_k$. Zaključujemo da su svojstvene vrijednosti matrice A jednake $\omega^0 + \overline{\omega^0}, ..., \omega^{n-1} + \overline{\omega^{n-1}}$.

Za graf G pokazali smo već ogradu na koeficijent ekspanzije grafa s obzirom na $\lambda(G)$. Promotrimo sada i suprotnu situaciju.

Teorem 1.2.13. *[1]*
Ako je G d-regularan graf koji je (n, d, ϵ)-ekspander, tada vrijedi

$$\lambda(G) \leq d - \frac{\epsilon^2}{4 + 2\epsilon^2}.$$

Prije dokaza navedenog teorema, spomenimo tvrdnje i definicije s kojima se nismo još susreli u radu. Bit će nam potrebne u dokazu.

Definicija 1.2.14.

- ***Mreža*** *je usmjeren graf $G = (V, E)$ za koji postoje:*
  - *vrhovi $s \in V$ koji nazivamo **izvor** te $t \in V$ koji nazivamo **ponor**. Oznake s i t za vrhove u nekoj mreži koristit ćemo isključivo kada se radi o izvoru ili ponoru.*
  - *Funkcija $c : E \to [0, \infty)$ koju nazivamo **kapacitet**, te za $(u, v) \in E$ vrijednost kapaciteta brida (u, v) označavamo sa $c(u, v)$.*
- *Za mrežu $G = (V, E)$ s kapacitetom c, funkciju $f : E \to [0, \infty)$ zovemo **tok** mreže, ako zadovoljava*
  - *Za svaki brid $(u, v) \in E$ imamo $f(u, v) \leq c(u, v)$.*
  - *(Kirchhoffovo pravilo) Ako je $v \in V$ te $v \neq s, t$, tada je zadovoljena jednakost*

$$\sum_{u:(u,v)\in E} f(u, v) = \sum_{w:(v,w)\in E} f(v, w).$$

- ***Vrijednost*** *toka f definiramo kao $|f| := \sum_{v:(s,v)\in E} f(s, v)$. Tok koji ima maksimalnu vrijednost nazivamo **maksimalnim tokom**.*
- *Ako je dana mreža $G = (V, E)$, tada uređeni par $C = (S, T)$, gdje S i T čine particiju vrhova grafa te $s \in S$ i $t \in T$, nazivamo **rezom**. Za rez (S, T) definiramo i kapacitet reza $c(S, T) := \sum_{(u,v)\in E} c(u, v)$. Rez (S, T) za koji je $c(S, T)$ najmanji mogući nazivamo **minimalnim rezom**.*

U grafu često nalazimo puno rezova, ali „teško" pronalazimo rezove malog kapaciteta. Idući teorem, koji navodimo bez dokaza, govori nam kako je vrijednost minimalnog reza jednaka vrijednosti maksimalnog toka. Dokaz možemo pronaći u [4], a zasniva se na tzv. Ford-Fulkersonovom algoritmu.

Teorem 1.2.15. *Vrijednost maksimalnog toka u mreži $G = (V, E)$ jednaka je kapacitetu minimalnog reza.*

Sada smo spremni dokazati Teorem 1.2.13.

Dokaz. Za početak uočimo da su svojstvene vrijednosti matrice $Q = dI - A$ jednake $d - \lambda_1, ..., d - \lambda_n$. Također, najveća svojstvena vrijednost matrice susjedstva A, odnosno $\lambda(G)$, odgovara po apsolutnoj vrijednosti najmanjoj svojstvenoj vrijednosti matrice Q. Zato je dovoljno pokazati

$$d - \lambda(G) \geq \frac{\epsilon^2}{4 + 2\epsilon^2}.$$

Stavimo $d - \lambda(G) = \mu$ i neka je $f = (f_1, ..., f_n) \in \mathbb{R}^n$ pripadajući svojstveni vektor matrice Q. Poznato je da su svojstveni prostori matrice Q međusobno ortogonalni pa s obzirom na

to da je 0 svojstvena vrijednost kojoj odgovara vektor sa svim koordinatama jednakim 1, slijedi

$$\sum_{i=1}^{n} f_i = 0.$$

Neka je $V^+ = \{i \in \{1, ..., n\} : \ f_i \geq 0\}$ te $V^- = V \setminus V^+$. Bez smanjenja općenitosti smijemo pretpostaviti $|V^+| \leq \frac{n}{2}$, inače umjesto f možemo promatrati svojstveni vektor $-f$. Definirajmo vektor $g = (g_1, ..., g_n) \in \mathbb{R}^n$ tako da vrijedi

$$g_i = \begin{cases} f_i, \text{ ako je } i \in V^+ \\ 0, \text{ inače} \end{cases}$$

Sada imamo

$$\begin{aligned} \frac{\sum\limits_{i \in V^+} (Qf)_i f_i}{\sum\limits_{i \in V^+} f_i^2} &= \frac{\sum\limits_{i \in V^+} ((dI - A)f)_i f_i}{\sum\limits_{i \in V^+} f_i^2} \\ &= \frac{\sum\limits_{i \in V^+} (d - \lambda(G)) f_i f_i}{\sum\limits_{i \in V^+} f_i^2} \\ &= \mu. \end{aligned}$$

Zbog definicije Q vrijedi

$$\begin{aligned} \sum_{i \in V^+} (Qf)_i f_i &= \sum_{i \in V^+} (deg(i) f_i^2 - \sum_{j:(i,j) \in E} f_i f_j) \\ &= \sum_{(i,j) \in E(V^+, V^+)} (f_i - f_j)^2 + \sum_{(i,j) \in E(V^+, V^-)} f_i (f_i - f_j) \\ &\geq \sum_{(i,j) \in E} (g_i - g_j)^2. \end{aligned}$$

Očito je

$$\sum_{i \in V^+} f_i^2 = \sum_{i \in V^+} g_i^2 = \sum_{i \in V} g_i^2$$

pa

$$\mu \geq \frac{\sum\limits_{(i,j) \in E} (g_i - g_j)^2}{\sum\limits_{i \in V} g_i^2} \qquad (*)$$

Kako bismo dokazali potrebnu ogradu, konstruirat ćemo prikladnu mrežu te koristiti činjenicu da je graf ekspander i Teorem 1.2.15. Promotrimo mrežu s vrhovima $\{s, t\} \cup X \cup Y$, gdje je $X = V^+$, $Y = V$, pritom razlikujemo vrhove $x \in X$ te $y \in Y \cap V^+$. Definirajmo skup bridova E_1 i kapacitet c kao:

1. Ako je $u \in X$, tada $(s,u) \in E_1$ i stavimo $c(s,u) = 1+\epsilon$.

2. Za sve $u \in X$ i $v \in Y$ neka je $(u,v) \in E_1$ i $c(u,v) = 1$ ako $(u,v) \in E$ ili $u = v$, a 0 inače.

3. Za svaki $v \in Y$, neka je $(v,t) \in E_1$ i $c(v,t) = 1$.

Tvrdimo da je vrijednost minimalnog reza jednaka $(1+\epsilon)|V^+|$. Uzevši rez $(s, \{t\} \cup X \cup Y)$ vidimo da je njegova vrijednost $(1+\epsilon)|V^+|$.
Neka je $C = (S,T)$ neki drugi rez, stavimo $U = \{u \in X : \ (s,u) \notin E(S,T)\}$. Iz definicije mreže i činjenice da je G ekspander, slijedi da u mreži imamo $N(U) \geq (1+\epsilon)|U|$. Za svaki $v \in N(U)$, mora postojati barem jedan $u \in S$ takav je $(u,v) \in E(S,T)$, budući da svaki takav brid ima kapacitet 1, vrijedi

$$c(S,T) \geq (1+\epsilon)|X \setminus U| + |N(U)| \geq (1+\epsilon)|V^+|,$$

pa je vrijednost minimalnog reza zaista $(1+\epsilon)|V^+|$. Prema Teoremu 1.2.15 postoji tok $h : E_1 \to [0,\infty)$ takav da:

1. Za sve $(i,j) \in E$ je $0 \leq h(i,j) \leq 1$.

2. Ako $i \in X$, tada je $\sum_{j:(i,j)\in E} h(i,j) = 1+\epsilon$, a 0 u suprotnom.

3. $\sum_{i:(i,j)\in E} h(i,j) \leq 1$ za $j \in Y$.

Uvjerimo se da prethodna svojstva zaista vrijede:

1. S obzirom na to da za $(i,j) \in E$ vrijedi $c(i,j) = 1$, po definiciji toka mora vrijediti i $0 \leq h(i,j) \leq 1$.

2. Za $i \in Y$ nemamo bridova $(i,j) \in E_1$ pa je suma trivijalno jednaka 0. Zbog maksimalnosti toka i $c(s,i) = 1+\epsilon$ za $i \in X$ mora vrijediti

$$(1+\epsilon)|V^+| = |h| = \sum_{(s,i):i\in X} h(s,i) \leq \sum_{(s,i):i\in X} (1+\epsilon) = (1+\epsilon)|V^+|.$$

   Zaključujemo da je $h(s,i) = 1+\epsilon$ za $i \in X$, pa je tražena jednakost zadovoljena po Kirchhoffovom pravilu iz definicije toka.

3. Za $j \in Y$ vrijedi $c(j,t) = 1$ pa po Kirchhoffovom pravilu slijedi tvrdnja.

Iz prethodnih svojstava toka h i A-G nejednakosti dobiva se

$$\begin{aligned}\sum_{(i,j)\in E} h^2(i,j)^2(g_i+g_j)^2 &\leq 2\sum_{(i,j)\in E} h^2(i,j)(g_i^2+g_j^2)\\ &= 2\sum_{i\in V}\left(\sum_{i:(i,j)\in E} h^2(i,j)+\sum_{j:(j,i)\in E} h^2(j,i)\right)\\ &\leq (4+2\epsilon^2)\sum_{i\in V} g_i^2\end{aligned}$$

i

$$\begin{aligned}\sum_{(i,j)\in E} h^2(i,j)^2(g_i^2-g_j^2) &= \sum_{i\in V}\left(\sum_{i:(i,j)\in E} h^2(i,j)-\sum_{j:(j,i)\in E} h^2(j,i)\right)\\ &\leq \epsilon\sum_{i\in V} g_i^2.\end{aligned}$$

Konačno, koristeći (*), prethodne dvije tvrdnje te Cauchy-Schwarzovu nejednakost, slijedi

$$\begin{aligned}\mu &\geq \frac{\sum_{(i,j)\in E}(g_i-g_j)^2}{\sum_{i\in V} g_i^2}\\ &= \frac{\sum_{(i,j)\in E}(g_i-g_j)^2\cdot\sum_{(i,j)\in E} h^2(i,j)^2(g_i+g_j)^2}{\sum_{i\in V} g_i^2\cdot\sum_{(i,j)\in E} h^2(i,j)^2(g_i+g_j)^2}\\ &\geq \frac{\left(\sum_{(i,j)\in E} h(i,j)\left|g_i^2-g_j^2\right|\right)^2}{(4+2\epsilon^2)\left(\sum_{i\in V} g_i^2\right)^2}\\ &\geq \frac{1}{4+2\epsilon^2}\cdot\left(\frac{\sum_{(i,j)\in E}(h(i,j)(g_i^2-g_j^2))}{\sum_{i\in V} g_i^2}\right)^2\\ &\geq \frac{\epsilon^2}{4+2\epsilon^2}\end{aligned}$$

□

1.3 Cayleyevi grafovi

Nakon što smo se upoznali s općenitim grafovima te ekspanderima, promotrit ćemo još jednu vrstu grafova. Pokazat će se da su oni jedan od ključnih alata koji nam omogućavaju pristup ekspanderima.

Definicija 1.3.1. *Neka je G konačna grupa i $S \subset G$. Za G i S definiramo Cayleyev graf $Cay(G, S) = (V, E)$ gdje je skup vrhova V jednak G, a za skup bridova vrijedi*

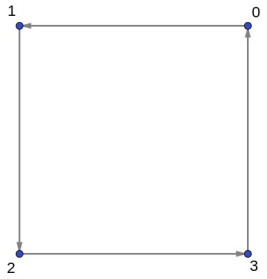
$$E = \{(a, b) \mid a, b \in V,\ \exists s \in S, a = sb\}.$$

Svaki graf X koji je izomorfan sa $Cay(G, S)$ također nazivamo Cayleyevim grafom.

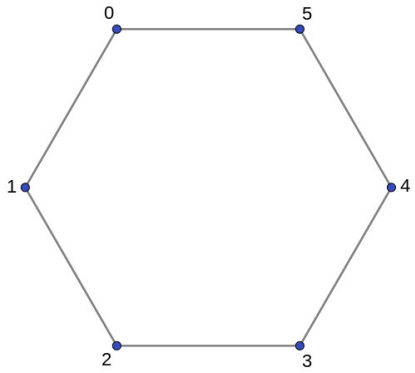
Iz defincije vidimo da je Cayley graf zapravo usmjeren graf, no ukoliko $s \in S \implies s^{-1} \in S$, tada je $Cay(G, S)$ neusmjeren. Definirajmo službeno i takve skupove.

Definicija 1.3.2. *Ako je dana grupa G i $S \subseteq G$ podskup elemenata grupe, kažemo da je S simetričan ukoliko $s \in S$ povlači $s^{-1} \in S$.*

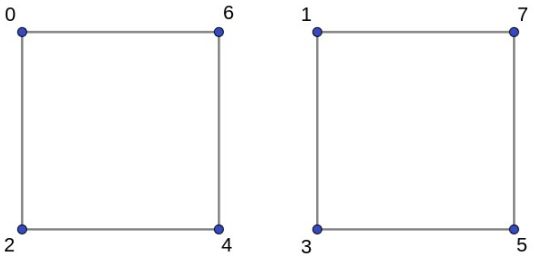
Primjer 1.3.3. *Neka je $G = Z_4$ i $S = \{1\}$, tada $Cay(G, S)$ izgleda kao na slici.*



Primjer 1.3.4. *Za $G = Z_6$ i $S = \{1, 5\}$, $Cay(G, S)$ možemo prikazati ovako.*



Primjer 1.3.5. *Ako je $G = Z_8$ i $S = \{2, 6\}$, tada $Cay(G, S)$ ima dvije komponente povezanosti.*



Najjednostavnije pitanje o Cayleyevim grafovima koje si možemo postaviti je kada su oni nužno povezani.

Lema 1.3.6. *Neka je H podgrupa od G generirana simetričnim skupom S, gdje je $S \subseteq G \setminus \{e\}$. Dva vrha x i y grafa $Cay(G, S)$, nalaze se u istoj komponenti povezanosti tog grafa ako i samo ako vrijedi $xH = yH$.*

Dokaz. $\Longrightarrow$
Pretpostavimo da su x i y u istoj komponenti G_1 grafa $Cay(G, S)$. U tom slučaju mora postojati barem jedan put iz x u y.
Označimo vrhove na tom putu sa $x = x_1, x_2, ..., x_n = y$. Zbog definicije grafa slijedi $x_{k+1}^{-1} x_k \in S$ za $1 \leq k < n$. Slijedi

$$y = (yx_{n-1}^{-1})(x_{n-1}x_{n-2}^{-1})...(x_2x^{-1})x = hx.$$

Za neki $h \in H$. Slijedi $h = yx^{-1} \implies yx^{-1} \in H \implies xH = yH$
$\Longleftarrow$
Pretpostavimo $xH = yH$. Tada $yx^{-1} \in H$, stoga je $y = hx$ za neki $h \in H$, te $h = x_n x_{n-1}...x_1$ gdje $x_k \in S$ za $k = 1, ..., n$.
Vidimo da x, x_1x, x_2x_1x, ..., $x_nx_{n-1}...x_1x = y$ čine put od x do y u danom grafu. Prema tome, x i y nalaze se u istoj komponenti povezanosti. □

Korolar 1.3.7. *Cayleyev graf $Cay(G, S)$ povezan je ako i samo ako S generira G.*

Dokaz. $\Longrightarrow$
Ako je $Cay(G, S)$ povezan, on ima samo jednu komponentu povezanosti. Zbog prethodne leme mora vrijediti $[G : \langle S \rangle] = 1$, tj. $G = \langle S \rangle$.
$\Longleftarrow$
Suprotno, ako S generira G, tada $[G : \langle S \rangle] = [G : G] = 1$, pa $xH = yH$ za sve $x, y \in G$, pa po istoj lemi slijedi da je $Cay(G, S)$ povezan. □

Korolar 1.3.8. *Neka je H podgrupa od G generirana simetričnim skupom S, gdje je $S \subseteq G \setminus \{e\}$ te neka je $n = [G : H]$. Tada graf $Cay(G, S)$ ima n komponenti povezanosti, a skup vrhova svake komponente povezanosti odgovara jednoj lijevoj klasi iz G/H.*

Dokaz. Prema dokazanoj lemi, svaka dva elementa $x, y \in G$ nalaze se u istoj komponenti povezanosti $Cay(G, S)$ ako i samo ako se nalaze u istoj lijevoj klasi od G po H. Prema tome, svaka lijeva klasa predstavlja sve vrhove jedne komponente povezanosti $Cay(G, S)$. □

Iz svega navedenog vidimo da Cayleyev graf može biti usmjeren, povezan te može sadržavati petlje. Zato uvodimo tri dodatne pretpostavke na S

- S je simetričan, time promatrani Cayleyev graf postaje neusmjeren
- S generira grupu G, što nam garantira povezanost
- $e \notin S$, iz ovoga slijedi da graf ne sadrži petlje.

Osim toga, iz prethodnih pretpostavki jednostavno vidimo i da je $Cay(G, S)$ regularan stupnja $|S|$.
Prije nego navedemo osnovnu karakterizaciju Cayleyevog grafa, definirajmo još pojam tranzitivnosti po vrhovima.

Definicija 1.3.9. *Za graf $G = (V, E)$ kažemo da je **tranzitivan po vrhovima**, ako za sve $x, y \in V$ postoji $f \in Aut(G)$ takav da $f(x) = y$. Za skup svih takvih f kažemo da djeluje **tranzitivno** nad G. Ako dodatno vrijedi da je za $x, y \in V$ pripadna $f \in Aut(G)$ jedinstvena, tada kažemo da skup svih takvih f djeluje **strogo tranzitivno** nad G.*

Sljedeća propozicija daje nam glavnu karakterizaciju Cayleyevog grafa.

Propozicija 1.3.10. *Povezan graf G je Cayleyev graf ako i samo postoji podgrupa $H \subseteq Aut(G)$ koja djeluje strogo tranzitivno nad G*

Dokaz. Pretpostavimo prvo da je G Cayleyev, možemo promatrati njemu izomorfan graf $G' = Cay(X, S)$.
Za $x \in X$ vrijedi da množenjem svih elemenata grupe sa x slijeva dobivamo permutaciju grupe, te za sve $a, b \in X$ postoji jedinstveni $x' \in X$ takav da $b = x'a$, stoga je G' tranzitivan po vrhovima.
Dokažimo i suprotan smjer, neka je G povezan i $H \subseteq Aut(G)$ koji djeluje tranzitivno nad G. Fiksirajmo vrh v i definirajmo

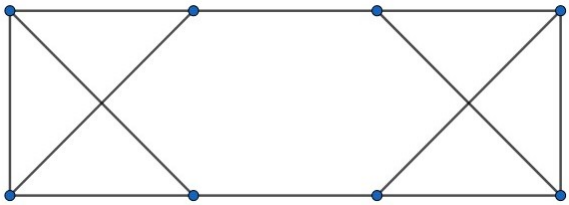
$$S = \{h \in H \mid hv \text{ i } v \text{ su susjedni vrhovi}\}.$$

Skup S je simetričan jer je H podskup skupa automorfizama pa su hv i v susjedni vrhovi ako i samo ako su v i $h^{-1}v$ susjedni vrhovi. Definiramo izomorfizam između G i $Cay(H, S)$ na sljedeći način, ako je u vrh grafa, tada postoji jedinstveni $h \in H$ za koji $hv = u$, pa preslikajmo $u \to h$.

□

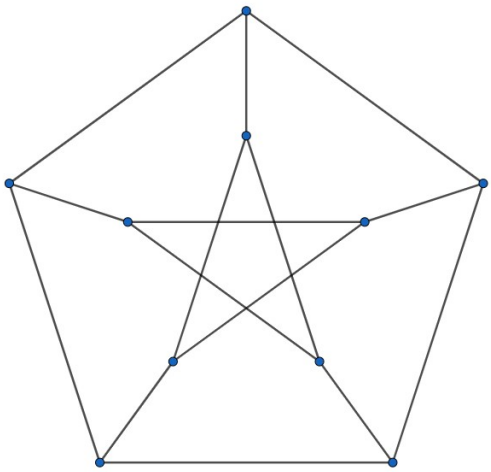
Iz prethodne propozicije slijedi da povezan graf nije nužno Cayleyev.

Primjer 1.3.11. *Na slici ispod možemo vidjeti primjer najmanjeg regularnog grafa koji nije Cayleyev.*



Navodimo još i primjer grafa koji je tranzitivan po vrhovima, a nije Cayleyev.

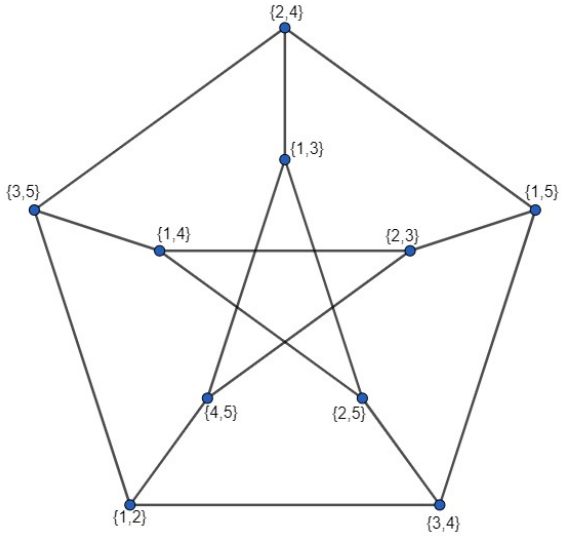
Primjer 1.3.12. *Slika ispod predstavlja Petersenov graf koji nije Cayleyev, ali je tranzitivan po vrhovima.*



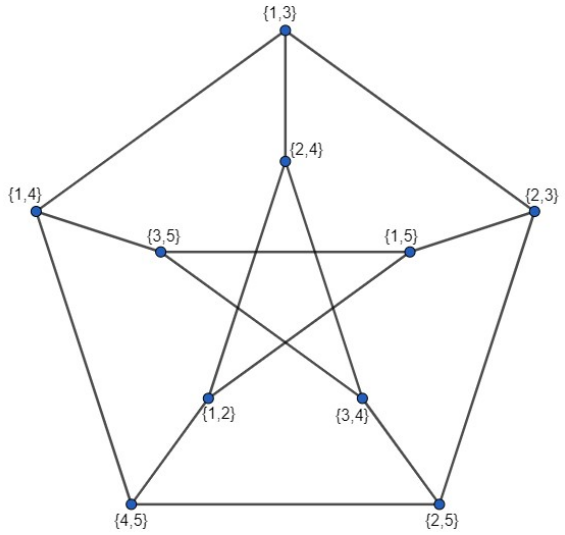
Dokažimo još činjenicu iz prethodnog primjera.

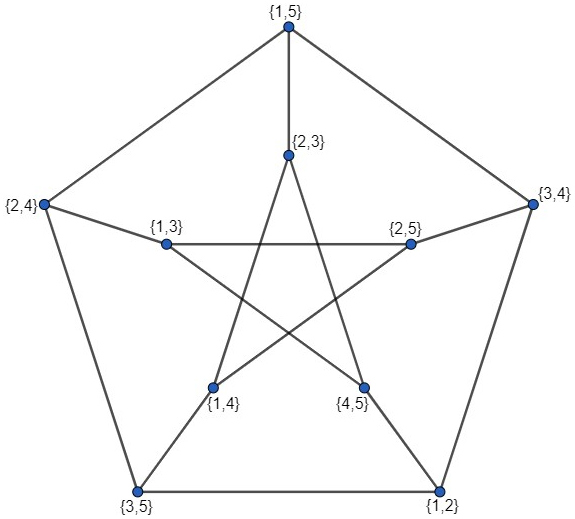
Propozicija 1.3.13. *Petersenov graf je tranzitivan po čvorovima, ali nije Cayleyev graf.*

Dokaz. Uočimo da ako kreiramo graf gdje su vrhovi svi dvočlani podskupovi skupa $\{1, 2, 3, 4, 5\}$, te povežemo dva vrha ako je presjek skupova u njima prazan, dobili smo graf izomorfan Petersenovom grafu.



Permutacijom (15)(24), unutrašnjih 5 vrhova zamijeni mjesta sa vanjskim vrhovima, a permutacijom (14523) vrhovi zamijene mjesta u smjeru suprotnom od kazaljke na satu.





Kombiniranjem prethodnim dvjema permutacijama možemo pronaći permutaciju koja proizvoljan vrh x šalje u proizvoljan vrh y, stoga je graf tranzitivan po vrhovima.
Dokažimo sada da graf nije Cayleyev. Pretpostavimo suprotno i primijetimo da su jedine dvije neizomorfne grupe reda 10, Z_{10} i D_5, gdje je D_5 dihedralna grupa.
S obzirom da naš graf mora biti izomorfan s nekim $Cay(G, S)$, jasno je da $G = Z_{10}$ ili $G = D_5$, te $|S| = 3$.
U prvom slučaju, neka su x i y neka dva elementa iz Z_{10}. S obzirom da je grupa Abelova i S simetričan, za neki $z \in G \setminus S$ vrijedi $z = xyx^{-1}y^{-1}z$ pa bi u grafu morao postojati ciklus duljine 4 u grafu, a vidimo da takvog nema.
Neka je sada $G = D_5$, zbog $|S| = 3$ barem jedan od elemenata u S mora biti reda 2, nazovimo ga x. Ako postoji y u S reda 5, tada bi za neki z mora vrijediti $z = ababz$ pa bi ponovo morao postojati ciklus duljine 4 u grafu. Slijedi da svaki element u s ima red jednak 2, ali tada ne postoji kombinacija 5 elemenata iz S koji daju e. □

Poglavlje 2

Teorija reprezentacije konačnih grupa

2.1 Osnovni pojmovi i činjenice

Definicija 2.1.1. *Neka je dana konačna grupa G i vektorski prostor V nad $\mathbb{C}$, homomorfizam grupa $\rho : G \to GL(V)$ nazivamo* ***reprezentacijom*** *konačne grupe G (ako je jasno o kojoj reprezentaciji ρ se radi, ponekad ćemo i sam V nazivati reprezentacijom).*

Teorija reprezentacije ključna je poveznica teorije grupa i linearne algebre. Najčešće ju koristimo kako bismo rezultate iz linearne algebre primijenili u dokazima vezanim uz teoriju grupa. Konkretno, linearna reprezentacija konačne grupe omogućava da se umjesto elementima grupe koristimo linearnim operatorima koji „čuvaju" informacije o grupi.

Primjer 2.1.2. *Za konačnu grupu G i vektorski prostor V najjednostavniji primjer reprezentacije je homomorfizam $\rho : G \to GL(V)$ koji svakom elementu $g \in G$ pridružuje operator identitete $I \in GL(V)$. Tu reprezentaciju nazivamo trivijalnom reprezentacijom.*

Definicija 2.1.3. *Neka je $\rho : G \to GL(V)$ reprezentacija konačne grupe G. Ako je na V definiran i skalarni produkt $\langle \cdot, \cdot \rangle$ takav da za sve $g \in G$ i $v, w \in V$ vrijedi*

$$\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle.$$

Tada kažemo da je ρ ***unitarna reprezentacija*** *s obzirom na skalarni produkt $\langle \cdot, \cdot \rangle$ (ili samo* ***unitarna*** *ako je jasno o kojem skalarnom produktu se radi).*

Primjer 2.1.4. *Za proizvoljnu konačnu grupu G promotrimo njenu trivijalnu reprezentaciju nad $\mathbb{C}$. Jasno je da za sve $g \in G$ i $\alpha, \beta \in \mathbb{C}$ vrijedi*

$$\langle \rho(g)\alpha, \rho(g)\beta \rangle = \langle \alpha, \beta \rangle.$$

Stoga je ova reprezentacija unitarna.

Definicija 2.1.5. *Za svaki podskup elemenata S konačne grupe G i reprezentaciju $\rho : G \to GL(\mathbb{C}[G])$ definiramo prosjek reprezentacije ρ na S kao*

$$S_\rho = \frac{1}{|S|} \sum_{s \in S} \rho(s) \in L(V).$$

Definicija 2.1.6. *Za konačnu grupu G definiramo $|G|$-dimenzionalni vektorski prostor*

$$\mathbb{C}[G] = \left\{ \sum_{g \in G} \alpha_g \cdot g \mid \alpha_g \in \mathbb{C} \right\}$$

te ga snabdijevamo skalarnim produktom koji za $a, b \in G$ zadovoljava

$$\langle a, b \rangle = \begin{cases} 1, & ako\ a = b \\ 0, & inače \end{cases}$$

Primjer 2.1.7. *Još jedan primjer reprezentacije koja se često koristi u dokazima je tzv.* ***regularna reprezentacija*** *$R : G \to \mathbb{C}[G]$ koju definiramo kao*

$$R(a)\left(\sum_{g \in G} c_g g \right) = \sum_{g \in G} c_g ab$$

pri čemu je $a \in G$ i za svaki $g \in G$ vrijedi $c_g \in \mathbb{C}$. Dokažimo da je ona dobro definirana.

Dokaz. Pretpostavimo da postoje $a, b \in G$ takvi da $a \neq b$ i $R(a) = R(b)$. Prema definiciji R, za neutralni element e grupe G vrijedi $a = ae = R(a)e = R(b)e = be = b$, što je kontradikcija sa početnom pretpostavkom. □

Propozicija 2.1.8. *Neka je S bilo koji simetričan podskup od G, tada je matrični prikaz operatora S_R u bazi $\{g \mid g \in G\}$ jednak normaliziranoj matrici susjedstva grafa $Cay(G, S)$.*

Dokaz. Označimo sa N normaliziranu matricu susjedstva grafa $Cay(G, S)$ te sve operatore promatramo u bazi $\{g \mid g \in G\}$.
Uočimo da je $R(g)$ permuatacija baze dobivena množenjem svakog elementa sa g slijeva. Iz toga slijedi da za $s \in S$ matrica $R(s)$ prikazuje sve bridove (a, b) u grafu $Cay(G, S)$ dobivene zbog jednakosti $a = sb$.
Prema tome $\sum_{s \in S} R(s)$ je matrica susjedstva grafa $Cay(G, S)$, a s obzirom da iz svakog vrha izlazi $|S|$ bridova, slijedi tvrdnja propozicije. □

Kod najčešćih primjera linearnih operatora $f : V \to V$, koristimo se podskupovima $W \in V$ takvim da $f(W) \in W$ koje nazivamo invarijantnim skupovima. Definirajmo ekvivalentan pojam u teoriji reprezentacije.

Definicija 2.1.9. *Neka je $\rho : G \to GL(V)$ linearna reprezentacija i W vektorski potprostor od V, kažemo da je W* ***invarijantan s obzirom na*** *ρ, ako je invarijantan s obzirom na svaki $\rho(g)$, $g \in G$. Tada je $p|_W$ također linearna reprezentacija. Reprezetaciju $p|_W$ nazivamo podreprezentacijom od ρ.*

Primjer 2.1.10. *Neka je V reprezentacija neke konačne grupe G dana regularnom reprezentacijom, neka je W jednodimenzionalni potprostor od V razapet sa $v = \sum_{g\in G} e_g$.*
Tada je $R(g)v = v$ za sve $g \in G$. Prema tome, $R|_W$ je podreprezentacija od R.

Kao što smo u linearne operatore rastavljali na sumu operatora na svojstvenim potprostorima, tako i linearnu reprezentaciju možemo zapisati kao direktnu sumu operatora na invarijantnim potprostorima.

Teorem 2.1.11. *[19] Neka je $\rho : G \to GL(V)$ linearna reprezentacija i W vektorski potprostor od V koji je invarijantan s obzirom na ρ . Tada postoji komplement $W^\perp$ od W koji je također invarijantan s obzirom na ρ.*

Dokaz. Neka je W' proizvoljan ortogonalni komplement od W u V i neka je p projekcija na W. Promotrimo

$$G_{\rho\cdot p\cdot\rho^{-1}} = \frac{1}{|G|}\sum_{g\in S}\rho(g)\cdot p\cdot\rho(g)^{-1}.$$

S obzirom da p slika V u W i W je $\rho(g)$ invarijantan, slijedi da $G_{\rho p\rho^{-1}}$ preslikava V u W.
Osim toga, za $x \in W$ vrijedi $\rho(g)x \in W$ pa imamo

$$p\cdot\rho(g)^{-1}x = \rho(g)^{-1}x$$

$$\rho(g)\cdot p\cdot\rho(g)^{-1}x = x.$$

To jest

$$G_{\rho\cdot p\cdot\rho^{-1}}x = x.$$

Zato je $G_{\rho\cdot p\cdot\rho^{-1}}$ projekcija V na W, koja odgovara nekom komplementu $W^\perp$ od W.
Također, za sve $h \in G$ zbog

$$\rho(h)\cdot G_{\rho\cdot p\cdot\rho^{-1}}\cdot\rho(h)^{-1} = \frac{1}{|G|}\sum_{g\in S}\rho(h)\cdot\rho(g)\cdot p\cdot\rho(g)^{-1}\cdot\rho(h)^{-1}$$

$$= \sum_{g\in S}\rho(hg)\cdot p\cdot\rho(hg)^{-1}.$$

$$\overset{hG=G}{=} \sum_{g\in S}\rho(g)\cdot p\cdot\rho(g)^{-1} = G_{\rho\cdot p\cdot\rho^{-1}}$$

vrijedi

$$\rho(h) \cdot G_{\rho \cdot p \cdot \rho^{-1}} = G_{\rho \cdot p \cdot \rho^{-1}} \cdot \rho(h).$$

Ako je sada $x \in W^{\perp}$ i $h \in G$, mora vrijediti

$$G_{\rho \cdot p \cdot \rho^{-1}} x = 0.$$

Odnosno

$$G_{\rho \cdot p \cdot \rho^{-1}} \cdot \rho(h)x = \rho(h) \cdot G_{\rho \cdot p \cdot \rho^{-1}} x = 0.$$

Što nam govori da je $W^{\perp}$ invarijantan s obzirom na $\rho(g)$ za svaki $g \in G$. □

Definicija 2.1.12. *Kažemo da je reprezentacija V (ili $\rho : G \to GL(V)$) **ireducibilna**, ako V nije nulprostor i ne postoji netrivijalan ρ-invarijantni podprostor W od V.*

Teorem 2.1.13. *[19] Svaka reprezentacija je direktna suma ireducibilnih reprezentacija.*

Dokaz. Neka je $\rho : G \to GL(V)$ reprezentacija grupe G. Tvrdnju dokazujemo indukcijom po $dim(V)$.
Za bazu indukcije kada je $dim(V) = 0$, nemamo što dokazivati.
Pretpostavimo da tvrdnja vrijedi za $dim(V) < n$ te neka je sada $dim(V) = n$.
Ako je V ireducibilna, tada je $V = 0 \oplus V$. U suprotnom postoji netrivijalan ρ-invarijantni podprostor $W \subseteq V$, prema Teoremu 2.1.11 slijedi da je V jednak direktnoj sumi W i $W^{\perp}$.
Po pretpostavci indukcije, slijedi tvrdnja. □

Definicija 2.1.14. *Neka su ρ i ρ' dvije reperezentacije konačne grupe G na vektorskim prostorima V i V′. Kažemo da su ρ i ρ' izomorfne ukoliko postoji lineran operator $\tau : V \to V'$ koji je izomorfizam, te za sve $g \in G$ vrijedi:*

$$\tau \circ \rho(g) = \rho'(g) \circ \tau$$

Teorem 2.1.15 (Schurova lema)**.** *[19] Ako su $\phi : G \to V$ i $\theta : G \to W$ dvije ireducibilne reprezentacije grupe G nad poljem kompleksnih brojeva, i $\psi : V \to W$ linearan operator takav da*

$$\theta(g)\psi = \psi\phi(g) \ \forall g \in G$$

tada vrijedi:

1. *Ako ϕ i θ nisu izomorfne, tada je $\psi = 0$*
2. *Ako je $V = W$ i $\phi = \theta$, tada je $\psi = \lambda Id$*

Dokaz. 1. Pretpostavimo da $\psi \neq 0$, tj. postoji $v \in V$ takav da $\psi(v) \neq 0$. Sada mora vrijediti $\mathrm{Im}\{\psi\} \neq 0$, stoga je prema uvjetu iz teorema, $\theta_{\mathrm{Im}\{\psi\}}$ podreprezentacija od W. Zbog ireducibilnosti imamo $\mathrm{Im}\{\psi\} = W$.
Analogno iz pretpostavke $\psi \neq 0$, $\ker\{\psi\} \neq V$ i ireducibilnosti od V slijedi $\ker\{\psi\} = 0$ pa je ψ izomorfizam.

2. Neka je λ svojstvena vrijednost od ψ. Promotrimo operator $\psi' = \psi - \lambda Id$.
Jasno je da $\ker\{\psi'\} \neq 0$, te u uvjetu teorema ψ možemo zamijeniti sa ψ'. Zbog dokaza prvog dijela teorema, mora vrijediti $\psi' = 0$, odnosno $\psi = \lambda Id$

□

Sada bez dokaza iznosimo dvije tvrdnje potrebne za dokaz u radu. Njihova pozadina izlazi van opsega ovog rada, a dokaze možemo pronaći u [19].

Teorem 2.1.16. *[19] Konačna grupa ima konačno mnogo ireducibilnih reprezentacija (do na izomorfizam).*

Teorem 2.1.17. *[19] Za regularnu reprezentaciju R konačne grupe G uz oznaku $d_\rho = dim\rho$ vrijedi*

$$R = \bigoplus \underbrace{\rho \oplus ... \oplus \rho}_{d_\rho} \tag{2.1}$$

gdje je direktna suma uzeta po svim ireducibilnim reprezentacijama od G (kojih ima konačno mnogo prema prethodnom teoremu).

Ako sa $\hat{G}$ označimo skup svih međusobno neizomorfnih ireducibilnih reprezentacija sa G u $GL(\mathbb{C}[G])$, brojeći dimenzije s obje strane jednakosti prethodnog teorema dobivamo $|G| = \sum_{\rho\hat{G}} d_\rho^2$. Uz oznaku $D(G) = \sum_{\rho\hat{G}} d_\rho$ (pisati ćemo samo D ako znamo o kojoj grupi se radi) vrijedi

$$\sqrt{|G|} < D(G) \leq |G|$$

Objasnimo još zašto je prva nejednakost stroga, kako bismo to učinili dovoljno je pronaći pravi podprostor od $\mathbb{C}[G]$ koji je invarijantan s obzirom na R. Neka je $K \subseteq \mathbb{C}[G]$ jednodimenzionalni vektorski podprostor razapet vektorom $e = \sum_{g\in G} g \in \mathbb{C}[G]$. S obzirom da je $R(a)e = e$, R invarijantna na podprostoru K iz čega slijedi tvrdnja.

Poglavlje 3

Alon-Roichmanov teorem

3.1 Hoeffdingova nejednakost

Rezultat ovog poglavlja omogućit će nam relativno kratak dokaz Alon-Roichmanovog u usporedbi s prvobitnim dokazom iz [2].

Lema 3.1.1. *[18] Neka su $X_1, ..., X_t$ nezavisne slučajne varijable takve da $0 \leq X_i \leq 1$ te $\mathbf{E}X_k = \mu_k$ za $k = 1, ..., t$. Vrijedi*

$$\mathbf{P}\left(\frac{\sum_{k=1}^{t} X_k}{t} - \frac{\sum_{k=1}^{t} \mu_k}{t} \geq \epsilon \right) \leq e^{-2\epsilon^2 t}.$$

Navedeni, osnovni oblik Hoeffdingove nejednakosti daje nam gornju ogradu na prosjek n ograničenih nezavisnih slučajnih varijabli. U glavnome dokazu ovog rada koristiti ćemo se nezavisnim slučajnim linearnim operatorima. Zbog toga ćemo dokazati verziju Hoeffdingovog teorema za slučajne operatore.

Definicija 3.1.2. *Radi lakšeg zapisa, definirajmo **težinsku funkciju entropije** H_p kao*

$$H_p(x) = x \ln\left(\frac{x}{p}\right) + (1 - x) \ln\left(\frac{1 - x}{1 - p}\right).$$

Na Hilbertovom prostoru V dimenzije d označavamo sa $A(V)$ skup svih hermitskih operatora te sa $B(V)$ skup svih pozitivnih operatora. Tada je na skupu $A(V)$ dan parcijalni uređaj gdje pišemo $A \leq B$ ako i samo ako vrijedi $B - A \in B(V)$. Također, s $[A, B]$ označavamo skup svih operatora $C \in A(V)$ takvih da $A \leq C \leq B$.
Kako što za slučajne varijable često koristimo ograde vezane za njihove funkcije izvodnice momenata, pokazat ćemo ogradu na funkcije izvodnicu momenata slučajnog operatora.

Definicija 3.1.3. *Za proizvoljnu matricu $X \in M_n$ definiramo* ***eksponencijalnu funkciju matrice*** *X kao*

$$e^X := \sum_{k=0}^{\infty} \frac{1}{k!} X^k \in M_n.$$

Upotpunimo prethodnu definiciju obrazloženjem da prethodno definirani eksponencijalni opeator matrice X uvijek postoji. Uzimanjem porizvoljne norme $\|\cdot\|$ na M_n (svejedno nam je koju normu promatramo jer su one sve ekvivalentne na konačnodimenzionalnom prostoru M_n) imamo

$$\left\| \sum_{k=0}^{n} \frac{1}{k!} X^k \right\| \leq \sum_{k=0}^{\infty} \frac{1}{k!} \|X\|^k = e^{\|X\|}.$$

S obzirom da je red $\sum_{k=0}^{\infty} \frac{1}{k!} X^k$ apsolutno konvergentan i M_n Banachov prostor, slijedi da on konvergira i obično.

Lema 3.1.4. *[3]*

Neka je V d-dimenzionalan Hilbertov prostor, $r \in [0,1]$ i X slučajan operator koji poprima vrijednosti u $[-rI, (1-r)I] \subseteq A(V)$ i $\mathbf{E}X = 0$. Za svaki $h \geq 0$ vrijedi

$$\mathbf{E}e^{hX} \leq (1-r)Ie^{-rh} + rIe^{(1-s)h}.$$

Dokaz. Uočimo da je funkcija $f(t) = e^t$ konveksna, prema Jensenovoj nejednakosti dobivamo

$$e^{hy} \leq (1-r-y)e^{-rh} + (r+y)e^{(1-s)h}.$$

Jasno je da ukoliko su odgovarajući dijgonalni elementi dijagonalne matrice K manji od pripadnih dijagonalnih elemenata matrice L, tada je $L \leq K$. Neka je Y dijagonalna matrica, prema definicije e^Y slijedi da je i ona dijagonalna pa iz navedenih tvrdnji i prethodne nejednakosti slijedi

$$e^{hY} \leq (I - rI - Y)e^{-rh} + (rI + Y)e^{(1-s)h}.$$

S obzirom da postoje ortogonalna matrica U i dijagonalna D takve da $X = UDU^T$ te općenito za invertibilnu matricu U iz definicije eksponencijalne matrice od UDU^{-1} slijedi $e^{UDU^{-1}} = Ue^DU^{-1}$, imamo

$$e^{hX} = e^{hUDU^T} = Ue^{hX}U^T \leq (I - rI - X)e^{-rh} + (rI + X)e^{(1-s)h}.$$

Uzimanjem očekivanja u prethodnoj nejednakosti slijedi tvrdnja leme. □

Prethodna lema dokazuje se potpuno analogno i u slučaju uvjetnog očekivanja.

Dokažimo sada još jednu jednostavnu, ali veoma važnu lemu.

Lema 3.1.5. *[3] Neka je X slučajan operator koji poprima vrijednosti na B(V), gdje je V Hilbertov prostor. Vrijedi*

$$\mathbf{P}(X \not\leq I) \leq \mathrm{Tr}(\mathbf{E}X).$$

Dokaz. Imamo

$$\mathbf{E}X = \sum_{A \in B(V)} \mathbf{P}(X = A)A \geq \sum_{A \in B(V): A \not\leq I} \mathbf{P}(X = A)A.$$

S obzirom da za $A \in B(V)$ takav da $A \not\leq I$ nužno vrijedi $\mathrm{Tr}(A) \geq 1$, uzimanjem traga navedene nejednakosti slijedi tvrdnja. □

Spremni smo dokazati i Hoeffdingov teorem za linearne operatore.

Teorem 3.1.6 (Hoeffdingov teorem za linearne operatore)**.** *[3] Neka je V Hilbertov prostor dimenzije d i $\{X_k\}_{k=1}^n$ martingal s obzirom na prirodnu filtraciju $\{\mathcal{F}_k\}_{k=1}^n$ koji poprima vrijednosti u A(V), te za razliku njegovih članova $Y_i = X_i - X_{i-1}$ vrijedi $Y_i \in B(V)$ i $Y_i \in [r_i I, (1 - r_i)I]$ za neke realne brojeve $r_i \in [0, 1]$. Uz oznaku $r = \sum_{i=1}^{n} r_i$ imamo*

$$\mathbf{P}(X_n - \mathbf{E}X_n \not\leq nhI) \leq d \exp\left(-nH_r(r + h)\right)$$

i

$$\mathbf{P}(X_n - \mathbf{E}X_n \not\geq nhI) \leq d \exp\left(-nH_r(r - h)\right).$$

Dokaz. Neka je $s > 0$ proizvoljan realan broj. Za svaki $n \in N$ slučajna varijabla $\sum_{i=1}^{n-1} Y_i$ je $\mathcal{F}_{n-1}$-izmjeriva pa i $e^{s\sum_{i=1}^{n-1} Y_i}$ mora biti $\mathcal{F}_{n-1}$ izmjeriva. Zbog prethodnih tvrdnji i svojstva uvjetnog očekivanja imamo

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n} Y_i}\right)\right) &= \mathrm{Tr}\left(\mathbf{E}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n} Y_i}|\mathcal{F}_{n-1}\right)\right)\right) \\ &= \mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n-1} Y_i}\right)\mathbf{E}\left(e^{sY_n}|\mathcal{F}_{n-1}\right)\right).\end{aligned}$$

Pa s obzirom na to da

$$\mathbf{E}\left(Y_n|\mathcal{F}_{n-1}\right) = \mathbf{E}\left(X_n - X_{n-1}|\mathcal{F}_{n-1}\right) = X_{n-1} - X_{n-1} = 0$$

i $Y_n \in [-r_i, 1 - r_i]$ po Lemi 3.1.4 mora vrijediti

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n} Y_i}\right)\right) &\leq \mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n-1} Y_i}\right)\left((1 - r_n)e^{-sr_n} + r_n e^{s(1-r_n)}\right)I\right) \\ &= \left((1 - r_n)e^{-sr_n} + r_n e^{s(1-r_n)}\right)\mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n-1} Y_i}\right)\right).\end{aligned}$$

Induktivno zaključujemo

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n}Y_i}\right)\right) &\leq \prod_{i=1}^{n}\left((1-r_i)e^{-sr_i}+r_ie^{s(1-r_i)}\right)\\ &= e^{-snr}\prod_{i=1}^{n}\left((1-r_i)+r_ie^{s}\right).\end{aligned}$$

Zbog *AG* nejednakosti slijedi

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n}Y_i}\right)\right) &\leq e^{-snr}\left(\frac{\sum_{i=1}^{n}(1-r_i)+\sum_{i=1}^{n}r_ie^{s}}{n}\right)^{n}\\ &= d\left((1-r)e^{-sr}+re^{s(1-r)}\right)^{n}\end{aligned}$$

Po Lemi 3.1.5 i prethodnom računu, za $s>0$ dobiva se

$$\begin{aligned}\mathbf{P}(X_n-\mathbf{E}X_n \not\leq nhI) &= \mathbf{P}\left(\sum_{i=1}^{n}Y_i \not\leq hnI\right)\\ &= \mathbf{P}\left(e^{s\sum_{i=1}^{n}Y_i} \not\leq e^{shnI}\right)\\ &\leq e^{-shn}\mathrm{Tr}\left(\mathbf{E}\left(e^{s\sum_{i=1}^{n}Y_i}\right)\right)\\ &\leq d\left((1-r)e^{-s(r+h)}+re^{s(1-r-h)}\right)^{n}\end{aligned}$$

s time da smo u prelasku iz prvog u drugi red koristili činjenicu da se $\sum_{i=1}^{n}Y_i$ može dijagonalizirati. Minimiziranjem prethodnog izraza po s, slijedi da se minimum postiže za $s=\ln\frac{(r+h)(1-r)}{r(1-r-h)}$.

Uz oznaku $y = \frac{(r+h)(1-r)}{r(1-r-h)}$, uvrštavanjem točke minimuma imamo

$$\begin{aligned}
\mathbf{P}(X_n - \mathbf{E}X_n \not\leq nhI) &\leq d\left((1-r)e^{-(r+h)\ln y} + re^{(1-r-h)\ln y}\right)^n \\
&= d\left((1-r)y^{-(r+h)} + ry^{1-r-h}\right)^n \\
&= d\left(y^{-(r+h)}\left((1-r) + ry\right)\right)^n \\
&= d\left(\exp\left(-(r+h)\ln y + \ln(1-r+ry)\right)\right)^n \\
&= d\left(\exp\left(-(r+h)\ln\frac{(r+h)(1-r)}{r(1-r-h)} + \ln\frac{r-1}{r+h-1}\right)\right)^n \\
&= d\exp\left(-n\left((r+h)\ln\frac{(r+h)}{r} + (1-r-h)\ln\frac{1-r-h}{1-r}\right)\right) \\
&= d\exp\left(-nH_r(r+h)\right)
\end{aligned}$$

čime je dokazana prva tvrdnja teorema. Druga nejednakost dobiva primjenom prve nejednakosti promatrajući martingal $-X_k$, odnosno zamjenom $r \to 1-r$ u prethodnom rezultatu te činjenicom da $H_p(x) = H_{1-p}(1-x)$. □

Vratimo se kratko na Lemu 3.1.1. Zbog činjenice da je $\sum_{k=1}^{t}(X_k - \mathbf{E}X_k)$ martingal, sada vidimo da je ona zaista slabija verzija upravo dokazanog teorema.

3.2 Dokaz Alon-Roichmanovog teorema

Prisjetimo se najprije nekoliko pojmova iz prva dva poglavlja.

Definicija. *Za konačnu grupu G i $S \subset G$ definiramo Cayleyev graf $Cay(G,S) = (V,E)$ gdje je skup vrhova V jednak G, a za skup bridova vrijedi*

$$E = \{(a,b) \mid a,b \in V,\ \exists s \in S, a = sb\}.$$

Podsjetimo se još jednog pojma iz drugog poglavlja.

Definicija. *Neka je dana konačna grupa G i prostor $\mathbb{C}[G]$ i $\hat{G}$ skup svih međusobno neizomorfnih ireducibilnih reprezentacija sa G u $GL(\mathbb{C}[G])$. Definiramo $D(G)$ (ili samo D ako je jasno o kojoj grupi se radi) kao sumu dimenzija po svim ireducibilnim reprezentacijama $\rho : G \to \mathbb{C}[G]$, odnosno $D := \sum_{\rho\in\hat{G}} d_\rho$*

Ključno će nam u dokazu biti da iz svih vrhova izlazi točno $2|S|$ bridova, zato dopuštamo "višestruke" bridove između vrhova u slučaju kada nisu svi elementi iz S različiti ili se u

S nalaze i element $s \in G$ i njegov inverz.
Time nam je garantirano da svaki vrh ima točno $2|S|$ izlaznih bridova, dok ćemo u matrici susjedstva na mjestu i-tog retka i j-tog stupca jednostavno upisati broj svih bridova koji povezuju i sa j (ako je i povezan sa samim sobom, na i-tom mjestu dijagonale matrice susjedstva nalazit će se broj 2).
U praksi, vjerojatnost da smo izabrali duple elemente u S će biti otprilike $\left(\frac{log|G|}{|G|}\right)^2$ što nam neće predstavljati problem.
Glavni teorem dokazat ćemo kao posljedicu sljedećeg, pomoćnog teorema.

Teorem 3.2.1. *Neka je G konačna grupa, $k \in \mathbb{N}$ i $0 < \epsilon < 1$ tada vrijedi*

$$\mathbf{P}\left(\frac{\lambda(Cay(G,S))}{2k} \geq \epsilon\right) \leq 2D \exp\left\{-kH_{\frac{1}{2}}\left(\frac{1+\epsilon}{2}\right)\right\},$$

pri čemu su $s_1, ..., s_k$ nezavisne slučajne varijable uniformno distribuirane na G i $S = \{s_1, ..., s_k\}$.

Teorem 3.2.2 ([Alon-Roichman [3]). *Za svaki $\epsilon > 0$ postoji $k = k(D) = \left(\frac{2}{\epsilon^2} + o(1)\right)\log D$ takva da za sve konačne grupe G vrijedi*

$$\mathbf{E}\left[\frac{\lambda(Cay(G,S))}{2k}\right] \leq \epsilon.$$

Pri čemu su $s_1, ..., s_k$ nezavisne slučajne varijable, uniformno distribuirane na G, a S je skup $\{s_1, ..., s_k\}$ i $D = \sum_{\rho \in \hat{G}} d_\rho$.

Dokažimo da Alon-Roichmanov teorem zaista slijedi iz Teorem 3.2.1.

Dokaz. S obzirom na to da $\frac{\lambda(Cay(G,S))}{2k}$ poprima vrijednosti u $[0, 1]$, uzimanjem $\delta = \delta(D)$ koja teži u nulu i za koju $\ln \delta^{-1} = o(\ln D)$, $\epsilon' = \epsilon(1-\delta)$, $b = -\log(\epsilon\delta)$ te $k = \dfrac{1}{H_{\frac{1}{2}}\left(\frac{1+\epsilon}{2}\right)}(\ln D + b + \ln 2)$ u Teoremu 3.2.1 slijedi

$$\begin{aligned}\mathbf{P}\left(\frac{\lambda(Cay(G,S))}{2k} \geq \epsilon'\right) &\leq 2D \exp\left\{-\frac{\ln\left(2De^b\right)}{H_{\frac{1}{2}}\left(\frac{1+\epsilon}{2}\right)} H_{\frac{1}{2}}\left(\frac{1+\epsilon}{2}\right)\right\} \\ &= 2D \exp\left\{\ln\left(\frac{e^{-b}}{2D}\right)\right\} \\ &= e^{-b} = \epsilon\delta\end{aligned}$$

Uz oznaku $X = \frac{\lambda(Cay(G,S))}{2k} \in [0,1]$ dobivamo

$$\begin{aligned}
&= \mathbf{E}\left[X\mathbb{1}_{\{X<\epsilon'\}}\right] + \mathbf{E}\left[X\mathbb{1}_{\{X\geq\epsilon'\}}\right] \\
&\leq \epsilon'\mathbf{P}(X < \epsilon') + \mathbf{P}(X \geq \epsilon') \\
&\leq \epsilon' + \epsilon\delta \\
&= \epsilon(1-\delta) + \epsilon\delta \\
&= \epsilon
\end{aligned}$$

□

Sada nam je preostalo još dokazati Teorem 3.2.1.

Dokaz. Za element $a = \sum_{g\in G} a_g \cdot g \in \mathbb{C}[G]$ i reprezentaciju ρ, definiramo

$$\hat{a}(\rho) := \sum_{g\in G} a_g \cdot \rho(g).$$

Neka je

$$s = \frac{1}{2k}\sum_{i=1}^{k}(s_i + s_i^{-1}) \in \mathbb{C}[G].$$

Napomenimo da prema Propoziciji 2.1.8 za normaliziranu matricu susjedstva N grafa $Cay(G,S)$ vrijedi da je N prikaz operatora $\hat{s}(R)$ u bazi $\{g|\ g \in G\}$ prostora $\mathbb{C}[G]$. U ostatku dokaza, sve ćemo operatore promatrati u prethodno spomenutoj bazi. Promotrimo dekompoziciju R u ireducibilne reprezentacije dane sa 2.1 iz Teorema 2.1.17, ona odgovara ortogonalnoj direktnoj sumi dekompozicije $\mathbb{C}[G]$ u prostore invarijantne za svaki $R(g)$. Također, svojstvena vrijednost 1 odgovara trivijalnoj reprezentaciji u $\mathbb{C}[G]$, zato je dovoljno ograničiti spektar operatora $\hat{s}(R)$ po skupu netrivijalnih reprezentacija koje se pojavljuju u dekompoziciji R, odnosno

$$\frac{\lambda(Cay(G,S))}{2k} = \max_{\rho\neq 1} \|\hat{s}(\rho)\|.$$

Neka je ρ netrivijalna reprezentacija G te uvedimo oznaku $a_i = \frac{1}{2}(s_i + s_i^{-1})$ za $i = 1, ..., k$. Tada je $s = \frac{1}{k}\sum_{i=1}^{k} a_i$ te zbog unitarnosti $\rho(s_i^{-1}) = \rho(s_i)^{-1} = \rho(s_i)^*$ vrijedi da je slučajni operator

$$A_i := \frac{1}{2}(\rho(s_i) + \rho(s_i^{-1})) = \frac{1}{2}(\rho(s_i) + \rho(s_i)^*)$$

hermitski. Označimo sa $X_i = \sum_{j=1}^{i} A_j$.

Matrica operatora $\sum_{g\in G} R(g)$ jednaka je matrici sa svim elementima jednakim 1, stoga je ona ranga 1. Osim toga, i matrica trivijalne dekompozicije ima rang jednak 1. Sada zbog dekompozicije R u ireducibilne reprezentacije po Teoremu 2.1.17, uzimanjem ranga lijeve i desne strane jednakosti dane spomenutim teoremom, slijedi da je $\sum_{g\in G} \rho(g)$ ranga 0, odnosno nuloperator, dobivamo

$$\mathbf{E}[A_i] = \frac{1}{2k|G|}\left(\sum_{g\in G}\rho(g)\right) = 0,$$

odnosno

$$\begin{aligned}\mathbf{E}[X_i|X_{i-1}] &= \mathbf{E}[X_{i-1} + A_i|X_{i-1}]\\ &= \mathbf{E}[X_{i-1}|X_{i-1}] + \mathbf{E}[A_i|X_{i-1}] = X_{i-1}.\end{aligned}$$

Slijedi da je X_i martingal koji zadovoljava uvjete Teorema 3.1.6. Prema tome

$$\begin{aligned}\mathbf{P}(\|\rho(s)\| \geq \epsilon) &= \mathbf{P}\left(\left\|\frac{1}{k}\sum_{i=1}^{k} A_i\right\| \geq \frac{\epsilon}{2}\right)\\ &= \mathbf{P}\left(\|X - \mathbf{E}X\| \geq \frac{\epsilon k}{2}\right)\\ &\leq 2d_\rho \exp\left\{-kH_{\frac{1}{2}}\left(\frac{1+\epsilon}{2}\right)\right\}.\end{aligned}$$

Zbrajanjem po svim ireducibilnim reprezentacijama slijedi tražena tvrdnja.

□

Poglavlje 4

Primjene

4.1 Slučajna šetnja

Šetnja na grafu $G = (V, E)$ je niz vrhova $v_1, v_2, ..., v_k \in V$ takvih da je v_{i+1} susjedan vrhu v_i. Ako je v_{i+1} izabran uniformno nasumično među susjedima v_i, takvu šetnju nazivamo *slučajnom šetnjom*. Početni vrh slučajne šetnje obično odabiremo iz neke početne distribucije π_1. Time induciramo vjerojatnosnu distribuciju π_i na V takvu da je vjerojatnost da $v_i = v \in V$ jednaka $\pi_i(x)$. Sa slučajnom šetnjom smo se već susreli na kolegiju Markovljevi lanci, navedimo formalnu definicju.

Definicija 4.1.1. *Neka je $p \in R^n$ takav da za $i = 1, 2, ..., n$ vrijedi $p_i \geq 0$, te je zadovoljeno $\sum_{i=1}^{n} p_i = 1$. Tada p nazivamo **vjerojatnosnom distribucijom**. Sa $u = \frac{1}{n}(1, 1, ..., 1) \in R^n$ označavamo uniformnu distribuciju.*

Na spomenutom kolegiju dokazali smo da za povezan graf G, koji nije bipartitan, distribucije π_i konvergiraju graničnoj (pa i stacionarnoj) distribuciji ([22] Teorem 8.9.). Također, ako je G regularan, tada je granična distribucija zapravo uniformna distribucija. Unatoč tome, nismo odgonetnuli sva pitanja vezana uz slučajnu šetnju, jedno od njih je koliko brzo slučajna šetnja zapravo konvergira prema ganičnoj distribuciji. To je ipak preopćenito pitanje, proučavat ćemo zato slučajnu šetnju na d-regularnom grafu s malom drugom svojstvenom vrijednošću. Pokazat će se da tada slučajna šetnja „brzo" konvergira prema graničnoj distribuciji. Prisjetimo se formalnih definicija potrebnih pojmova.

Definicija 4.1.2. *Za vektore $u, v \in R^n$ definiramo skalarni produkt i norme l_1, l_2 te l_∞ kao*

$$\langle u, v\rangle = \sum_{i=1}^{n} u_i v_i$$
$$\|u\|_1 = \sum_{i=1}^{n} |u_i|$$
$$\|u\|_2 = \sqrt{\langle u, u\rangle} = \left(\sum_{i=1}^{n} u_i^2\right)^{\frac{1}{2}}$$
$$\|u\|_\infty = \max_{1\le i\le n} |u_i|$$

Definicija 4.1.3. *Neka je $p \in R^n$ takav da za $i = 1, 2, ..., n$ vrijedi $p_i \geq 0$, te je zadovoljeno $\sum_{i=1}^{n} p_i = 1$. Tada p nazivamo **vjerojatnosnom distribucijom**. Sa $u = \frac{1}{n}(1, 1, ..., 1) \in R^n$ označavamo uniformnu distribuciju.*

U ostatku poglavlja promatramo slučaj kada je graf G na kojem promatramo slučajnu šetnju d-regularan graf. Jednostavno se pokaže da je tada N, normalizirana matrica susjedstva, zapravo prijelazna matrica slučajne šetnje na G.

Teorem 4.1.4 (Teorem 3.4. [7])**.** *Neka $G = (V, E)$ graf sa n vrhova, $\lambda(G) = \lambda$ i $p \in R^n$ proizvoljna vjerojatnosna distribucija. Tada vrijedi*

$$\|N^k p - u\|_1 \leq \left(\frac{\lambda}{d}\right)^k \sqrt{n}.$$

Prethodni teorem nam govori da slučajna šetnja konvergira prema graničnoj distribuciji otprilike logaritamskom brzinom, bez obzira na početnu distribuciju ako je druga najveća svojstvena vrijednost po apsolutnoj vrijednosti pripadnog grafa mala.

Dokaz. Budući da je N simetrična matrica, postoji ortonormirana baza R^n u kojoj je ona dijagonalna sa svojstvenim vrijednostima na dijagonali. Označimo tu bazu sa $\{u = v_1, v_2, ..., v_n\}$ te pripadne svojstvene vrijednosti sa $\left\{\frac{\lambda_1}{d}, \frac{\lambda_2}{d}, ..., \frac{\lambda_n}{d}\right\}$.
Promotrimo sada rastav p na sumu uniformne distribucije u i ostatka e, tj. stavimo $e = p - u$. Suma koordinata u i p jednaka je 1 pa suma koordinata vektora e mora biti jednaka 0, stoga je $\langle u, e\rangle = 0$ pa se e nalazi u prostoru razapetom sa $\{v_2, ..., v_n\}$. Slijedi

$$\begin{aligned} Np - u &= N(e + u) - u \\ &= Nu - Ne - u \\ &= u + Ne - u \\ &= Ne. \end{aligned}$$

Koristeći činjenicu da je e linearna kombinacija ortonomiranih vektora, koji su ujedno svojstveni vektori matrice N s pripadnim svojstvenim vrijednostima manjim od λ, a zatim nejednakost trokuta, dobivamo

$$||Np - u||_2 = ||Ne||_2 \leq \frac{\lambda}{d}||e||_2 \leq \frac{\lambda}{d}||p||_2.$$

Zaključujemo da vrijedi

$$||N^k p - u||_2 \leq \left(\frac{\lambda}{d}\right)^k.$$

Cauchy-Schwarzovom nejednakošću slijedi tvrdnja teorema. □

4.2 Poboljšanja vjerojatnosnih algoritama

U ovom poglavlju proučit ćemo kako uz pomoć slučajne šetnje na grafu koji je ekspander možemo smanjiti broj slučajnih bitova potrebnih za izvršavanje vjerojatnosnih algoritama.
Pretpostavimo da imamo funkciju $f : \{0,1\} \to \{0,1\}$ te vjerojatnosni algoritam A takav da $\forall a \in \{0,1\}^n$ i x uniformno odabran iz $\{0,1\}^{p(|a|)}$ za neki polinom p vrijedi

$$\mathbf{P}(A(a,x) = f(a)) \geq \frac{2}{3}.$$

Voljeli bismo naći način kojim bismo vjerojatnost $A(a,x) = f(a)$ proizvoljno približili broju 1. Promotrimo prvi način na koji to možemo napraviti.
Najjednostavnija metoda za postizanje veće preciznosti algoritma A jest više puta generirati nezavisne $x \in \{0,1\}^{p(|a|)}$, recimo t puta, te kao konačnu odluku za $A(a,x)$ uzeti većinu među svim generiranim slučajevima. Označimo modificirani algoritam sa $A^*(a, x_1, ..., x_t)$. Uočimo da ako generiramo nezavisne $x_1, ..., x_t$, tada će naš modificirani algoritam biti netočan ako početni algoritam A pogriješi u više od pola slučajeva, odnosno kada

$$\sum_{k=1}^{t} Y_k > 0.5t,$$

pri čemu je $Y_k = 1_{A(a,x_k) \neq f(a)}$. Osim toga, vrijedi i

$$\mathbf{E}\left[\sum_{k=1}^{t} Y_k\right] = \sum_{k=1}^{t} \mathbf{E}[1_{A(a,x_k)\neq f(a)}] \leq \frac{1}{3}t.$$

Sada imamo

$$\begin{aligned}\mathbf{P}(A^*(a,x_1,...,x_t) \neq f(a)) &= \mathbf{P}\left(\frac{\sum_{k=1}^{t} Y_k}{t} \geq 0.5\right)\\ &\leq \mathbf{P}\left(\frac{\sum_{k=1}^{t} Y_k}{t} - \frac{\mathbf{E}[\sum_{k=1}^{t} Y_k]}{t} \geq 0.5 - \frac{1}{3}\right)\\ &= \mathbf{P}\left(\frac{\sum_{k=1}^{t} Y_k}{t} - \frac{\mathbf{E}[\sum_{k=1}^{t} Y_k]}{t} \geq \frac{1}{6}\right).\end{aligned}$$

Grešku algoritma A^* ograničavamo pomoću Leme 3.1.1. Koristeći navedenu lemu za naše slučajne varijable $Y_1, ..., Y_t$ dobivamo

$$\mathbf{P}\left(\frac{\sum_{k=1}^{t} Y_k}{t} - \frac{\mathbf{E}[\sum_{k=1}^{t} Y_k]}{t} \geq \frac{1}{6}\right) \leq e^{\frac{-t}{36}} \leq 2^{\frac{-t}{36}}.$$

Ako algoritam A koristi m slučajnih bitova, tada algoritam A^* koristi $O(mt)$ slučajnih bitova kako bi vjerojatnost greške smanjio na barem $2^{-O(t)}$.

Dokazat ćemo sada da jednaku grešku algoritma možemo postići i s manje slučajnih bitova. Najprije iskoristimo prethodno opisan A^* kako bismo vjerojatnost greške doveli na najviše $\frac{1}{100}$. Označimo potreban broj slučajnih bitova potrebnih za taj proces sa $r = O(m)$. Sada ćemo pomoću slučajne šetnje na prikladnom grafu koji je ekspander postići jednaku grešku algoritma, ali koristeći samo $O(t + r)$ slučajnih bitova.

Ključna će nam biti tvrdnja Teorema 1.2.13 za d-regularan graf G koji je (n, d, ϵ)-ekspander vrijedi $\frac{\lambda(G)}{d} \leq 1 - c$ za neki $c = \frac{\epsilon^2}{4+2\epsilon^2}$. Za graf $G = (V, E)$ na kojem ćemo promatrati slučajnu šetnju uzmimo 7-regularan graf sa 2^r vrhova opisan u [5]. Uvedimo oznaku $\lambda = \frac{\lambda(G)}{d}$. Kako bismo osigurali ogradu na vjerojatnost pogreške, bit će nam potrebno da vrijedi $\lambda \geq -1$. Budući da je G bipartitan, umjesto klasične slučajne šetnje, promatrat ćemo modificiranu šetnju u kojoj s vjerojatnošću $\frac{1}{2}$ ostajemo u trenutnom vrhu, a inače posjećujemo slučajnog susjeda trenutnog vrha.

Modificirana šetnja ima prijelaznu matricu $\frac{I+N}{2}$ te su njene svojstvene vrijednosti $\frac{1+\frac{\lambda}{d}}{2}$. Najveća svojstvena vrijednost po apsolutnoj vrijednosti ove šetnje ograničena je odozgo sa $q + \frac{c}{2}$, te odozdo sa 0.

Algoritam provodimo na sljedeći način. Neka je t najmanji prirodan broj takav da

$$\left(1 - \frac{c}{2}\right)^t \leq \frac{1}{10}.$$

Koristeći r slučajnih bitova, uniformno slučajno pronađimo početni vrh X_0 naše šetnje. Zatim provedimo modificiranu šetnju za $7tk$ koraka te označimo $X_{it} = Y_i$. Na kraju, za svaki $i = 1, ..., 7k$ provjerimo rezultat $A(a, Y_i)$ te prebrojimo dobivene bitove i kao konačan rezultat algoritma vratimo većinu od $7k$ promotrenih vrijednosti. Primijetimo da je ukupan broj slučajnih bitova koji su nam potrebni za algoritam jednak $r + t \log d$ jer što sa r bitova generiramo prvi vrh modificirane šetnje, moramo još t puta generirati jednog od d susjeda trenutnog vrha.
Označimo navedeni algoritam sa A^* i dokažimo da je vjerojatnost pogreške tog algoritma zaista manja od 2^{-k}.

Teorem 4.2.1. *[9] Neka je A^* vjerojatnosni algoritam opisan u tekstu iznad. Za njega vrijedi vrijedi*

$$\mathbf{P}(A^*(a, x) \neq f(a)) < 2^{-k}.$$

Dokaz. Sa $C \subseteq V$ označimo skup vrhova za koje algoritam vraća točnu vrijednost. Neka je S vektorski prostor $\mathbb{R}^s$, uz $s = 2^r$, koji predstavlja vjerojatnost da se nalazimo u nekim vrhovima. Sa W označimo potprostor razapet sa $p_0 = (2^{-r}, ..., 2^{-r})$ i neka je W' njegov ortogonalni komplement.
Uvedimo matricu $B = \left(\frac{I+N}{2}\right)^t$ te sa e_i označimo vektor iz S čija je i-ta koordinata jednaka 1, a ostale su 0. Neka je $Q : S \to S$ linearan operator zadan sa

$$Q(e_i) = \begin{cases} e_i, \text{ ako je } i \in V \setminus C \\ 0, \text{ inače} \end{cases}$$

Stavimo $M = I - Q$. Primijetimo da je B matrica stanja nakon t koraka modificirane šetnje. Ako je p vjerojatnosni vektor koji na i-tom mjestu sadrži vjerojatnost da se nalazimo u i-tom vrhu, tada Bp predstavlja vjerojatnost stanja naše šetnje nakon t koraka. Također, QBp predstavlja vjerojatnost da se nalazimo u nekom od stanja koje nije u C. Nizom z, koji se sastoji 0 i 1 duljine $7k$ označimo događaj da se u našoj šetnji i-ti vrh nalazio u C ako je $z_i = 1$, a u suprotnom je vrh pripadao skupu $V \setminus C$. Sada je na primjer vjerojatnost događaja da je točno prvih i elemenata niza $Y_1, ..., Y_{7k}$ bilo unutar C jednaka

$$\mathbf{P}(Y_i) = |\underbrace{(QB)...(QB)}_{i \text{ puta}} \underbrace{(MB)...(MB)}_{7t-i \text{ puta}} p_0|.$$

Dokažimo dvije korisne nejednakosti.

Tvrdnja 4.2.2. *Za $z \in S$ vrijedi*

1. $||MBz||_2 \leq ||z||_2$
2. $||NBz||_2 \leq \frac{||z||_2}{5}$

Dokaz. 1. Prema definiciji matrice M i činjenice da su svojstvene vrijednosti matrice B jednake $\left(\frac{1+\frac{\lambda_i}{d}}{2}\right)^t$, pa su zbog izbora t one omeđene sa 0 i $\frac{1}{10} \leq 1$ osim za $i = 1$ kada je svojstvena vrijednost jednaka 1. Tvrdnja sada slijedi jer je operatorska norma simetrične matrice jednaka njenoj svojstvenoj vrijednosti s najvećom apsolutnom vrijednosti.

2. Zapišimo $z = w + w'$ pri čemu je $w \in W$ i $w' \in W'$. Zbog $Bw = w$ i $|V \setminus C| \leq \frac{|V|}{100}$ dobivamo
$$||QBw||_2 \leq \frac{||w||_2}{10} \leq \frac{||z||_2}{10}.$$
Sve svojstvene vrijednosti matrice B, osim najveće, omeđene su sa 0 i $\frac{1}{10}$ pa imamo
$$||QBw'||_2 \leq ||Bw'||_2 \leq \frac{||w'||_2}{10} \leq \frac{||z||_2}{10}.$$
Konačno, prema nejednakosti trokuta vrijedi
$$||QBz||_2 \leq ||QBw||_2 + ||QBw'||_2 \leq \frac{||z||_2}{5}.$$

□

Zbog Cauchy-Schwarzove nejednakosti vrijedi $||z||_1 \leq 2^{\frac{s}{2}}||z||_2$ pa prethodna Lema povlači da ako je z niz vrhova modificirane šetnje, s barem $\frac{7k}{2}$ grešaka algoritma A među svojim vrhovima, vrijedi
$$\begin{aligned}\mathbf{P}(z) &\leq 2^{\frac{s}{2}}||(QB)^{\frac{7k}{2}}p_0||_2 \\ &\leq 2^{\frac{s}{2}}\left(\frac{1}{5}\right)^{\frac{7k}{2}}||p_0||_2 \\ &= 5^{\frac{-7k}{2}}.\end{aligned}$$
S obzirom na to da postoji 2^{7k} mogućih nizova z, imamo
$$\mathbf{P}(\exists z \text{ takav da } A \text{ griješi na barem pola vrhova šetnje}) \leq 2^{7k}5^{\frac{-7k}{2}} < 2^{-k}.$$

□

Bibliografija

[1] Noga Alon, *Eigenvalues and expanders*, Combinatorica **6** (1986), 83–96.

[2] Noga Alon i Yuval Roichman, *Random Cayley graphs and expanders*, Random Structures & Algorithms **5** (1994), br. 2, 271–284, https://onlinelibrary.wiley.com/doi/abs/10.1002/rsa.3240050203.

[3] Demetres Christofides i Klas Markström, *Expansion properties of random Cayley graphs and vertex transitive graphs via matrix martingales*, Random Structures & Algorithms **32** (2008), br. 1, 88–100, https://onlinelibrary.wiley.com/doi/abs/10.1002/rsa.20177.

[4] L. R. Ford i D. R. Fulkerson, *Maximal Flow Through a Network*, str. 243–248, Birkhäuser Boston, Boston, MA, 1987, ISBN 978-0-8176-4842-8, https://doi.org/10.1007/978-0-8176-4842-8_15.

[5] Ofer Gabber i Zvi Galil, *Explicit constructions of linear-sized superconcentrators*, Journal of Computer and System Sciences **22** (1981), br. 3, 407–420, ISSN 0022-0000, https://www.sciencedirect.com/science/article/pii/0022000081900404.

[6] W. Hoeffding, *Probability inequalities for sums of bounded random variables*, Journal of the American Statistical Association **58** (1963), br. 301, 13–30.

[7] Shlomo Hoory, Nathan Linial i Avi Wigderson, *Expander Graphs and Their Applications*, Bull. Amer. Math. Soc. **43** (2006), br. 04, 439–562, ISSN 0273-0979.

[8] R. Impagliazzo i D. Zuckerman, *How to Recycle Random Bits*, Proceedings of the 30th Annual Symposium on Foundations of Computer Science (USA), SFCS '89, IEEE Computer Society, 1989, str. 248–253, ISBN 0818619821, https://doi.org/10.1109/SFCS.1989.63486.

[9] _____, *How to recycle random bits*, 30th Annual Symposium on Foundations of Computer Science, 1989, str. 248–253.

[10] M. Krebs i A. Shaheen, *Expander Families and Cayley Graphs: A Beginner's Guide*, EBSCO ebook academic collection, Oxford University Press, USA, 2011, ISBN 9780199767113, https://books.google.hr/books?id=GVOcmY4-o-oC.

[11] Zeph Landau i Alexander Russell, *Random Cayley Graphs are Expanders: a Simple Proof of the Alon–Roichman Theorem*, Electr. J. Comb. **11** (2004).

[12] Alexander Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhäuser Basel, 1994, http://dx.doi.org/10.1007/978-3-0346-0332-4.

[13] Alexander Lubotzky, Ralph Phillips i Peter Sarnak, *Ramanujan graphs*, Combinatorica **8** (2017), 261–277.

[14] G. A. Margulis, *Explicit constructions of concentrators*, Probl. Peredachi Inf. **9** (1973), br. 4, 71–80, https://www.mathnet.ru/php/archive.phtmlwshow=paper&jrnid=ppi&paperid=925&option_lang=eng.

[15] P. Erdos N. Alon, J. Spencer, *The Probabilistic Method*, (2015).

[16] A. Nilli, *On the second eigenvalue of a graph*, Discrete Mathematics **91** (1991), br. 2, 207–210, ISSN 0012-365X, https://www.sciencedirect.com/science/article/pii/0012365X9190112F.

[17] M. Pinsker, *On the complexity of a concentrator*, 1973.

[18] Nikola Sandrić, *Teorija statističkog učenja*, https://meduza.carnet.hr/index.php/media/watch/20302, preuzeto 21.6.2023.

[19] J. P. Serre, *Linear representations of finite groups*, Springer, New York, 1977.

[20] Daniel A. Spielman, *Spectral and Algebraic Graph Theory*, 2019.

[21] Salil P. Vadhan, *Pseudorandomness*, Now Publishers Inc., Hanover, MA, USA, 2012, ISBN 1601985940.

[22] Zoran Vondraček, *Markovljevi lanci*, https://web.math.pmf.unizg.hr/~vondra/ml-p8.pdf, preuzeto 29.1.2023.

Sažetak

Cilj ovog rada je upoznati čitatelja s važnošću i raznim svojstvima ekspander grafova i slučajnih Cayleyevih grafova. Kroz prva poglavlja iznosimo i dokazujemo rezultate potrebne za glavni teorem ovog rada, Alon-Roichmanov teorem. Taj teorem omogućava nam konstrukciju slučajnih Cayleyevih grafova koju su s velikom vjerojatnosti ekspanderi. Za kraj, demonstriramo kako ekspander grafove možemo koristiti za smanjenje pogreške u nekim vjerojatnosnim algoritmima.

Summary

The focus of this thesis was to showcase the significance and remarkable properties of expander graphs, along with random Cayley graphs. In the initial chapters, we furnish the reader with all the necessary results to establish the central theorem of this thesis, namely, the Alon-Roichman theorem. This theorem provides us with an efficient tool for the successful generation of expander graphs. Afterwards, we elaborate on how expander graphs can be leveraged to minimize the quantity of random bits required in certain probabilistic algorithms.

Životopis

Rođen sam u Zagrebu 24. travnja 1998. godine. Po završetku Osnovne škole Malešnice 2013. godine, upisujem opći smjer Gimnazije Lucijana Vranjanina. Kroz prva dva razreda srednje škole te pohvale i osvojenog trećeg mjesta na B razini državnog natjecanja iz matematike, odlučujem se iduće dvije godine natjecati na A razini. Osim razvijanja matematičkih vještina zadnja dva razreda, osvajam redom treće i drugo mjesto na A razini natjecanja, brončanu medalju na natjecanju MYMC u trećem razredu, te plasman na Međunarodnu matematičku olimpijadu u četvrtom razredu, gdje 2017. godine osvajam počasnu pohvalu.
Nakon toga upisujem preddiplomski studij Prirodoslovno-matematičkog fakulteta u Zagrebu. Tijekom studija povremeno sudjelujem na studentskim natjecanjima kao što su Vojtech Jarnik te IMC. 2020. godine osvajam treću nagradu na natjecanju IMC poslije čega upisujem diplomski studij matematičke statistike na istom fakultetu. Godinu dana kasnije osvajam drugu nagradu na već spomenutom natjecanju IMC i time zaključujem poglavlje matematičkih natjecanja.