Sadržaj

Uvod

Od rada Leonharda Eulera o sedam Kenigsberških mostova (1736), koji slovi za prvi pisani rad u istoriji teorije grafova, teorija grafova je našla fundamentalne primene i odigrala značajnu ulogu u razvoju drugih nauka. Eulerova formula o odnosu broja čvorova, ivica i površi konveksnog poligona, koju su kasnije generalizovali Cauchy i L'Huillier, je imala veliki značaj u nastajanju algebarske topologije i topologije uopšte. U 19. veku, dok je Listing uvodio topologiju, Cayley je otpočeo proučavanje stabala (klase grafova), vođen rezultatima dobijenim posmatranjem odredjenih analitičkih formi nastalih iz diferencijalnog računa. Stabla su imala veliku primenu u teorijskoj hemiji. Naime, Cayley je povezao svoje rezultate o stablima sa tadašnjim rezultatima iz oblasti hemijske kompozicije. Korišćenje tehnika algebre uslovilo je zajednički razvoj teorije grafova i topologije. Upotreba tih tehnika u ovim oblastima, upotrebljena je u radu fizičara Gustava Kirchhoffa iz 1845, u kome je uspostavio čuvene Kirkohove zakone u strujnim kolima između napona i jačine struje.

I danas, teorija grafova ima sve značajniju primenu u drugim oblastima matematike, nauci i tehnologiji. Aktivno se koristi na različitim naučnim poljima: biohemija (genomi), elektronika (komunikacione mreže i teorija kodova), informatika (algoritmi i teorija izračunavanja) i operaciona istraživanja (planiranje). Kombinatorni metodi teorije grafova se koriste u dokazivanju fundamentalnih rezultata u drugim oblastima teorijske matematike. Pomenućemo samo neke skorašnje rezultate i aktuelne primene. Dokazivanjem egzistencije uparivanja ("matching") u određenim beskonačnim bipartitnim grafovima Miklós Laczkovich je dao pozitivan odgovor na čuveno pitanje Alfreda Tarskog (postavljeno 1925) o mogućoj kvadraturi kruga. Takođe je zanimljivo pomenuti da je Thomas konstruisao neizmerljiv podskup skupa realnih brojeva $\mathbb{R}$ u Lebegovom smislu, samo korišćenjem kombinatornih metoda na bipartitnim grafovima. Pomenimo i to da je Babai dokazao Nielson-Schreierovu teoremu o podgrupama slobodnih grupa, kao i druge rezultate iz te oblasti, korišćenjem Cayleyevih grafova i njegove leme o kontrakciji. U literaturi se može naći još mnogo primera primena u drugim delovima matematike [**?**, **?**].

Veoma su značajne primene u novijim istraživanjima iz oblasti kompjuterske biohemije. Korišćenjem algoritma za nalaženje minimalnog pokrivača skupa čvorova vrši se eliminacija nekih sekvenci koje dovode do konflikta, pri mutaciji DNK. Isti algoritam je koristila grupa informatičara predvođena Ericom Filiolom za simulaciju prenošenja virusa (worms) na velikim kompjuterskim mrežama. Takođe su dizajnirali optimalnu strategiju za zaštitu mreža od virusa u realnom vremenu. Zanimljivo je istaći da mreža GSM mobilne telefonije radi na samo četiri različite frekvencije, što je direktna posledica čuvene teoreme o četiri boje (formulisao je Francis Guthrie 1852). Dobro su poznate primene algoritama za bojenje grana u problemima planiranja (raspored časova) i korišćenje Hamiltonovih kontura u šahovskim problemima.

Teorija grafova se koristi u proučavanju molekularne hemije i fizike, jer graf predstavlja prirodni model za reprezentaciju molekula, gde čvorovi predstavljaju atome, a ivice veze među

atomima. Takođe se, socijalne mreže i konačni automati mogu formalizovati usmerenim grafovima. U ovim primenama proučavaju se svojstva grafova koji modeliraju topologiju atoma ili mere međusobni uticaj učesnika socijalne mreže.

Glavni zadatak predložene doktorske disertacije sastojao bi se u proučavanju fenomena na kvantnim sistemima za procesiranje i prenos informacija, kao i izučavanje bisimulacija na nedeterminističkim automatima tehnikama teorije grafova. Rezultati disertacije predstavljaju i doprinos teoriji integralnih i cirkularnih grafova. Takođe ćemo se osvrnuti na neke primene hemijskoj teoriji grafova i teoriji konkurencije.

Disertacija sadrži rezultate iz različitih matematičkih i oblasti koje pripadaju računarskim naukama: teorija grafova, kvantna informatika, teorija automata, teorija brojeva, spektralna teorija grafova, teorija algoritama, linearna algebra, teorija prostora i operatora itd...

Disertacija je bazirana na originalnim rezultatima autora koji su publikovani u vodećim međunarodnim časopisima, prvenstveno iz oblasti računarskih nauka i matematike, ali takođe sadrži i značajan broj rezultata koji se ovom prilikom prvi put pojavljuju.

Rad je podeljen u 4 glave:

1. Osnovni pojmovi i rezultati

2. Kvantna dinamika na cirkularnim topologijama

3. Parametri integralnih cirkularnih grafova i primene

4. Bisimulacije na nedeterminističkim automatima,

a svaka glava je podeljena na nekoliko sekcija, a sekcije na podsekcije.

Poslednjih godina je postignut veliki naučni napredak u opisivanju fenomena koji se javljaju u sistemima za prenos i procesiranje kvantnih informacija. Sa druge strane, klasa cirkularnih grafova ima značajne primene u projektovanju topologije ovih sistema, kao i drugih vrsta mreža (računarskih, telekomunikacionih) u paralelnom i distribuiranom računarstvu. Takođe, za opisivanje i praktičan rad sa njima neophodno je prikazati značajan broj svojstava cirkluranih grafova. Zato ćemo u prvoj glavi prezentovati osnovne pojmove i rezultate teorije grafova, kvantne mehanike i teorijske informatike, sa osvrtom na dinamiku kvantnih mreža tj. kvantnih šetnji na njima. U ovom delu ćemo takođe dati pregled skorašnjih rezultata iz teorije cirkularni i integralnih grafova. Predmet poslednje sekcije ove glave je uloga bisimulacija i njenih primena, pre svega u modeliranju ekvivalencija na automatima.

Predmet proučavanja druge glave predstavlja opisivanje fenomena kvantne dinamike na težinskim i netežinskim cirkularnim topologijama, pre svega imajući u vidu savršeni transfer stanja (eng. perfect state transfer, skraćeno PST).

U prvoj sekciji se opisuje problem egzistencije savršenog transfera kvantnih stanja na proizvoljnim kvantnim mrežama.

U drugoj sekciji dajemo potrebne i dovoljne uslove koji karakterizuju težinske cirkularne grafove sa PST, u terminima sopstvenih vrednosti matrice susedstva grafa. Ova sekcija je bazirana na novim rezultatima datim u [**?**] i oni predstavljaju nastavak i uopštenje rezultata iz [**?**]. Naime, pokazali smo da je dinamika kvantne mreže periodična ako i samo ako je količnik razlike bilo koja dva para sopstvenih vrednosti matrice susedstva racionalan. Prethodni uslov implicira da matrica susedstva mora imati celobrojne sopstvene vrednosti, odnosno da graf mora biti integralan. Zbog toga su integralni cirkularni grafovi potencijalni kandidati za modeliranje kvantnih mreža koje bi mogle imati PST između neka dva čvora u mreži. Pomenimo da se

u težinskim integralnim cirkularnim grafovima sa neparnim brojem čvorova ne javlja PST. U trećoj podsekciji ove sekcije, direktnom primenom prethodnih rezultata, karakterišemo grafove u klasi unitarnih Kejlijevih grafova (podklasa inegralnih cirkularnih grafova) u kojima se javlja PST.

U trećoj sekciji dajemo rešenje problema opšte karakterizacije integralnih cirkularnih grafova u kojima se javlja PST, što je i glavni rezultat sekcije. Klasa integralnih cirkularnih grafova sa svojstvom PST, kao i njihov spektar, opisana je u prve dve podsekcije. Rezultati iz ove sekcije su originalni i preuzeti su iz rada [**?**]. Kao posledica ovog rezultata, izračunato je savršeno kvantno rastojanje i određen broj integralnih cirkularnih grafova koji poseduju PST. Interesantno je uočiti da je broj integralnih cirkularnih grafova sa PST, asimptotski jednak broju integralnih cirkularnih grafova datog reda. U nastavku su konstruisane neke značajnije klase pomenutih grafova (broj čvorova grafa je proizvod prostih delioca, skup delioca grafa je dvoelementan, skup delioca grafa se sastoji samo od neparnih delioca, itd...). U trećoj podsekciji dajemo odgovor na interesantno pitanje Godsila [**?**], o tome da li su čvorovi u proizvoljnoj mreži, između kojih se odvija PST, uvek antipodalni (nalaze se na dijametru)? Na ovo pitanje dajemo negativan odgovor određivanjem dijametra svih integralnih cirkularnih grafova sa dvoelementnim skupom deliocima, a koji imaju PST.

Četvrta sekcija je posvećeno težinskim cirkularnim mrežama sa celobrojnim težinama. Motiv za proučavanje ovih kvantnih mreža je taj što se komunikaciona distanca na kojoj se PST ostvaruje može povećati na mrežama na kojima je sparivanje kubitova fiksno ali različito [**?**]. A to dalje znači da se ovakve mreže mogu modelirati težinskim grafovima i u tom slučaju je Hamiltonijan sistema jednak težinskoj matrici susedstva grafa. U ovom poglavlju predstavljamo nove klase težinskih cirkularnih grafova koji imaju PST. Štaviše, pokazujemo da postoji težinski integralnih cirkularnih grafova reda n koji ima PST ako i samo ako je n paran. Takođe, dajemo kompletnu karakterizaciju težinskih cirkularnih grafova sa PST, koji imaju dvoelementni skup delioca. Rezultati ovog poglavlja su preuzeti iz još uvek neobjavljenog rada [**?**].

Da bi se projektovala dobra kvantna mreža poželjno je znati što više parametara integralnih cirkularnih grafova, [**?**]. Inspirisani ovom činjenicom i otvorenim problemima datim u [**?**], tema trećeg dela disertacije sastojala bi se u nalaženju klike, hromatskog broja, dijametra i grupe automorfizama integralnih cirkularnih grafova. Rezultati izloženi u ovoj glavi su originalni i preuzeti iz naših radova [**?**, **?**, **?**, **?**].

U prvoj sekciji je izvršena karakterizacija bipartitnih integralnih cirkularnih grafova.

Tražeći maksimalan put koji informacija može potencijalno da pređe, u drugoj sekciji ispitujemo dijametar integralnih cirkularnih grafova. Gornja granica dijametra integralnih cirkularnih grafova je data u [**?**]. U radu [**?**] je poboljšana prethodno utvrđena granica i pokazano je da je asimptotska ocena dijametara najviše $O(\ln \ln n)$, pa su ovi rezultati priključeni ovom poglavlju.

U trećoj i četvrtoj sekciji izračunavamo veličinu klike i hromatskog broja integralnih cirkularnih grafova sa jednim i dva delioca, i dajemo gornju ocenu u opštem slučaju. Takođe pokazujemo da hipoteza postavljena u [**?**] da veličina klike i hromatskog broja dele red grafa, nije tačna. To činimo konstrukcijom klase grafova koji predstavljaju kontraprimere. Sekcije zaključujemo time što ćemo dati oštre gornje i donje granice za ova dva parametra, u opštem slučaju, za proizvoljni integralni cirkularni graf.

U petoj sekciji je kompletno određena grupa automorfizama unitarnih Kejlijevih grafova. Takođe izračunamo kardinalnost grupe automorfizam za specijalne strukture skupa delioca integralnih cirkularnih grafova, kada je red grafa stepen prostog broja ili proizvod prostih brojeva.

Centralno mesto četvrte glave disertacije zauzima razmatranje bisimulacija na nedeterminističkim automatima. Većina rezultata izložena u ovoj glavi je preuzeta iz [**?**]. Bisimulacije definisane na stanjima dva različita sistema su značajno manje proučavane, zbog nedostatka odgovarajućeg koncepta relacije između različitih skupova koja bi se ponašala kao ekvivalencija, tj. modelirala je. U najvećem broju slučajeva predloženi koncept simulacija se zasnivao ili na relacijama (što se ispostavilo kao suviše uopšten koncept) ili na funkcijama (što se sa druge strane ispostavilo kao suviše specijalan).

Za razliku od predhodnih konceptata, u predloženoj disertaciji važno mesto imao bi koncept uniformnih relacija uvedenih u [**?**], što će biti predmet druge sekcije.

U trećoj sekciji definišemo pojam nedeterminističkog automata i pri tome navidimo neke tipove automata bazirane na sličnim koneptima.

U četvrtoj sekciji definišemo četiri vrste relacija između nedeterminističkih automata: direktna (forward), povratna (backward), direktna-povratna (forward-backward) i povratna direktna (backward-forward) bisimulacija.

U petoj sekciji su ispitana svojstva ovih relacija koje su uniformne. Može se pokazati da uniformna relacija ϕ definisana na stanjima nedeterministiǩih automata A i B je direktna bisimlacija ako i samo ako su jezgro i kojezgro ove realacije takođe direktne bisimulacione ekvivalencije. Realacija ϕ indukuje i izomorfizam između odgovarajućih faktora automata pomenutih ekvivalencija [**?**].

U šestoj sekciji smo pokazali da su dva automata A i B UFB-ekvivalentna (postoji uniformna direktna bisimulacija definisana na $A \times B$) ako i samo ako su odgovarajući faktor automati, u odnosu na najveću direktnu bisimulacionu ekvivalenciju, izomorfni. Direktne i povratne bisimulacione ekvivalencije nedeterminističkog automata su zapravo desno i levo invarijantne ekvivalencije, korišćene u [**?**, **?**, **?**] za redukciju nedeterminističkih automata.

U nastavku glave dajemo odgovarajuće rezultate za uniformne povratne-direktne bisimulacije i slabe direktne bisimulacije. Napomenimo i to da se koncept bisimulacija može "fazifikovati" i uopštiti na fazi i težinskim automatima [**?**, **?**]. U tom slučaju bi se moglo dokazati da su fazi automati A i B UFB-ekvivalentni ako i samo ako postoji odgovarajući izomorfizam između faktor fazi automata u odnosu na najveću bisimulacionu fazi ekvivalenciju na A i B. Uniformne fazi realcije se takođe mogu primeniti na proučavanje ekvivalencija između determinističkih fazi prepoznavača [**?**, **?**] i samo za ovu vrstu automata važi da jezička ekvivalencija može biti modelirana strukturalnom.

U petoj glavi dajemo izvorni MATHEMATICA kod za određivanje energija integralnih cirkulantnih grafova i generisanje integralnih cirkularnih grafova sa PST, kao i Java kod za izračunavanje nekih parametara grafa kao što je dijametar, komponente povezanosti, klika i hromatski broj.

Na kraju, želim da izrazim zahvalnost komentorima, profesorima Miroslavu Ćiricu i Draganu Stevanoviću, na savremenoj i interesantoj tematici u koju su me uputili i na pomoći i izdojenom vremenu koje su mi tokom izrade ove disertacije posvetili. Takođe želim da se zahvalim svojoj porodici i svim prijateljima koji su mi, prilikom izrade disertacije, pružili neophodno razumevanje.

Glava 1

Osnovni pojmovi i rezultati

U ovoj glavi dajemo formalne matematičke definicije pojmova koje koristimo u tezi, a koje predstavljaju osnov za razmatranje pojmova kvantne mehanike. Zadržaćemo se, pre svega, na elemente osnova kvantne mehanike koji su od interesa za oblast kvantne informatike. Za razumevanje sadržaja osnovnih postulata neophodno je predznanje osnova Hilbertovog prostora, tj. potrebno je upoznati se sa fizičarskom notacijom i interpretacijom stanja faznih postora elementima Hilbertovog prostora. Kako je dinamika kvantnog sistema modelirana grafom (i njegovom matricom susedstva), najpre dajemo neke osnovne formalizme teorije grafova koji će biti od važnosti u daljim razmatranima. U poslednjoj sekciji hronološki opisujemo motivaciju za uvođenje bisimulacija na tranzicionim sistemima.

1.1 Formalne definicije teorije grafova

Na početku dajemo neke osnovne definicije iz teorije grafova (pratimo knjige [**?**, **?**, **?**, **?**, **?**]).

Definicija 1.1.1. *Graf G (eng. graph) je uređeni par (V, E), gde je $E \subseteq \binom{V}{2}$ (skup svih dvoelementnih podskupova skupa V). Elementi skupa V se zovu čvorovi (eng. vertex), a elementi skupa E grane (eng. edge) grafa G. Graf $G = (V, E)$ je usmeren ili digraf, ako su grane usmerene tj. $e = u \to v$. Multigraf je specijalna vrsta grafa, kada je dozvoljeno više različitih grana koje spajaju dva čvora, kao i grane koje spajaju čvor sa samim sobom.*

U tezi se ćemo najčešće razmatrati neorijentisane grafove bez petlji i višestrukih grana (prosti grafovi), ali ćemo se u 4. glavi osvrnuti kako na orjentisane grafove, tako i multigrafove.

Definicija 1.1.2. *Dva čvora grafa u i v su susedna ako su spojena granom $e = uv$. Pod okolinom čvora $v \in V$ grafa $G = (V, E)$ (eng. neighborhood) podrazumeva se skup $N(v) = \{u \in V : vu \in E\}$ suseda čvora v. Stepen čvora v (eng. degree) je broj suseda čvora v, $deg(v) = |N(v)|$. Najmanji stepen grafa G je $\delta = \min_{v \in V} deg(v)$, a najveći stepen grafa G je $\Delta = \max_{v \in V} deg(v)$.*

Definicija 1.1.3. *Graf $G' = (V', E')$ je podgraf (eng. subgraph) grafa $G = (V, E)$, ako važi $V' \subseteq V$ i $E' \subseteq E \cap \binom{V'}{2}$. Graf $G' = (V', E')$ je indukovani podgraf (eng. induced subgraph) grafa $G = (V, E)$, ako važi $V' \subseteq V$ i $E' = E \cap \binom{V'}{2}$.*

Itnuitivno jasne pojmove puta, ciklusa i rastojanja između čvorova, definisaćemo precizno.

Definicija 1.1.4. *Šetnja (eng. walk) W dužine k u grafu G je niz $v_0, e_1, v_1, e_2, v_2, \ldots, e_k, v_k$ čvorova i grana tako da je $e_i = v_{i-1}v_i$ za $i = 1, 2, \ldots, k$. Čvorovi v_0 i v_k su krajnji čvorovi šetnje W. Šetnja je zatvorena ukoliko je $v_0 = v_k$. Staza (eng. trail) je šetnja u kojoj se nijedna grana ne ponavlja. Put (eng. path) je šetnja u kojoj se nijedan čvor ne ponavlja. Ciklus (eng. cycle) je zatvorena staza u kojoj se nijedan čvor ne ponavlja, izuzev prvog i poslednjeg.*

Čvorovi u i v grafa G su povezani ako u G postoji put čiji su krajnji čvorovi baš u i v. Za graf G kažemo da je *povezan* (eng. connected) ako su svaka dva njegova čvora povezana - u suprotnom je graf nepovezan i može se podeliti na komponente povezanosti.

Definicija 1.1.5. *Ako su čvorovi u i v grafa G povezani, tada je rastojanje $d(u, v)$ od čvora u do čvora v jednako dužini najkraćeg puta između čvorova u i v. Ekscentricitet čvora v je jednak maksimalnom rastojanju od v do svih ostalih čvorova $\varepsilon(v) = \max_{u \in V} d(u, v)$. Dijametar grafa G je najveće rastojanje između neka dva čvora grafa $D(G) = \max_{u,v \in V} d(u, v)$, dok se radijus grafa G definiše kao najmanji ekscentricitet među čvorovima $r(G) = \min_{v \in V} \varepsilon(v)$.*

Čvorovi minimalnog ekscentriciteta formiraju centar grafa. Stablo ima jedan ili dva centralna čvora (u drugom slučaju govorimo o bicentru). Tada važi

$$D(T) = \begin{cases} 2r(T) - 1 & \text{ako } T \text{ ima bicentar} \\ 2r(T) & \text{ako } T \text{ ima centar.} \end{cases}$$

Graf G je r-regularan, $r \in N$, ako je stepen svakog čvora jednak r, tj. $\delta = \Delta = r$. *Kompletan graf* sa n čvorova (eng. complete graph) je graf K_n, $n \in N$, sa skupom čvorova $\{1, 2, \ldots, n\}$, i za svako $1 \leq i, j \leq n$ važi $\{i, j\} \in E$. Graf $G = (V, E)$ je *bipartitan* (eng. bipartite graph) ako postoji particija $\{A, B\}$ skupa čvorova $V = A \cup B$, $A \cap B = \emptyset$, tako da za svaku granu $e \in E$ važi da ona spaja čvor iz A sa čvorom iz B. Graf G je *planaran* (eng. planar) ako se može nacrtati u ravni, tako da se nikoje dve grane ne seku.

Definicija 1.1.6. *Uniju grafova $G_1 = (V_1, E_1)$ i $G_2 = (V_2, E_2)$ definišemo kao graf $G_1 \cup G_2 = (V_1 \cup V_2, E_1 \cup E_2)$. Spajanje (eng. join) grafova $G_1 \vee G_2$ se dobija od grafa $G_1 \cup G_2$, tako što spojimo granom svaki čvor iz grafa G_1 sa svakim čvorom iz G_2. Komplement $\overline{G}$ grafa $G = (V, E)$ je graf $\overline{G} = \left(V, \binom{V}{2} \setminus E\right)$, dakle on sadrži tačno one grane koje graf G nema.*

Definicija 1.1.7. *Neka je G prost graf, $v \in V$ proizvoljan čvor i $e = uv$ proizvoljna grana. Graf $G' = G - v$ je dobijen brisanjem čvora v i svih grana koje su susedne sa njim. Graf $G - e$ dobijamo kada iz grafa G uklonimo granu $e = uv$.*

Definicija 1.1.8. *Povezan graf bez ciklusa naziva se stablo (eng. tree). Graf koji ne sadrži cikluse, tj. graf čija je svaka komponenta povezanosti stablo, naziva se šuma (eng. forest). Čvor stepena 1 u grafu G naziva se list ili viseći čvor (eng. leaf ili pendant vertex).*

Stabla imaju višestruku primenu u različitim oblastima nauke (pri parsiranju, kompresiji, za sortiranje i pretraživanje podataka). Svako stablo možemo nacrtati, tako što fiksiramo koren stabla, a zatim crtamo sve njegove direktne susede u sledećem nivou, pa onda susede na rastojanju 2 u sledećem nivou i tako dalje. Ovo se radi algoritmom pretrage u širinu (eng. Breadth First Search). Kako do svakog čvora postoji jedinstven put od korena, dubinu stabla definišemo kao najveće rastojanje od korena do ostalih čvorova. Vrlo važna struktura podataka u programiranju je korensko binarno stablo, gde svaki čvor ima najviše dva potomka.

Definicija 1.1.9. *Razapinjuće stablo $T = (V, E')$ (eng. spanning tree) je podgraf grafa $G = (V, E)$, koji je stablo i sadrži sve čvorove i neke njegove grane, tj. $E' \subseteq E$.*

Za dva grafa sa istim brojem čvorova, koji su povezani "na isti način" kažemo da su izomorfna (eng. isomorphic).

Definicija 1.1.10. *Grafovi G i H sa skupom čvorova $V = \{1, 2, \ldots, n\}$ su izomorfni, ako postoji permutacija tj. bijekcija $p : V \to V$ čvorova V, tako da je $(u, v) \in E(G)$ ako i samo ako je $(p(u), p(v)) \in E(H)$. Tada pišemo $G \cong H$.*

Definicija 1.1.11. *Graf je unicikličan ako je povezan i sadrži tačno jedan ciklus, odnosno $n+1$ granu. Graf je bicikličan ako je povezan i sadrži tačno dva ciklusa, odnosno $n + 2$ grane.*

Sada ćemo definisati još neke složenije grafovske invarijante.

Definicija 1.1.12. *Graf G je k-povezan, ako ne postoji skup od $k - 1$ čvorova čijim se uklanjanjem graf raspada na nekoliko komponenti (odnosno čvorna povezanost je $\geq k$). Čvor $v \in V$ grafa G se naziva artikulacioni čvor (eng. articulation vertex) ako $G - v$ ima više komponenti povezanosti od G. Grana $e \in E$ grafa G se naziva most (eng. bridge), ako $G - e$ ima više komponenti povezanosti od G.*

Prema tome, povezani graf je 1-povezan, a 2-povezani graf (eng. biconnected graph) ne sadrži artikulacioni čvor.

Definicija 1.1.13. *Skup čvorova S u grafu G je nezavisan, ako nikoja dva čvora iz S nisu povezana granom. Broj nezavisnosti $\alpha(G)$ je maksimalna veličina nezavisnog skupa grafa G.*

Definicija 1.1.14. *Uparivanje M je skup nesusednih grana grafa G – nikoje dve grane ne dele zajednički čvor. Maksimalno uparivanje je uparivanje sa najvećim brojem grana, dok je uparivajući broj upravo veličina maksimalnog uparivanja. Čvor v je uparen ako je incidentan sa granom koja je u uparivanju; inače je čvor neuparen. Čvor je* perfektno uparen *ako je uparen u svim maksimalnim uparivanjima grafa G.*

Linearni algoritam za konstruisanje najvećeg uparivanja u stablu je grabljiv i zasnovan na matematičkoj indukciji. Naime, uzmemo proizvoljan list v i uparimo ga sa njegovim roditeljem w. Oba čvora uklonimo iz stabla i preostali deo rešavamo indukcijom. Za više detalja o implementaciji videti [**?**]. Lako se pokazuje da ukoliko stablo ima savršeno uparivanje, tada je ono jedinstveno.

Definicija 1.1.15. *Hromatski broj grafa G je najmanji broj boja $\chi(G)$ potrebnih da se oboje čvorovi grafa G, tako da nikoja dva susedna čvora nemaju istu boju – odnosno najmanja vrednost χ, za koju je graf χ-obojiv. Klika broj grafa G predstavlja veličinu najvećeg kompletnog pografa (klike) grafa G i označava se sa $\omega(G)$.*

Iz definicije direktno sledi nejednakost $\chi(G) \geq \omega(G)$. Da ne bi došlo do terminološke konfuzije između pojmova klike i klika broja, u ostatku teze ćemo za klika broj koristiti sintagmu, veličina maksimalne klike.

Grafovi se obično predstavljaju grafički crtanjem tačke za svaki čvor i linije između dva čvora koji su susedni. Postoji mnogo načina da se graf predstavi u memoriji računara. Struktura podataka koja se koristi zavisi od osobina grafa i algoritma koji primenjujemo. Teoretski se mogu razlikovati dinamičke i matrične strukture, ali se u praksi koriste u kombinaciji. Ukoliko

se koristi *lista suseda* (eng. neighbor list), tada za svaki čvor v čuvamo listu čvorova koji su susedni sa njim. Ukoliko se radi o *matrici susedstva* (eng. adjacency matrix) - tada se koristi matrica A dimenzija $n \times n$, gde je n broj čvorova u grafu. Element a_{ij} je jednak broju grana koje polaze iz čvora i, a završavaju se u čvoru j. Kod težinskih grafova na polju (i, j) se nalazi težina grane koja povezuje čvorove i i j. Ako je graf prost i neusmeren, matrica je simetrična sastavljena samo od 0 i 1, a na glavnoj dijagonali se nalaze nule.

Tehnike iz teorije grupa i linearne algebre su nezamenljive u proučavanju strukture i enumeracije grafova.

Definicija 1.1.16. *Sopstvena vrednost (eng. eigenvalue) matrice A je realan broj λ, ako matrična jednačina*

$$A \cdot \mathbf{x} = \lambda \cdot \mathbf{x}$$

ima netrivijalno rešenje, koje nazivamo sopstveni vektor (eng. eigenvector). Sopstvene vrednosti grafa su sopstvene vrednosti matrice susedstva.

Spektar grafa (eng. graph spectrum) je skup sopstvenih vrednosti matrice susedstva, zajedno sa njihovim algebarskim višestrukostima. Skup svih sopstvenih vektora operatora A za sopstvenu vrednost λ, zajedno sa nula vektorom, u oznaci V_λ, naziva se sopstveni potprostor za λ. Višestrukost za sopstvenu vrednost λ je jednaka $n - \text{rang}(\lambda I - A)$. Ako su različite sopstvene vrednosti matrice A takve da važi $\lambda_1 > \lambda_2 > \ldots > \lambda_k$, a njihove višestrukosti $m(\lambda_1), m(\lambda_2), \ldots, m(\lambda_k)$, tada spektar grafa označavamo sa:

$$Spec_G = \begin{pmatrix} \lambda_1 & \lambda_2 & \ldots & \lambda_k \\ m(\lambda_1) & m(\lambda_2) & \ldots & m(\lambda_k) \end{pmatrix}$$

Sopstvene vrednosti $\lambda_1, \lambda_2, \ldots, \lambda_n$ su nule karakterističnog polinoma (eng. characteristic polynomial) matrice A

$$P(x; A) = \det(xI - A) = (-1)^n \det(A - xI) = \prod_{i=1}^{n} (x - \lambda_i).$$

Kako je $P(x; A)$ moničan polinom sa celobrojnim koeficijentima, sve njegove racionalne nule su celobrojne – pa su sopstvene vrednosti matrice susedstva ili iracionalne ili celobrojne. U radu ćemo označavati sa $P(x; G)$ karakteristični polinom matrice susedstva grafa G. Ako je dat moničan polinom, vrlo je teško odrediti da li je on karakterističan polinom nekog grafa. Dva grafa su *kospektralna* ako njihove matrice susedstva imaju iste sopstvene vrednosti. Kospektralni grafovi ne moraju da budu izomorfni, ali su izomorfni grafovi uvek kospektralni.

O sopstvenim vrednostima matrica i operatora biće više reči u narednom odeljku.

1.2 Hilbertovi prostori i operatori na njemu

U ovoj sekciji ćemo navesti osnovne definicije i poznata svojstva Hilbertovih prostora (bez dokaza), koja su od važnosti za razumevanje kvantno-mehaničkih pojava. Više o ovoj temi može se naći, na primer u [**?**, **?**].

Definicija 1.2.1. *Skalarni proizvod na kompleksnom prostoru X je funkcija $s : X \times X \to \mathbb{C}$ koja zadovoljava sledeće uslove:*

$$\begin{aligned} s(\lambda_1 x_1 + \lambda_2 x_2, y) &= \lambda_1 s(x_1, y) + \lambda_2 s(x_2, y), && (1.1)\\ s(x, \lambda_1 y_1 + \lambda_2 y_2) &= \overline{\lambda_1} s(x, y_1) + \overline{\lambda_2} s(x, y_2), && (1.2)\\ s(x, y) &= \overline{s(y, x)}, && (1.3)\\ s(x, x) &= 0 \text{ ako i samo ako je } x = 0. && (1.4) \end{aligned}$$

za svako $x, y, x_1, y_1, x_2, y_2 \in X$ i $\lambda_1, \lambda_2 \in \mathbb{C}$.

Vektorski prostor X sa skalarnim proizvodom s, odnosno uređeni par (X, s) naziva se *unitarni prostor* (*pre-Hilbertov*).

Definicija 1.2.2. *Neka je X vektorski prostor nad poljem $\mathbb{C}$. Funkcija $x \mapsto \|x\|$ koja slika X u $\mathbb{R}$ naziva se norma za X, ako zadovoljava sledeće uslove*

$$\begin{aligned} \|x\| &\geq 0, && (1.5)\\ \|x\| &= 0 \text{ ako i samo ako je } x = 0, && (1.6)\\ \|\lambda x\| &= |\lambda| \|x\|, && (1.7)\\ \|x + y\| &= \|x\| + \|y\|, && (1.8) \end{aligned}$$

za svako $x, y \in X$ i $\lambda \in \mathbb{C}$.

Definicija 1.2.3. *Normirani prostor (normirani vektorski prostor) je par $(X, \|\cdot\|)$, gde je X vektorski prostor, a $x \mapsto \|x\|$ norma za X.*

Ukoliko je X normirani vektorski prostor i dimenzija vektorskog prostora X konačna (beskonačna), tada se kaže da je prostor *konačno-dimenzionalan* (*beskonačno-dimanzionalan*) prostor. Za X se kaže da je *separabilan* ako je baza prostora prebrojiva.

Definicija 1.2.4. *Neka je X normiran prostor i d funkcija koja slika $X \times X$ u $\mathbb{R}$, definisana sa*

$$d(x, y) = \|x - y\|,$$

za svako $x, y \in X$. Za funkciju d kaže se da je metrika definisana normom ili da je prirodna metrika na normiranom prostoru. Uređeni par (X, d) je metrički prostor.

Normirani prostor X naziva se kompletnim ako je svaki Košijev niz konvergentan. Napomenimo da je niz Košijev ako je

$$\|x_n - x_m\| \to 0, \ (m, n \to \infty).$$

Definicija 1.2.5. *Normiran prostor X je Banahov prostor ako je (X, d) kompletan metrički prostor, gde je d metrika definisana normom.*

Definicija 1.2.6. *Neka je X unitarni prostor. Za normu*

$$\|x\| = s(x, x)^{1/2}, \ x \in X$$

kaže se da je norma definisana skalarnim proizvodom.

Ako je unitarni prostor X Banahov, tada se za X kaže da je Hilbertov.

Podsetimo da je prostor X kompaktan ako svaki otvoreni pokrivač prostora X ima konačni podpokrivač.

U kvantnoj mehanici se pod Hilbertovim prostorom podrazumeva, u opštem slučaju beskonačno-dimenzionalni separabilni Hilbertov prostor.

Element x Hilbertovog prostora X se označava sa $|x\rangle$-*Dirakova notacija*. Takođe, transponovano-konjugovani vektor, vektora x se označava sa $\langle x|$. Koristeći ovako uvedenu notaciju, prirodno se skalarni proizvod vektora x i y označava sa, $s(x,y) = \langle x|y\rangle$.

Neka je dat indeksni skup I. *Bazis (baza)* vektorskog prostora X predstavlja maksimalni skup vektora $\{|v_i\rangle\}_{i\in I}$ koji zadovoljava

$$\sum_{i\in I} \alpha_i |v_i\rangle = 0 \Rightarrow \alpha_i = 0, \quad \text{za svako } i \in I.$$

Ortonormirani bazis je skup vektora baze, gde za svaka dva vektora iz ovog skupa važi uslov ortonormiranosti:

$$\langle v_i|v_j\rangle = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

Svaki element prostora se jednoznačno razlaže po datom ortonormiranom bazisu:

$$|x\rangle = \sum_{i\in I} \xi_i |v_i\rangle, \ \xi_i = \langle v_i|x\rangle. \tag{1.9}$$

Normu vektora $|x\rangle$ definišemo kao

$$\||x\rangle\| = \sqrt{\langle x|x\rangle} = \sqrt{\sum_{i\in I} |\xi_i|^2}.$$

Konjugovano-transponovani vektor od $|x\rangle$, u oznaci $|x\rangle^\dagger$, se u Dirakovoj notaciji označava kao $\langle x|$ i ima razlaganje:

$$|x\rangle^\dagger = \langle x| = \left(\sum_{i\in I} \xi_i |v_i\rangle\right)^\dagger = \sum_{i\in I} \xi_i^* |v_i\rangle.$$

Sa ξ_i^* smo označili konjugovano-kompleksni broj, broja ξ_i. Ako je $|y\rangle = \sum_{i\in I} \eta_i |v_i\rangle$ razlaganje vektora $|y\rangle$ u bazi $\{|v_i\rangle\}_{i\in I}$, onda skalarni proizvod dva vektora ima oblik:

$$\langle x|y\rangle = \sum_{i\in I} \xi^* \eta_i.$$

U narednim pasusima uvodimo definiciju linearnog operatora i dajemo osnovna svojstva. Pri tome nećemo koristiti Dirakovu notaciju zbog jasnoće izlaganja, osim tamo gde to nije neophodno.

Neka su X i Y vektorski prostori dati nad istim poljem skalara $\mathbb{K}$. Preslikavanje $A : X \to Y$ koje zadovoljava uslove aditivnosti i homogenosti:

$$\begin{aligned} A(x+y) &= A(x) + A(y) \\ A(\lambda x) &= \lambda A(x), \end{aligned}$$

za svako $x, y \in X$ i $\lambda \in \mathbb{K}$, naziva se *linearnim preslikavanjem* ili *linearnim operatorom*. Ako je $X = Y$ tada A nazivamo linearni operator (ili samo operator) prostora X (*endomorfizam prostora* X) i zapisujemo $A \in End(X)$.

Definicija 1.2.7. *Neka je A linearni operator na datom vektorskom prostoru V nad poljem $\mathbb{K}$. Proizvoljan vektor $x \in V \setminus \{0\}$ za koji postoji $\lambda \in \mathbb{K}$ takav da je*

$$A(x) = \lambda x$$

naziva se sopstveni vektor operatora A. Skalar $\lambda \in \mathbb{K}$ za koji je ispunjena ova jednakost naziva se sopstvena vrednost operatora A odgovarajuća sopstvenom vektoru x. Skup svih sopstvenih vrednosti operatora A naziva se spektar operatora A.

Neka je X unitarni vektorski prostor. Za operator $A \in End(X)$ definišemo operator $A^\dagger$ tako da za proizvoljne $x, y \in X$ važi

$$s(A(x), y) = s(x, A^\dagger(y)).$$

Lako se proverava da je $A^\dagger \in End(X)$ i da je jedinstveni endomorfizam od X za koji važi prethodna relacija. Operator $A^\dagger$ nazivamo *adjungovanim operatorom* operatora A. U oznakama Dirakove notacije, poslednju jednakost možemo zapisati kao

$$\langle x|A|y\rangle = \langle x|A^\dagger|y\rangle.$$

Za operator A na unitarnom vektorskom prostoru X kažemo da je ermitski ako je $A = A^\dagger$, tj. ako je

$$s(A(x), y) = s(x, A(y)),$$

za svako $x, y \in X$.

Sada možemo navesti glavni rezultat za ermitske operatore bez dokaza:

Propozicija 1.2.1. *Za operator A na unitarnom prostoru X, sledeći uslovi su ekvivalentni:*

i) A je ermitski;

ii) Spektar operatora A je realan i A se može dijagonalizirati u ortonormiranoj bazi za X sastavljenoj od sopstvenih vektora od A;

iii) $\langle x|A|x\rangle \in \mathbb{R}$ za svaki $x \in X$.

Neka su M i N potrostori unitarnog prostora X. Tada

$$Z = M + N = \{x + y \mid x \in M, y \in N\}$$

označava *sumu potprostora* M i N. Ako je $M \cap N = \{0\}$, kaže se da je Z direktna suma potprostora M i N, i u tom slučaju koristi se oznaka

$$Z = M \oplus N.$$

Ako je $Z = M \oplus N$, kaže se da je potprostor N *algebarski komplement* potprostora M. Poznato je da u vektorskom prostoru X svaki potprostor ima komplement.

Za preslikavanje $P : X \to X$ kaže se da je *idenpotent* ako je $P^2 = P$. Linearni idenpotent naziva se *(algebarski) projektor*. Identičko preslikavanje I predstavlja *trivijalni projektor*. Za svaki projektor prostori

$$\begin{aligned} R(P) &= \{P(x) \mid x \in X\} \\ N(P) &= \{x \in X \mid P(x) = 0\} \end{aligned}$$

su algebarski komplementi, tj. P određuje razlaganje prostora X na direktnu sumu

$$X = R(P) \oplus N(P).$$

Potprostori $R(P)$ i $N(P)$ nazivaju se redom, *slikom* i *jezgrom* operatora P.

Sa druge strane, svaka direktna suma potprostora X određuje projektor. Naime, ako je $X = M \oplus N$, tada se svako $x \in X$ može jednoznačno prikazati kao $x = x_1 + x_2$, gde je $x_1 \in M$ i $x_2 \in N$. Preslikavanje $P : X \to X$, definisano sa $P(x) = x_1$ je projektor i $R(P) = M$ i $N(P) = N$. Kaže se da je P *projektor na* M *paralelno* N.

Neka je sada X Hilbertov prostor i M zatvoren potprostor u X. Tada se skup $M^\perp = \{y \in X \mid (\exists x \in X)\ \langle x|y\rangle = 1\}$ naziva *ortogonalni komplement* skupa M. Na osnovu poznate teoreme o ortogonalnoj dekompoziciji imamo da za svako $z \in X$ postoje jedinstveno određeni vektori $x \in M$ i $y \in M^\perp$ takvi da je $z = x + y$. Prema tome imamo da je

$$X = M \oplus M^\perp,$$

i ova direktna suma naziva se *ortogonalna suma*. Kako važi ovakvo razlaganje, to projektor $P : X \to M$ nazivamo *ortogonalan projektor na* M. U Hilbertovom prostoru X za projektor P imamo da je ortogonalan ako i samo ako je ermitski.

Dakle, jednoznačno pridruživanje ortogonalnih projektora i ortogonalnih prostora (na koje se oni projektuju) H_n, definiše jedno razlaganje Hilbertovog prostora X, na međusobno ortogonalne prostore H_n, što se u kvantnoj mehanici označava:

$$X = \bigoplus_n H_n.$$

Neka je X unitarni prostor i A ermitski operator na njemu. Ako su $\lambda_1, \lambda_2, \ldots, \lambda_k$ različite sopstvene vrednosti od A, $S_i(A)$ sopstveni potprostori koji redom odgovaraju vrednostima λ_i i P_i ortogonalni operatori potprostora $S_i(A)$, redom. Tada važi:

$$\begin{aligned} A &= \sum_{i=1}^{k} \lambda_i P_i \text{ spektralna dekompozicija operatora } A; \\ I &= \sum_{i=1}^{k} = P_i \text{ rezolucija identičkog operatora indukovana sa } A. \end{aligned}$$

Ako su $|x_1^{(i)}\rangle, |x_2^{(i)}\rangle, \ldots, |x_l^{(i)}\rangle$ vektori baze potprostora $S_i(A)$, za neko $1 \leq i \leq k$, tada odgovarajući projektor ima oblik zbira "dijada":

$$P_i = \sum_{j=1}^{l} |x_j^{(i)}\rangle\langle x_j^{(i)}|.$$

Neka je $|v_1\rangle, |v_2\rangle, \ldots, |v_k\rangle$ konačna baza unitarnog prostora. Svaki operator se zadaje delovanjem na neki ortonormirani bazis:

$$A(|v_i\rangle) = u_i = \sum_{j=1}^{k} a_{ji}|v_j\rangle,$$

gde matrični elementi $a_{ji} = \langle v_j|A|v_i\rangle$, *daju matričnu reprezentaciju operatora* u datom ortonormiranom bazisu. Zato identifikujemo (uspostavljamo izomorfizam između skupa operatora i skupa kvadratnih matrica, čiji je red dimenzija vektorskog prostora. Ermitski operatori se, na primer, reprezentuju ermitskim matricama za koje važi $a_{ij} = a^*_{ji}$, dok su dijagonalni elementi a_{ii} realni brojevi.

Zbir dijagonalnih elemenata matrice reprezentacije operatora ne zavisi od izbora bazisa u kojem se operator reprezentuje, i naziva se *trag operatora*, a označava se sa

$$trA = \sum_{i=1}^{n} \langle v_i|A|v_i\rangle.$$

Operator A u reprezentaciji sopstvenog bazisa postaje dijagonalna matrica, gde su dijagonalni elementi sopstvene vrednosti opearatora A.

Unitarni operator U definisan je izrazom

$$UU^\dagger = U^\dagger U = I,$$

tj. $U^\dagger = U^{-1}$, gde U^{-1} predstavlja operator inverzan u odnosu na operator U. Svaki unitarni operator se može predstaviti u obliku:

$$U = \exp(\imath\alpha A),$$

gde je α realan broj, a operator A ermitski. Na osnovu spektralne dekompozicije ermitskih opearatora, imamo i spektralnu dekompoziciju unitarnog operatora, za koji važi:

$$U = \sum_{i=1}^{n} \exp(\imath\alpha\lambda_i)P_i,$$

gde su λ_i sopstvene vrednosti operatora A i P_i odgovarajući sopstveni potprostori.

Tenzorski (direktni) prozivod vektorskih prostora H_1 i H_2, označen sa $H = H_1 \otimes H_2$, definiše se kao skup svih uređenih parova $(|\varphi\rangle, |\chi\rangle)$, gde je $|\varphi\rangle \in H_1$ i $|\chi\rangle \in H_2$, a skalarni proizvod definisan na njemu kao

$$s((\langle\varphi|, \langle\chi|), (|\psi\rangle, |\phi\rangle)) = s_1(\langle\varphi|\psi\rangle)s_2(\langle\chi|\phi\rangle),$$

za $|\varphi\rangle, |\psi\rangle \in H_1$ i $|\chi\rangle, |\phi\rangle \in H_2$. Preslikavanja s_1 i s_2 predstavljaju skalarne proizvode na Hilbertovim prostorima H_1 i H_2, redom. Prostori H_1 i H_2 se nazivaju faktor prostorima od H. U kvantno-mehaničkoj notaciji se stanja prostora H još zapisuju kao $|\varphi\rangle \otimes |\chi\rangle$. Tenzorski proizvod konačne familije Hilbertovih prsotora je takođe Hilbertov prostor, koji označavamo sa

$$H = \otimes_{i=1}^{n} H_i.$$

Dakle svaki element $|\Psi\rangle$ prostora $H = H_1 \otimes H_2$, se može jednoznačno razviti po bazisu $(|\varphi_i\rangle, |\chi_j\rangle)$, $1 \leq i \leq n$, $1 \leq j \leq m$:

$$|\Psi\rangle = \sum_{i,j} C_{ij}(|\varphi_i\rangle, |\chi_j\rangle),$$

gde su $|\varphi_i\rangle$ i $|\chi_j\rangle$ redom baze prostora H_1 i H_2. Koeficijenti C_{ij} se na osnovu ortonormiranosti baze dobijaju kao $C_{ij} = (\langle\varphi_i|, \langle\chi_j|)|\psi\rangle$. Uslov normiranosti vektora Ψ, $\langle\Psi|\Psi\rangle = 1$, povlači uslov:

$$\sum_{i,j} |C_{ij}|^2 = 1.$$

Sada se delovanje svakog operatora A, koji deluje samo na faktor prostoru H_1, zapisuje u obliku ("jednočestični operator"):

$$A_1 \otimes I_2,$$

gde jedinični (identički) operator sugeriše nemenjanje vektora u drugom faktor prostoru stanja H_2. Analogno, "jednočestični" operator B, na drugom faktor prostoru stanja, se zapisuje u obliku:

$$I_1 \otimes B_2.$$

U opštem slučaju, operatori na ukupnom prostoru stanja su "dvočestični" opearatori oblika:

$$A_1 \otimes B_2,$$

gde se delovanje operatora na ukupni prostor zadaje izrazom:

$$(A_1 \otimes B_2)(|\varphi\rangle, |\chi\rangle) = (A_1(|\varphi\rangle), B_2(|\chi\rangle)).$$

1.3 Osnovni postulati kvantne mehanike

Osnovni fizički pojam je pojam *stanja*. Poznavanje stanja fizičkog sistema povlači i poznavanje vrednosti svih fizičkih veličina u klasičnoj fizici, kao i odgovor na pitanje vremenske promene stanja, tj. vrednosti fizičkih veličina. Naime, svaka *materijalna tačka* definisana je parom vektora položaja i impulsa $(\overrightarrow{r}, \overrightarrow{p})$, i time skup svih ovakvih uređenih parova čini vektorski prostor (*fazni prostor*). Rešavanjem jednačina kretanja za sistem čestica (materijalnih tačaka), kao rešenje se dobijaju jednoznačne funkcije vremena datih fizičkih veličina

$$\overrightarrow{r} = \overrightarrow{r}(t), \ \overrightarrow{p} = \overrightarrow{p}(t).$$

Tako se može reći da se realni fizički sistemi u klasičnoj mehanici modeluju skupom parametara (masa, naelekrisanje,...) i skupom vektora položaja i impulsa, tj. faznim prostorom kao prostorom stanja. Otuda se, efektivno, međusobno identifikuju pojmovi stanja i fizičkih veličina položaja i impulsa, $\overrightarrow{r}$ i $\overrightarrow{p}$.

Za razliku od klasične, kvantnu mehaniku odlikuje odsustvo vizualizacije fizičkih sistema i procesa koji su karakteristični za klasičnu fiziku. Pojmovi stanja i vrednosti fizičkih veličina se više ne identifikuju i o fizičkim događajima se govori samo u terminima verovatnoće. Ovi pojmovi su definisani postulatima kvantne mehanike.

Na osnovu *postulata o stanjima*, svako stanje kvantnog sistema predstavljeno je jednim elementom Hilbertovog prostora. Važi i obrnuto, svaki elemenat datog Hilbertovog prostora je jedno moguće stanje kvantnog sistema. Pri tome, ako važi jednakost $|\varphi\rangle = e^{\imath\delta}|\psi\rangle$, tada su stanja $|\varphi\rangle$ i $|\psi\rangle$ jednaka do na fazu δ. Takođe, se svako stanje Hilbertovog prostora stanja, na osnovu (**??**), može jednoznačno razložiti u linearnu superpoziciju stanja iz nekog ortonormiranog bazisa.

Na osnovu *postulata o opservablama(operatorima)*, svakoj klasičnoj promenljivoj fizičkog sistema A se jednoznačno može pridružiti jedan ermitski operator (opservabla) koji deluje u datom Hilbertovom prostoru-prostoru stanja kvantnog sistema. Važi i obrnuto, svaki ermitski operator koji deluje nad datim prostorom stanja je jedna fizička veličina koju je moguće izmeriti određenim mernim postupkom. Svaki ermitski operator je jednoznačno predstavljen svojom spektralnom formom (**??**), pri čemu se sopstvene vrednosti mogu dobiti merenjem ove opservable.

Na osnovu *postulata o verovatnoćama*, verovatnoća da se merenjem operatora A u stanju $|\psi\rangle$ dobija rezultat koji leži u intervalu $[\alpha, \beta]$, u oznaci $W(A, |\psi\rangle, [\alpha, \beta])$, se izračunava po formuli

$$\langle\psi|P_{[\alpha,\beta]}(A)|\psi\rangle, \tag{1.10}$$

gde je

$$P_{[\alpha,\beta]} = \sum_{\lambda_n \in [\alpha,\beta]} P_n.$$

Kao i u prošloj sekciji, sa λ_n smo označili sopstvene vrednosti operatora A, a sa P_n odgovarajuće sopstvene prostore. Dakle, sumiranje se vrši samo po onim sopstvenim vrednostima koje padaju u interval $[\alpha, \beta]$.

Dakle, u klasičnoj mehanici, poznavanje stanja određuje, i to jednoznačno, vrednosti svih fizičkih veličina datog sistema; to je, formalno, posledica činjenice da su sve fizičke veličine zapravo analitičke funkcije na faznom prostoru. U kvantnoj mehanici, poznavanje stanja ne određuje vrednosti fizičkih veličina (opearatora), već su te vrednosti definisane posebnim postulatom. Otuda se nameće očekivanje: ako jednom stanju ne odgovara jednoznačna vrednost neke opservable, onda je nužni element kvantnomehaničke teorije pojam verovatnoće.

Osnovni i opšti zadatak kvantne mehanike je proračun verovatnoća događaja (rezultata meranja) i očekivanih (srednjih) vrednosti opservabli tj. operatora. Tada se podrazumeva da je stanje sistema poznato u svakom trenutku (drugim rečima poznata je dinamika sitema, o čemu ćemo više u narednim sekcijama). Postulat o verovatnoćama implicira da se stanje sistema zapravo tiče *ansambla* - skupa po nečemu identičnih, međusobno neinteragujućih fizičkih sistema. Pojam verovatnoće ima smisla samo na asamblu, tj. na skupu identično obavljenih merenja na svim elementima asambla. Takođe, stanje pojedinačnog sistema ansambla nije unapred poznato, iako je poznato stanje ansambla. Međutim, ako se sistem nalazi u nekom stanju $|\psi\rangle$, što je element Hilbertovog prostora stanja, tada je stanje svakog pojedinačnog elementa (sistema) u ansamblu jednoznačno određeno. Ovaj postulat je od suštinskog značaja za kvantnu informatiku, u kojoj se barata pojedinačnim sistemima (tzv. kubitovima). U sekciji 2.1. dat je ansambl kubitova modeliran grafom.

Pomenućemo još dva bitna postulalta kvantne mehanike koja su od važnosti za kvantnu informatiku. Naime, prenos klasičnih varijabli (fizičkih veličina) u kvantni kontekst, a u skladu sa postulatima o opservablama, zahteva poseban propis, na osnovu koga razmatramo i višedimenzionalne sisteme. Dakle, po ovom *postulatu o kvantizaciji* se svakoj klasičnoj varijabli fizičkog sistema jednoznačno pridružuje jedan ermitski operator (koji deluje nad prostoromm stanja tog sistema). To znači da osnovni skup varijabli postaje osnovni skup opservabli- stepeni slobode i njima kanonski konjugovanih impulsa.

Osnovu primene ovog postulata određuje sledeći postulat kvantne mehanike. Na osnovu *postulata o stepenima slobode* svakom stepenu slobode fizičkog sistema pridružuje se jedan prostor stanja H_i. Ukupni prostor stanja H, kvantnog sistema definiše se kao tenzorski proizvod prostora stanja pojedinih stepeni slobode $H = \otimes_i H_i$. Podsetimo, da nezavisni parametri

pomoću kojih su u svakom trenutku vremena određeni položaji masa sistema predstavljaju stepene slobode dinamičkog sistema. Masa u ravni je određena sa tri parametra pomeranja: dve translacije i jedna rotacija, dok je masa u trodimenzionalnom prostoru definisana sa šest parametara pomeranja: tri translacije i tri rotacije.

Dakle, postulat o stepenima slobode formalno uvodi prostore stanja za date klasične stepene slobode sistema. Nad faktor prostorima stanja sada deluju opservable koje se, na osnovu klasično zadatih stepeni slobode, kvantuju u skladu sa prethodnim postulatom. Sve opservable sistema koje deluju nad ukupnim prostorom stanja su sada analitičke funkcije osnovnog skupa opservabli (tj. stepeni slobode i njima konjugovanih impulsa-baš kako je to u klasičnoj analitičkoj mehanici).

Više o temi osnovnih postulata kvantne mehanike čitalac može naći, na primer, u [**?**, **?**].

1.4 Unutrašnji stepeni slobode: Spin

Eksperiment poput slavnog Štern-Gerlahovog ([**?**]), ukazuju na teškoće objašnjenja nekih kvantnih efekata kada se model efekta zasniva na standardnim (prostornim, "spoljašnjim") stepenima slobode. Dakle, kada uračunavanje svih mogućnosti za objašnjenje efekata koji se modeluju na skupu opservabli vektora položaja i impulsa jednog višečestičnog sistema nije dovoljno, tada je neizbežna pretpostavka o postojanju novih, od opservabli položaja i impusla nezavisnih, "unutrašnjih" stepeni slobode. Objašnjenje Štern-Gerlahovog eksperimenta usledilo je na osnovu uvođenja unutrašnjeg stepena slobode, tj. *spina*.

Spin je "unutrašnja" osobina kvantne čestice čija se (vremenski nezavisna) vrednost s, fenomenološki utvrđuje. Na osnovu ove vrednosti izgrađuje se odgovarajući prostor stanja H_s. Ukupni prostor stanja čestice se uvodi kao tenzorski proizvod $H_o \times H_s$, gde je sa H_o označen orbitalni prostor stanja nad kojim deluju opservable položaja i impulsa, $\overrightarrow{r}$ i $\overrightarrow{p}$ ("spoljašnji stepeni slobode"). Spin nije funkcija bilo koje od ovih opservabli.

Vektorska opservabla spina $\overrightarrow{S}$, uvodi se po analogiji sa opservablom momenta impulsa $\overrightarrow{L} = \overrightarrow{r} \times \overrightarrow{p}$ i po definiciji, nije funkcija niti $\overrightarrow{r}$, ni $\overrightarrow{p}$. Njeno uvođenje je neophodno, jer Štern-Gerlahov eksperiment ne može biti objašnjen niti klasičnom, ni kvantnom fizikom, zasnovanom na spoljašnjim stepenima slobode. Otuda se spinu prilazi kao unutrašnjoj osobini kvantne čestice čija se vrednost fenomenološki utvrđuje za svaku česticu posebno. Ispostavlja se da su dozvoljene ili polubrojne ili celobrojne (nenegativne) vrednosti spina. Čestice sa polubrojnim spinom nazivaju se fermionima, a čestice sa celobrojnim spinom bozonima. Na primer, elektroni su fermioni za koje je $s = 1/2$; kvanti svetlosti ("fotoni") su bozoni gde je $s = 1$.

U formalizmu se uvodi Paulijeva opservabla $\hat{\sigma} = \{\hat{\sigma_x}, \hat{\sigma_y}, \hat{\sigma_z}\}$, definisana jednakošću $\overrightarrow{S} = \hbar\hat{\sigma}/2$. Komponente ovog operatora, tzv. Paulijevi operatori, zadovoljavaju sledeću algebru:

$$\hat{\sigma_i}\hat{\sigma_j} - \hat{\sigma_j}\hat{\sigma_i} = 2\imath\epsilon_{ijk}\hat{\sigma_k}, \tag{1.11}$$

$$\hat{\sigma_i}\hat{\sigma_j} + \hat{\sigma_j}\hat{\sigma_i} = 2\delta_{ij}, \tag{1.12}$$

gde (i, j, k) predstavlja bilo koju permutaciju skupa $\{x, y, z\}$ ([**?**, **?**]). Takođe, ϵ_{ijk} predstavlja permutacioni simbol definisan sa

$$\epsilon_{ijk} = \begin{cases} 0, & \text{ako je } i = j \text{ ili } i = k \text{ ili } j = k \\ 1, & \text{ako je } (i,j,k) = \{(1,2,3),(2,3,1),(3,1,2)\} \\ -1, & \text{ako je } (i,j,k) = \{(1,3,2),(3,2,1),(2,1,3)\}. \end{cases}$$

U slučaju kada je spin 1/2 Paulijevi operatori se reprezentuju Paulijevim matricama:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ako je zadat skup čestica, svaka čestica spina 1/2, tada je prostor stanja takvog skupa zapravo tenzorski proizvod prostora stanja pojedinih spinova $\otimes_i H_i$, gde je svaki H_i prostor stanja jednog spina 1/2. Ako se sistem sastoji od neidentičnih kvantnih čestica (što je od interesa za kvantnu informatiku), tada je svaki spinski faktor prostor H_i dvodimenzionalan i jedan ortonormirani sopstveni bazis se označava sa $\{|1/2\rangle_i, |-1/2\rangle_i\}$. Takođe, na osnovu definicije tenzorskog proizvoda imamo da je opšte stanje takvog skupa čestica dato oblikom:

$$\sum_{i,j,k,\ldots} c_{ijk\ldots}(|i\rangle_1|j\rangle_2|k\rangle_3\ldots),$$

gde $i, j, k, \ldots$ mogu uzeti vrednosti $\pm 1/2$. Ako uvedemo oznake $|1/2\rangle \equiv |0\rangle$ i $|-1/2\rangle \equiv |1\rangle$ za svaki spin u skupu, tada ortonormirani bazis sistema spinova kojeg čine isključivo nekorelisana stanja se može kraće zapisati, za skup od N takvih spinova, na sledeći način:

$$\begin{aligned}
|0\rangle_1|0\rangle_2\ldots|0\rangle_{N-1}|0\rangle_N \equiv |00\ldots00\rangle &\equiv |0\rangle \\
|0\rangle_1|0\rangle_2\ldots|0\rangle_{N-1}|1\rangle_N \equiv |00\ldots01\rangle &\equiv |1\rangle \\
|0\rangle_1|0\rangle_2\ldots|1\rangle_{N-1}|0\rangle_N \equiv |00\ldots10\rangle &\equiv |2\rangle \\
&\vdots \\
|1\rangle_1|1\rangle_2\ldots|1\rangle_{N-1}|1\rangle_N \equiv |11\ldots11\rangle &\equiv |2^N-1\rangle.
\end{aligned}$$

Tada se svako stanje sistema može predstaviti, u opštem slučaju, u obliku

$$\sum_{i=0}^{2^N-1} c_i|i\rangle.$$

1.5 Kvantna dinamika

Za kvantni sistem koji ne interaguje (međudeluje) ni sa jednim fizičkim sistemom i najviše se može naći u nekom spoljašnjem polju (električnom, magnetnom i sl.) kaže se da predstavlja izolovani kvantni sistem. Za ovakve sisteme uspostavlja se postulat o zakonu kretanja koji opisuje i određuje dinamiku sistema, tj. promenu njegovog stanja u vremenu. Zbog podvojenosti stanja od opservabli, postoji zapis zakona kretanja izolovanih sistema u terminima opservabli (Hajzenbergova slika) i zakon kretanja izolovanih sistema u terminima stanja (Šredingerova slika).

Dinamika sistema se uspostavlja po sledećem zakonu: kvantizacijom klasične Hamiltonove funkcije dobija se opservabla energije (Hamiltonijan) sistema H, koji se zamenjuje u operatorski izraz

$$U = \exp(-\imath H(t - t_0)/\hbar) \tag{1.13}$$

za sve "konzervativne" sisteme, definisane uslovom $\partial H/\partial t = 0$. Tada se promena stanja u vremenu može opisati jednakošću

$$|\psi(t)\rangle = U|\psi(t_0)\rangle, \tag{1.14}$$

ili, ekvivalentno, *Šredingerovom jednačinom*:

$$\imath\hbar\frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle. \tag{1.15}$$

Za konzervativne sistema Šredingerova jednačina (**??**) se svodi na rešavanje svojstvenog problema Hamiltonijana:

$$H|\psi_n\rangle = \lambda_n|\psi_n\rangle,$$

gde se vreme kao parametar ne pojavljuje. Ova jednačina je stacionarna Šredingerova jednačina, a vremenska zavisnost u stanjima, rešenjima Šredingerove jednačine (**??**), se pojavljuje kroz fazni faktor, tj. definišu se stacionarna stanja (isključivo za konzervativne sisteme) u obliku:

$$\exp(-\imath t\lambda_n/\hbar)|\psi_n\rangle,$$

gde je $t_0 = 0$.

Poznavanje stanja sistema u jednom trenutku uspostavlja jednoznačno stanje tog sistema u svakom kasnijem trenutku. Promena stanja u vremenu je jednoznačna i invertibilna (reverzibilna), jer je operator promene stanja u vremenu U, unitaran: $U^\dagger = U^{-1}$.

1.6 Kvantna mešavina stanja. Statistički operator

Ako stanje ansambla S, nije jednoznačno poznato, onda se ono opisuje nekom raspodelom verovatnoća za. Naime, neka su stanja iz nekog skupa $\{\psi_i\}_{i\in I}$, i neka su odgovarajuće verovatnoće date raspodelom verovatnoća, tj. skupom verovatnoća $\{W_i\}_{i\in I}$. Fizički, to znači da iz datog (mešanog) ansambla, možemo odabrati element koji se nalazi u stanju $|\psi_i\rangle$. Postavlja se pitanje matematičkog opisa mešanog ansambla, to jest stanja mešanog ansambla.

Neka je S_i skup svih elemenata ansambla koji se nalaze u stanju $|\psi_i\rangle$. Tada je $S = \bigcup_{i\in I} S_i$ i pri tome ćemo S_i nazvati podansamblom od S, koji odgovara stanju $|\psi_i\rangle$. Dakle, statistička težina podansambla S_i je u stvari verovatnoća W_i. Izračunajmo sada verovatnoću, da se merenjem na celom mešanom ansamblu, dobije vrednost a_n neke opservable A. Tada se merenje sastoji od sledećih međusobno nezavisnih događaja: (a) izbora elemenata iz jednog podasambla S_i i (b) dobijanja vrednosti a_n na tom slučajno odabranom podansamblu S_i. Kako su ovi događaji nezavisni, ukupna verovatnoća na celom ansamblu se dobija kao zbir proizvoda verovatnoća događaja iz (a) i (b):

$$W(A, S, a_n) = \sum_{i\in I} W_i W(A, |\psi_i\rangle, a_n).$$

Na osnovu (**??**), može se lako pokazati da desna strana gornjeg izraza postaje:

$$W_i W(A, |\psi_i\rangle, a_n) = tr(\rho P_n),$$

gde se operator ρ naziva *statistički operator (ili matrica gustine)*, definisan kao:

$$\rho = \sum_{i\in I} W_i|\psi_i\rangle\langle\psi_i|.$$

Ovaj operator predstavlja stanje mešanog ansambla.

1.7 Kvantne mreže kubitova

Kvantne mreže sa fiksiranim sparivanjem najbližih suseda (*fixed nearest-neighbor couplings*) imaju valiku primenu u kvantnim informacionim sistemima. Druge poznate primene su u kvantnoj gravitaciji i teoriji štimovanja. Transfer kvantnog stanja sa jedne lokacije ka drugoj je važna osobina u kvantinim sistemima za procesiranje informacija. Zavisno od tehnologije, kvantni sistemi mogu biti implementirani optičkim mrežama [**?**] ili nizovima kvantnih tačaka [**?**]. Kvantne mreže zapravo prestavljaju osnovnu jedinicu svakog kvantnog sistema za procesiranje inforamacija i sastaljene su od velikog broja interaktivnih komponenata. Kao takve koriste se za potrebe različitih tehnologija, kao komponente kvantnih celularnih automata, zatim magistrale kvantnih kompjutera ili u kvantnom internetu kvantnih kompjutera.

Kvantni računar je uređaj koji koristi principe kvantne mehanike za pamćenje i obradu podataka. Kvantno računartvo je još uvek u ranoj fazi razvoja. I pored toga, rađeni su eksperimenti na izvršavanju kvantnih operacija sa veoma malim brojem kubitova (*quantum binary digits*). Kvantni bit ili kubit je osnovna jedinica za količinu inforamcija u kvantnom računarstvu. Količina informacije koju sadži jedan kubit jednaka je količini informacije od jednog bita. Razlika između kvantnog i klasičnog računarstva se javlja u samom procesiranju informacija. Upravo ta činjenica čini kvantne računare moćnijim od klasičnih. Neke algoritme (na primer Shorov algoritam) koje klasični računar ne može da izvrši u polinomijalnom vrmenu, kvantni računar može. Kvanti bitovi se mogu opisati kao matematički objekti sa određenim svojstvima. Dva moguća stanja u kojima se može naći kubit označavaju se sa $|0\rangle$ i $|1\rangle$. Razlika između kubita i bita je u tome što se kubit može naći i drugim stanjima sem $|0\rangle$ i $|1\rangle$. Stanja kubita se opisuju *linearnom kombinacijom* (*superpozicija*) ortogonalnih vektora (stanja) $|0\rangle$ i $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

gde su α i β kompleksni brojevi koje nazivamo *amplitudama*. Za razliku od bita u digitalnoj elektronici, stanje kvantnog bita se ne može odrediti, već se može reći da je u stanju $|0\rangle$ sa verovatnoćom $|\alpha|^2$ ili u stanju $|1\rangle$ sa verovatnoćom $|\beta|^2$. Ako stanje kubita posmatramo kao slučajnu promenljivu, prirodno važi da je $|\alpha|^2 + |\beta|^2 = 1$. To znači da se stanje kubita može interpretirati kao dvodimenzionalni normalizovani kompleksni vektor. Dakle, pod kubitom se podrazumeva bilo koji dvodimenzionalni prostor stanja kvantnog sistem, pri čemu je sa $\{|0\rangle, |1\rangle\}$ označen jedan unapred fiksiran ortonormiran bazis. Međutim, kubit ne treba bukvalno shvatiti kao prostor stanja čestice spina-1/2, jer on može biti bilo koji fizički kvantni sistem, čiji se dvodimezionalni prostor stanja može dovoljno dobro iskontrolista, tako da nakon operacija na prostoru stanja sistema, on i dalje ostane dvodimenzionalan. Sa druge strane, uz pomoć gore definisanog dvodimenzionalnog bazisa, mogu se izgraditi opservable:

$$\begin{aligned}\sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|;\\ \sigma_y &= \imath|1\rangle\langle 0| + \imath|0\rangle\langle 1|;\\ \sigma_z &= |0\rangle\langle 0| + |1\rangle\langle 1|,\end{aligned}$$

tj. formalno, Paulijevi sigma-operatori. Naravno, to opet ne znači da se bukvalno radi o operatorima spina-1/2. Primeri modela kubitova su: efektivni spin fotona, ridbergova stanja atoma, kvantne tačke, stanja elektromagnetne šupljine, itd.

Iz ugla informatičkog procesiranja informacija, sve operacije se obavljaju na jednom kubitu (po analogiji sa klasičnom informatikom), pojam verovatnoće tiče se skupa kubitova tj. an-

sambla. Tako, kada se govori u terminima verovatnoće o, na primer, kvantnom računaru, zamišlja se da se ima posla sa ansamblom identičnih kvantnih računara.

Takođe, stanje kvantnog sistema (kvantnog registra od n bitova) može biti svaka reč nula i jedinica dužine n sa verovatnoćama $|\alpha_x|^2$ $(0 \leq x \leq 2^n - 1)$. Vektor stanja sistema se može opisati kao:

$$|\psi\rangle = \sum_{x=o}^{2^{n-1}} \alpha_x v_x,$$

gde su v_x binarne reči dužine n i $\sum_{x=0}^{2^{n-1}} |\alpha_x|^2 = 1$.

1.8 Kvantne šetnje i savršeni transfer stanja

Neka je dat graf $G = G(V, E)$ i neka je A_G matrica susedstva grafa G. Sa D_G označimo kvadratnu matricu formatata $|V| \times |V|$ definisanu sa

$$d_{ij} = \begin{cases} deg(v_i), & i = j \\ 0, & \text{u suprotnom.} \end{cases}$$

Definišimo Laplasovu matricu L_G tako da je $L_G = A_G - D_G$, za koju se pokazuje da je pozitivno semidefinitna. Tada je neprekidna kvantna šetnja, na osnovu (**??**), definisana unitarnim operatorom

$$U = \exp(-\imath L t)$$

za neko $t \in \mathbb{R}$. Primetimo da smo stavili da je $\hbar = 1$ i $t_0 = 0$. Verovatnoća šetnje da počne u čvoru u i završi se u čvoru v nakon vremena t je data sa $|\langle v|U(t)|u\rangle|^2$. Takođe, ako se sistem nalazi u stanju $|\psi_0\rangle$, vremenska zavisnost stanja sistema data je relacijom (**??**). U slučaju d-regularnih grafova imamo da je $D = dI$, gde je I jedinična matrica, pa je prema tome,

$$\exp(-\imath L t) = \exp(-\imath(A - dI)t) = \exp(\imath d t)\exp(-\imath A t),$$

pri čemu primećujemo da fazni faktor koji nije relevantan za dinamiku (evoluciju) sistema. Takođe se za Hamiltonijan sistema, pored Laplasove, uzima i matrica $H = \frac{1}{d}A$.

Neprekidne kvantne šetnje predstavljaju svojevrsno uopštenje neprekidnih Markovljevih lanaca na grafovima [**?**]. Kvantni analogon klasičnim slučajnim šetnjama je izučavan u mnogim radovima. Pomenućemo radove Moore i Russel [**?**], kao i Kempea [**?**], gde su date bolje procene granica za vremena obilaska u slučaju neprekidnih kvantnih šetnji na hiperkockama, u odnosu na klasične slučajne šetnje na istim strukturama. Neprekidne kvantne šetnje su definisali Farhi i Gutmann u [**?**]. U narednom radu, Childs i ostali [**?**] su konstruisali jednostavan primer u kome klasične i neprekidne kvantne šetnje pokazuju različito ponašanje po pitanju statistike vremena obilaska.

U drugoj glavi disertacije proučavamo fenomen transfera kvantnog stanja u kvantnim mrežama. Mreža se sastoji od n kubitova gde su neki od njih spregnuti XY-interakcijom. Kvantna mreža sa fiksiranim sparivanjem najbližih suseda je jedinstveno opisana neorijentisanim grafom G gde skup čvorova $V(G) = \{1, 2, \ldots, n\}$ predstavlja lokaciju svakog kubita u mreži. Skup ivica grafa $E(G)$ je određen spregnutim kubitovima, to jest čvorovi i i j su povezani ako su i-ti i j-ti kubitovi spregnuti. Označimo sa A matricu susedstva grafa G.

Transfer se ostvaruje vremenskom evolucijom sistema pod uticajem vremenski nezavisnog Hamiltonijana, bez dodatne spoljne kontrole:

$$H_G = \frac{1}{2} \sum_{(i,j)\in E(G)} \sigma_i^x \sigma_j^x + \sigma_i^y \sigma_j^y,$$

gde su σ_i^x, σ_i^y i σ_i^z predstavljaju Paulijeve matrice i-tog kubita. Ovaj izraz predstavlja opis sparivanja kubitova vezanih XY-interakcijom. U ovom mehanizmu se zanemaruju moguće greške nastale dinamičkom kontrolom interakcije kubitova. Ovakve kvantne mreže se nazivaju kvantnim spin mrežama, budući da se svakim kubitom u mreži generišu dva stanja: $|0\rangle$ sa spinom usmerenim na dole i $|1\rangle$ sa spinom usmerenim na gore. Inicijalno (u trenutku $t = 0$) se pretpostavlja da je stanje sistema $\underbrace{|00\ldots00\rangle}_{n}$, što odgovara stanju sistema sa energijom 0.

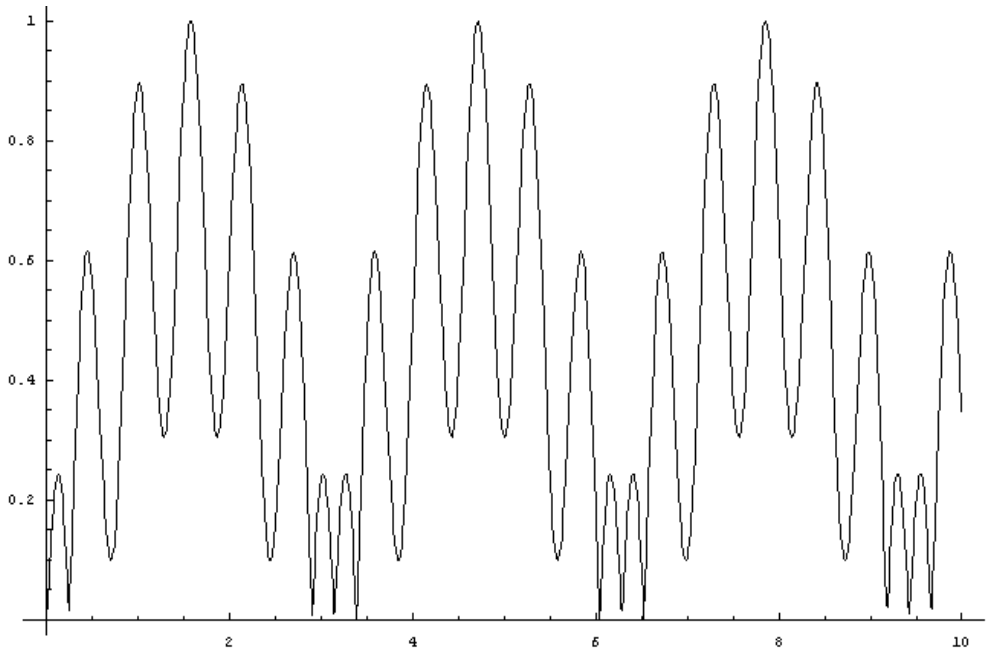
Po postulatu o stanjima, kvantnoj mreži od n kubitova možemo pridružiti Hilbertov prostor dimenzije 2^n. Restrihujući Hamiltonijan H_G na podprostor razapet standardnom bazom $|e_i\rangle = |00\ldots\underbrace{1}_{i}\ldots00\rangle$ (svi spinovi sem i-tog su usmereni na dole, $1 \leq i \leq n$) dobijamo da je identičan matrici susedstva A, [**?**].

Transfer između dva određena kubita a (ulazni) i b (izlazni) se realizuje tako što se najpre ulazni kubit a postavi u neko predefinisano stanje i nakon nekog vremena se očita stanje izlaznog kubita b. Transfer se naziva savršenim (engl. *perfect state transfer*-PST) ukoliko je inicijalno stanje kubita a podudarno finalnom stanju kubita b. Formalno, savršeni transfer (PST) između čvorova (kubitova) a i b ($1 \leq a, b \leq n$) javlja se posle nekog vremena τ, ako je

$$|F(\tau)_{ab}| = 1. \tag{1.16}$$

Operator $F(t) = \exp(-\imath At)$ predstavlja zakon po kome se menja ukupno kvantno stanje mreže protokom vremena (slobodna evolucija). Ovde je uzeto da je *Planckova konstanta* $\hbar = 1$, a eksponent matrice definisan na uobičajeni način $\exp(M) = \sum_{n=0}^{+\infty} \frac{1}{n!} M^n$. Matematički, PST se javlja u mreži ako mreža iz stanja $|e_a\rangle$ pređe u stanje $|e_b\rangle$ nakon vremena τ sa jediničnom amplitudom. Takođe, možemo primetiti da se PST može posmatrati u svetlu kvantnih šetnji [**?**]. Ilustracije radi, na osnovu gornje diskusije, dajemo MATHEMATICA kod za izračunavanje funkcije $F(t) = \exp(-\imath At)$ na proizvoljnom grafu (videti prilog). Korišćenjem tog programa dobijamo grafik funkcije prikazan na slici (1.1).

Poslednjih godina je postignut veliki naučni napredak u opisivanju fenomena koji se javljaju u sistemima za prenos i procesiranje kvantnih informacija. Istaćićemo neke od tih rezultata. Savršeni transfer kvantnih stanja od jednog kubita ka drugom, na prethodano definisanim kvantnim mrežama, prvi put je razmatran u radovima [**?**, **?**]. U literaturi su izučavane razlicite topologije kvantnih mreža koje dopuštaju postojanje PST-a. Na primer, Christandl i ostali, [**?**] su dokazali postojanje PST-a između krajnjih čvorova na putevima dužine jedan i dva. U slučaju grafova koji predstavljaju Kartezione stepene puteva, dokazano je da se PST javlja između čvorova na maksimalnom rastojanju. Prema tome, ovi grafovi su jedni od mogućih kandidata za modeliranje kvantnih mreža. U skorašnjem radu [**?**], Godsil je konstruisao klasu regularnih grafova po rastojanju (eng. distance regular graphs) dijametra tri koji imaju PST. Takođe su Saxena, Severini i Shparlinski [**?**] predložili cirkularne grafove kao moguće kandidate koji bi mogli imati PST. U istom radu je naglašeno da je neophodan uslov za postojanje PST-a periodičnost sistema. Stoga je korisno izučavati parametre grafova koji dopuštaju periodičnu dinamičnost sistema. Specijalno, interesantno je znati koliki je najveći mogući pređeni put



Slika 1.1: *Grafik funkcije $F(t)$, koji predstavlja dinamiku sistema između fiksiranih čvorova*

informacije između dva kubita u mreži. Drugim rečima, potrebno je naći najveće rastojanje među čvorovima grafa tj. dijametar. Kako veliki broj čvorova u grafu predstavlja veliki broj kubitova u mreži, a samim tim i otežani protok informacija, potrebno je za fiksirani dijametar imati što je moguće manje čvorova.

U svim predloženim tipovima mreža *savršena kvantno kuminikaciono rastojanje* (engl. perfect quantum communication distances), tj. rastojanje među čvorovima među kojima se PST javlja, je znatno manje u poređenju sa redom grafa. Ovo rastojanje se dalje može povećati razmatranjem mreža sa fiksnim ali različitim sparivanjem između kubitova. Ove mreže odgovaraju grafovima sa težinskom matricom susedstva, čiji je Hamiltonijan

$$H_G := \frac{1}{2} \sum_{(i,j)\in E} d_{ij}(\sigma_i^x \sigma_j^x + \sigma_i^y \sigma_j^y),$$

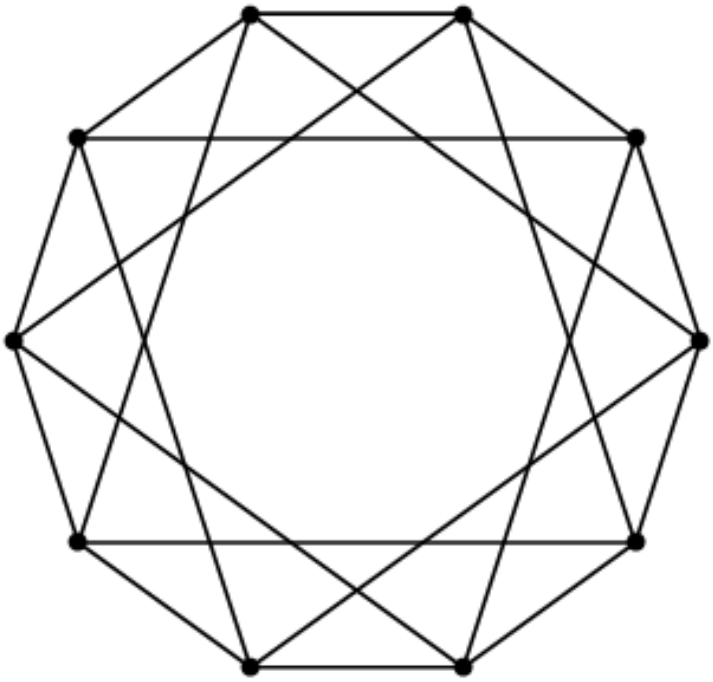
gde su σ_i^x, σ_i^y i σ_i^z standardne Paulijeve matrice koje deluju na kubit i, a $d_{ij} > 0$ predstavljaju konstante sparivanja [**?**]. Pokazano je da je moguće uspostaviti PST na proizvoljnom rastojanju u linearnom lancu između kubitova, ukoliko lanac predstavlja model mreže sa fiksnim ali različitim sparivanjem [**?**]. U nekoliko drugih skorašnjih radova je razmatran sličan prsitup [**?**, **?**, **?**].

1.9 Integralni cirkularni grafovi i njihove primene

Graf se naziva *cirkulantnim* ako je on Kejlijev graf na cirkulantnoj grupi, odnosno ako je njegova matrica susedstva cirkulantna. Graf se naziva *integralnim* ako su sve sopstvene vrednosti matrice susedstva celi brojevi. Integralni grafovi su intenzivno proučavani u poslednjih 20 godina i postoji mnogo konstrukcija specifičnih klasa grafova sa celobrojnim spektrom [**?**]. Klasa cirkulantnih grafova ima značajne primene u projektovanju svih vrsta mreža (računarskih, telekomunikacionih, kvantnih), kao i u paralelnom i distribuiranom računarstvu [**?**].

Integralni cirkulantni grafovi su generalizacija unitarnih Kejlijevih grafova, koje su nedavno proučavali Klotz i Sander [**?**]. Za dalju razradu teme najpre bi nam bila potrebna karakterizacija integralnih cirkularnih grafova data u [**?**]. Neka je D skup pozitivnih pravih delioca prirodnog broja $n > 1$. Integralni cirkularni graf, u oznaci $\mathrm{ICG}_n(D)$, je definisan skupom čvorova $Z_n = \{0, 1, \ldots, n-1\}$ i skupom grana

$$E(\mathrm{ICG}_n(D)) = \{\{a, b\} \mid a, b \in Z_n,\ \gcd(a-b, n) \in D\}\,.$$



Slika 1.2: *Integralni cirkulantni graf* $\mathrm{ICG}_{10}(1)$*, koji je ujedno i uitarni Kejlijev*

Integralni cirkulantni grafovi su predloženi kao potencijalni kandidati za modeliranje kvantnih spin mreža koje dopuštaju periodičnu dinamičnost sistema. Naime, za neke kvantne spin sisteme, potreban uslov za postojanje PST je periodičnost i simetričnost dinamičkog sistema [**?**, **?**]. Relevantni rezultati na ovu temu su dati u [**?**], gde je pokazano da je topologija kvantne mreže, koja je bazirana na regularnim grafovima sa bar četiri različite sopstvene vrednosti, periodična ako i samo ako je graf integralan.

Bašić i ostali [**?**, **?**, **?**] su odredili potreban i dovoljan uslov pod kojim integralni cirkulantni graf ima savršen transfer stanja. Ispostavilo se da stepen dvojke u faktorizaciji razlika susednih sopstvenih vrednosti mora biti konstanta i tačno jedan od delioca $n/4$ i $n/2$ mora pripadati skupu D. Takođe, u karakterizaciji integralnih cirkularnih grafova koji imaju PST, učestvuju samo oni grafovi za koje je $4 \mid n$. Ahmadi i ostali, su proučavali postojanje vremenske uniformne raspodele neprekidnih kvantnih šetnji na cirkularnim grafovima [**?**]. Saxena, Severini i Shraplinski [**?**] su proučavali parametre integralnih cirkulantnih grafova, kao što su dijametar, osobinu bipartitnosti i savršen transfer stanja. Takođe, Stevanović, Petković i Bašić su dali aimptotsku ocenu dijametra integralnih cirkularnih grafova. Klotz i Sander [**?**] su odredili, između ostalog, sopstvene vrednosti unitarnih Kejlijevih grafova i predložili generalizaciju ovih

grafova, koju su nazvali *gcd grafovi* (isti termin kao i integralni cirkulantni grafovi). Bašić i Ilić su u [**?**, **?**] odredili hromatski broj i najveću kliku integralnih cirkulantnih grafova sa jednim i dva delioca, i opovrgnuli hipotezu iz [**?**] da je broj čvorova grafa $\mathrm{ICG}_n(D)$ deljiv sa $\omega(\mathrm{ICG}_n(D))$ ili $\chi(\mathrm{ICG}_n(D))$. Treba pomenuti i skorašnje rezultate vezane za unitarne Kejlijeve grafove. Na primer, Berrizbeitia i Giudici [**?**] i Fuchs [**?**] su ustanovili donju i gornju granicu veličine najvećeg indukovanog cikla. Takođe su, Klotz i Sander [**?**] odredili dijametar, veličinu najveće klike, hromatski broj i sopstvene vrednosti unitarnih Kejlijevih grafova.

Na kraju dajemo interesantne primene integralnih cirkularnih grafova u hemijskoj teoriji grafova.

Neka su $\lambda_1, \lambda_2, \ldots, \lambda_n$ sopstvene vrednosti matrice susedstva. Energija grafa je definisana kao suma apsolutnih vrednosti sopstvenih vrednosti matrice susedstva

$$E(G) = \sum_{i=1}^{n} |\lambda_i|.$$

To je parametar koji proizilazi iz Hikelove molekulsko orbitalne aproksimacije za totalnu π-elektronsku energiju. Nedavno su uvedene razne modifikacije grafovske energije, kao što su Laplasova i energija rastojanja. Do sada su konstruisani parovi ili familije nekospektralnih grafova koji imaju jednaku energiju, ali su sve konstrukcije bazirane na kompozicijama i linijskim grafovima. Međutim, ispostavilo se da su integralni cirkularni grafovi pogodni za konstrukciju hiperenergetskih i ekvienergetskih familija [**?**]. Naime, konstruisane su familije od k hiperenergetskih nekospektralnih integralnih cirkulantnih grafova sa jednakom energijiom i n čvorova, za svako fiksirano k. Takođe su prikazani tri-ekvienergetski parovi nekospektralnih grafova, koji imaju jednaku energiju, Laplasovu energiju i energiju rastojanja [**?**] i date su eksplicitne formule za običnu energiju i energiju rastojanja unitarnih Kejlijevih grafova [**?**]. Takođe je interesantno istaći neke opšte karakteristike energije integralnih cirkularnih grafova. Kako je energija grafa uvek parna [**?**], ispostavlja se da je energija grafa $\mathrm{ICG}_n(D)$ deljiva sa 4, ako je n neparan broj. Takođe, da bi energija bila oblika $4\mathbb{N}+2$ to moraju biti zadovoljeni uslovi da $n/2 \notin D$ i $\lambda_{n/2} < 0$ [**?**]. U istom radu je pokazano da je minimalna energija, za n parno, upravo jednaka n. Svi rezultati su verifikovani u programskom paketu MATHEMATICA. U prilogu teze smo dali MATHEMATICA kod za generisanje integralnih cirkularnih grafova, računanje energije i energije rastojanja, generisanje integralnih cirkularnih grafova koji imaju PST. Takođe smo koristili programe u programskom jeziku Java za složenija pretraživanja najveće klike i optimalnog bojenja, kao i komponenata povezanosti i dijametra.

1.10 Simulacije i bisimulacije

Jedan od najvažnijih problema u teoriji automata je utvrđivanje da li su dva data automata ekvivalentna, što obično znači da je njihovo ponašanje identično. U kontekstu determinističkih i nedeterminističkih automata, ponašanje automata je određeno jezikom koji se njima raspoznaje, pri čemu se smatra da su dva automata *ekvivalentna*, ili preciznije *jezički ekvivalentna*, ako raspoznaju isti jezik. Za konačne determinističke automate problem ekvivalentnosti automata je rešiv u polinomijalnom vremenu, dok je za konačne nedeterminističke automate on težak za izračunavanje tj. PSPACE-kompletan [**?**, **?**]. Još jedan važan problem, koje se posledično može postaviti, sastoji se u opisivanju jezički ekvivalentnih automata relacijom među skupovima njihovih stanja, ukoliko takva relacija postoji. Ovaj problem se može relaksirati pitanjem nalaženja neke relacije među stanjima koja bi povlačila jezičku ekvivalentnost. Jezička ekvivalentnost

dva deterministička automata se može izraziti u terminima relacija među stanjima, ali u slučaju nedeterminističkih automata problem je komplikovanije prirode.

Za označavanje "ekvivalencije" među stanjima automata, u širokoj upotrebi je termin *bisimulacija*. Bisimulacije su prvi uveli Milner [?] i Park [?] za potrebe računarstva, kada su ih koristili za modeliranje ekvivalencije među različitim sistemima, kao i za redukciju broja stanja ovih sistema. Takođe, u isto vreme one su nezavisno otkrivene u drugim oblastima matematike, na primer, u modalnoj logici i teoriji skupova. One se danas upotrebljavaju u mnogim oblastima računarstva, kao što su funkcionalni jezici, objektno-orijentisani jezici, tipovi podataka, domeni, baze podataka, kompajlerska optimizacija, analiza i verifikacija programa, itd. [?, ?, ?, ?, ?, ?, ?, ?].

Najčešće strukture na kojima su se bisimulacije proučavale su označeni tranzicioni sistemi, tj. označeni direktni grafovi, što su u suštini nedeterministički automati bez fikasiranih inicijalnih i završnih stanja. Definiciju bisimulacija na nedertminističkim automatima u kojima se uzimaju u obzir inicijalna i završna stanja dao je Kozen u [?]. U mnogobrojnim radovima koji se bave bisimulacijama, uglavnom je jedan tip bisimulacija proučavan, nazvan jednostavna bisimulacija, kao što je to učinjeno u Kozenovoj knjizi [?], ili jaka bisimulacija, kao u [?, ?, ?]. U ovoj tezi razlikujemo dva tipa simulacija, direktne i povratne simulacije. Imajući u vidu ova dva tipa simulacija, imamo četiri slučaja kada su relacija R i njoj inverzna relacija R^{-1} direktna i povratna simulacija, a to znači da razlikujemo četiri tipa bisimulacija. Naime, definišemo dve istorodne bisimulacije, direktnu i povratnu bisimulaciju, gde su obe R i R^{-1} direktne i povratne simulacije, i dve raznorodne bisimulacije, povratna-direktna i direktna-povratna bisimulacija, gde je R povratna i R^{-1} direktna simulacija, i obrnuto. Razlika između direktnih i povratnih simulacija, i direktnih i povratnih bisimulacija, je data, na primer u [?, ?, ?] (za različite tipove automata), ali se manje-više ovi koncepti razlikuju od koncepata koje razmatramo u tezi. Sličniji koncepti našem konceptu direktnih i povratnih simulacija i bisimulacija su proučavani u [?] i u [?, ?] (za stabla automate).

Važno je napomenuti da su direktne i povratne bisimulacije, kao i povratne-direktne i direktne-povratne bisimulacije, dualni koncepti, tj., povratne i direktne-povratne bisimulacije na nedeterminističkom automatu su direktne i povratne-direktne bisimulacije na njemu reverzibilnom automatu. Ovo znači da za svako univerzalno tačno tvrđenje za direktne ili povratne-direktne bisimulacije postoji odgovarajuće univerzalno tačno tvrđenje za povratne i direktne-povratne bisimulacije. Iz tog razloga, mi se fokusiramo samo na direktne i povratne-direktne bisimulacije. U principu, ako uporedimo direktne i povratne-direktne bisimulacije, sa jedne, i povratne i direktne-povratne bisimulacije sa druge strane, možemo zaključiti da u praktičnim primenama ni jedan od koncepata nije bolji od drugog. Na primer, desno i levo invarijantne ekvivalencije (direktne i povratne bisimulacione ekvivalencije) Ilie, Yu i ostali [?, ?, ?, ?] su koristili u redukciji broja stanja nedeterminističkih automata. Pokazano je da postoje slučajevi kada jedna vrsta ekvivalencija bolje redukuje broj stanja, ali takođe postoje slučajevi kada druga vrsta daje bolju redukciju. Takođe su prezentovali slučajeve u kojima se pri primeni svake ekvivalencije posebno dobija polinomijalna redukcija broja stanja, dok se naizmeničnom primenom oba tipa ekvivalencija broj stanja redukuje eksponencijalno ([?, Sekcija 11]).

Kako smo već pomenuli, glavna uloga bisimulacija je modeliranje ekvivalencija između stanja jednog ili više automata. Međutim, bisimulacije obezbeđuju kompatibilnost sa funkcijom prelaza, inicijalnim i završnim stanjima automata, ali se u opštem slučaju ne ponašaju kao ekvivalencije. Vrste relacija definisane na elementima dva skupa koje su zamišljene kao ekvivalencije date su u [?] za fazi slučaj. Ovde razmatramo krisp verziju ovih relacija i zovemo ih *uniformnim relacijama*. Jedan od ciljeva ovog dela teze je da pokaže da vezom ova dva

koncepta, uniformnih relacija i bisimulacija, dobijamo veoma moćan alat u proučavanju ekvivalencija između nedeterminističkih automata, gde uniformne relacije služe kao ekvivalencije između stanja dva nedeterministička automata, a bisimulacije obezbeđuju kompatibilnost sa funkcijom prelaza, inicijalnim i završnim stanjima ovih automata. Naš drugi cilj je uvođenje računa na nivou relacija koji se pokazao efikasnim u proučavanju bisimulacija. Treće, uvodimo i proučavamo opštiji tip bisimulacija, tzv. *slabih bisimulacija*. Može se pokazati da je ekvivalentnost automata određena slabim bisimulacijama bliža jezičkoj ekvivalentnosti od ekvivalentnosti zasnovane na bisimulacijama. Takođe imamo da slabe bisimulacije prave manje autoamte od bisimulacija kada se koriste za redukciju broja stanja.

Glava 2

Kvantna dinamika na cirkularnim mrežama

U ovoj glavi proučavamo pitanje prisustva PST na netežinskim i težinskim cirkularnim mrežama, koje je prvi put postavljeno u [**?**]. Glavni rezultat glave je kompletna karakterizacija netežinskih cirkularnih mreža koje imaju PST. Najpre je pokazano da je evolucija kvantnih sistema, čiji je Hamiltonijan identičan matrici susedstva težinskog cirkularnog grafa, periodična ako i samo ako je taj graf integralan. Nakon toga su dati potrebni i dovoljni uslovi za egzistenciju PST na težinskim integralnim cirkularnim grafovima u terminima sopstvenih vrednosti grafa. U narednoj sekciji je izvršena karakterizacija netežinskih integralnih cirkularnih koji imaju PST. Korišćenjem prethodnih rezultata izračunali smo savršeno komunikaciono rastojanje i dali formulu za broj netežinskih integralnih cirkularnih koji imaju PST, u funkciji od reda grafa. U nastavku je dat odgovor na pitanje Godsila [**?**], o postojanju klase gravofa kod kojih se PST odvija između čvorova koji se ne nalaze na dijametru (neantipodalni čvorovi). Na ovo pitanje smo dali potvrdan odgovor konstrukcijom klasa integralnih cirkularnih grafova dijametra dva, u kojima se javlja PST. Na kraju smo našli nove klase težinskih cirkularnih grafova koje imaju PST, kao i one u kojima se PST ne može ostvariti. Problem kompletne karakterizacije težinskih cirkularnih grafova sa celobrojnim vrednostima je generalno težak i pristup rešenju ovog problema zahteva korišćenje tehnika kako teorije brojeva, tako i teorije grafova. Većina rezultata ove glave preuzeta je iz originalnih radova [**?**, **?**, **?**], dok su rezultati prve sekcije bazirani na radu [**?**].

2.1 PST proizvoljnog stanja na kvantnim spin mrežama

Da bi ramotrili problem kvantnog transfera stanja u kvantnim spin sistemima, definisaćemo najpre kvantnu mrežu kao prost, povezan graf $G := (V(G), E(G))$, gde $V(G)$ označava skup čvorova u grafu i $E(G)$ skup ivica. Dva čvora $i, j \in V(G)$ su susedna ako je $(i, j) \in E(G)$. Svakom ovako definisanom grafu G možemo pridružiti matricu susedstva $A(G)$ čiji su elementi dati sa

$$a_{i,j} \;=\; \begin{cases} 1, & (i,j) \in E(G) \\ 0, & \text{u suprotnom.} \end{cases} \tag{2.1}$$

Ako se svakom čvoru ovako definisanog grafa pridruži čestica spina $\frac{1}{2}$, onda govorimo o kvantnom spin sistemu pridruženom grafu G. To znači da svakom čvoru $i \in V(G)$ možemo pridružiti

Hilbertov prostor $\mathcal{H}_i \simeq C^2$, tj. Hilbertov prostor pridružen grafu G je dat sa

$$\mathcal{H}_G = \bigotimes_{i \in V(G)} \mathcal{H}_i = (C^2)^{\otimes N}.$$

gde N označava broj čvorova u grafu.

Definišimo rastojanje $d(i,j)$ između bilo koja dva čvora $i, j \in V(G)$ kao broj ivica najkraćeg puta između i i j, tj. kao grafovsku geodezu između dva čvora.

Ovde razmatramo dinamiku sistema koja je definisana kvantno-mehaničkim Hamiltonijanom:

$$H_G = \frac{1}{2} \sum_{(i,j) \in E(G)} J_{ij}[\sigma_i^x \sigma_j^x + \sigma_i^y \sigma_j^y], \tag{2.2}$$

gde su σ_i^x, σ_i^y i σ_i^z standardne Paulijeve matrice koje odgovaraju kubitu i i deluju na prostor $\mathcal{H}_i$, a $J_{ij} > 0$ su konstante koje predstavljaju jačinu sparivanja između i-tog i j-tog čvora u grafu. Primetimo da je $J_{ij} = J_{ji}$ jer je H_G is Hermitijan. Ukupna z-komponenta spina data je sa

$$\sigma_{tot}^z := \sum_{i \in V(G)} \sigma_i^z$$

za koju važi $\sigma_{tot}^z H_G - H_G \sigma_{tot}^z = [\sigma_{tot}^z, H_G] = 0$. Zato se može izvršiti dekompozicija Hilbertovog prostora $\mathcal{H}_G$ na invarijantne podprostore, gde je svaki od njih sopstveni prostor operatora σ_{tot}^z.

Za potrebe kvantnog transfera stanja, dovoljno je ograničiti se na proučavanje $N-$dimenzionalnog sopstvenog podprostora od σ_{tot}^z, koji odgovara sopstvenoj vrednosti $(2-N)/2$. Označimo taj podprostor sa $\mathcal{S}_G$. Inicijalna kvantna stanja ovog podprostora, pod uticajem vremenske evolucije će ostati u njemu. Stanja baze podprostora $\mathcal{S}_G$ odgovaraju konfiguraciji spina, gde su svi spinovi sem jednog usmereni na dole i taj jedan na gore. Zato ćemo ovu bazu bazičnih stanja označiti sa $|j\rangle$, gde je j čvor grafa G u kojem je jedan spin usmeren na gore. Prema tome, $\{|j\rangle \mid j \in V(G)\}$ označava kompletni skup ortonormalnih vektora baze koji razapinje $\mathcal{S}_G$.

Kada se Hamiltonijan H_G restrihuje na podprostor $\mathcal{S}_G$, on se može predstaviti u gore navedenoj bazi, $N \times N$ matricom koja je identična matrici susedstva $A(G)$ bazičnog grafa G [**?**]. Vremenska evolucija sistema pod uticajem Hamiltonijana H_G može se interpretirati kao neprekidna vremenska kvantna šetnja na grafu G (ovakav prsitup su dali najpre Farhi i Gutmann u [**?**]; videti takođe i [**?**]). To je zato što se dinamika sistema definiše kao vremenska evolucija $N-$dimenzioalnog Hilbertovog prostora razapetog stanjima $\{|j\rangle\}$, gde je $j \in V(G)$, sa Hamiltonijanom datim matricom susedstva grafa G.

Spin sistem definisan na grafu G igra ulogu bešumnog kvantnog kanala. Na osnovu narednog razmatranja, videćemo da se neprekidne vremenske kvantne šetnje na grafu G mogu sagledati kao transfer kvantnog stanja duž kanala.

Proces transmisije kvantnog stanja iz A u B se ostvaruje u četiri koraka:

1. Inicijalizacija sistema stanjem $|0_A 0 \ldots 0 0_B\rangle$, koje odgovara konfiguraciji gde su svi spinovi usmereni na dole. Ovakvo stanje sistema predstavlja sopstveno stanje Hamiltonijana H_G sa energijom nula.

2. Kreiranje kvantnog stanja $|\psi\rangle_A \in \mathcal{H}_\mathcal{A}$ (u čvoru A) koje treba biti trnsmitovano. Neka je $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$, gde su $\alpha, \beta \in \mathrm{C}$ i $|\alpha|^2 + |\beta|^2 = 1$.

3. Vremenska evolucija sistema u nekom vremenskom intervalu, označenim sa t_0.

4. Beleženje stanja u čvoru B, koji je dat redukovanom matricom ρ_B prostora $\mathcal{H}_B$.

Stanje celokupnog spin sistema nakon drugog koraka dat je sa

$$\begin{aligned} |\Psi(t=0)\rangle &= |\psi_A 00\ldots 0_B\rangle & (2.3)\\ &= \alpha|0_A 00\ldots 0_B\rangle + \beta|1_A 00\ldots 0_B\rangle = \alpha|0\rangle + \beta|1\rangle. & (2.4)\end{aligned}$$

Stanje sistema evoluira nakon vremena t u

$$|\Psi(t)\rangle = \alpha|0\rangle + \sum_{j=1}^{N} \beta_j(t)|j\rangle,$$

gde su α i $\beta_j(t)$, $1 \leq j \leq N$, kompleksni koeficijenti takvi da je $|\alpha|^2 + \sum_{j=1}^{N} |\beta_j(t)|^2 = 1$. Inicijalni uslovi dati su sa $\beta_A(0) = \beta$ i $\beta_j(0) = 0$ za sve $j \neq A$. Koeficijent α se ne menja protokom vremena, jer je $|0\rangle$ sopstveno stanje Hamiltonijana H_G sa energijom nula. Zato za ovaj koeficijente nije potrebno uračunati faktor fazu tokom evolucije stanja.

Izlazno stanje u čvoru B nakon vremena t je dato redukovanom matricom gustine:

$$\begin{aligned} \rho_B(t) &= tr_{\mathcal{H}_{G\setminus\{B\}}} |\Psi(t)\rangle\langle\Psi(t)| & (2.5)\\ &= \begin{pmatrix} 1-|\beta_B(t)|^2 & \alpha\beta_B^*(t) \\ \alpha\beta_B^*(t) & |\beta_B(t)|^2 \end{pmatrix}. & (2.6)\end{aligned}$$

Mera preklapanja između ulaznog stanja, $\rho_A = |\psi\rangle\langle\psi|$ i izlaznog stanja data je sa tačnošću,

$$\begin{aligned} F(\rho_A, \rho_B(t)) &= tr\sqrt{{\rho_A}^{1/2}\rho_B(t){\rho_A}^{1/2}} & (2.7)\\ &= \sqrt{\langle\psi|\rho_B(t){\rho_A}^{1/2}|\psi\rangle} & (2.8)\\ &= \sqrt{|\alpha|^2(1-2|\beta_B|^2 + \beta_B\beta^* + \beta_B^*\beta) + |\beta_B|^2}, & (2.9)\end{aligned}$$

gde se podrazumeva da β_B zavisi od t.

Kako je komponenta $|0\rangle_A$ stanja $|\psi\rangle_A$ invarijantna tokom evolucije, dovoljno je fokusirati se na komponentu $|1\rangle_A$ stanja, tj. dovoljno je u formuli (**??**) odabrati $\alpha = 0$ i $\beta = 1$. Zato razmatramo odgovarajuću tačnost transfera

$$F_{AB}(t) = \beta_B(t) \equiv \langle A|e^{\imath H_G t}|B\rangle.$$

U ovoj glavi mi razmatramo samo savršeni transfer stanja, tj. ispitujemo uslov

$$|F_{AB}(t_0)| = 1, \tag{2.10}$$

za neko $0 < t_0 < +\infty$. Ako postoje čvorovi A i B, kao i realan pozitivan broj t_0 koji zadovoljavaju poslednju formulu, kažemo još da je ostvarena savršena komunikacija između A i B u vremenu t_0. Efekat modula u (**??**) se sastoji u tome da stanje čvora B posle transmisije nije više $|\psi\rangle$, već je dato sa

$$\alpha|0\rangle + e^{\imath\phi}\beta|1\rangle.$$

Faktor faze $e^{\imath\phi}$ je nezavisan od α i β, pri čemu je on poznata veličina za dati graf. Uz uslov da je graf osno-simetričan i ako se savršeni transfer između A i B odvija u vremenu t_0, to će se odvijati i u vremenu

$$t = (2n+1)t_0, \text{ za } n \in \mathbb{Z}.$$

2.2 Potrebni i dovoljni uslovi za egzistenciju PST na cirkularnim mrežama

Ovu sekciju započinjemo svojstvom kvantne periodičnosti mreža, jer ovo svojstvo predstavlja potreban uslov za egzistenciju PST. Daokazujemo da je uslov, da količnik razlike parova sopstvenih vrenosti mora biti racionalan broj, potreban za postojanje PST na težinskim cirkularnim spin mrežama. Na ovaj način uopštavamo i kompletiramo tvrđenje Teoreme 1 date u [**?**]. Drugim rečima, pokazujemo da je težinski cirkularni graf periodičan ako i samo ako je integralan. Takođe dajemo karakterizaciju težinksih integralnih cirkularnih grafova sa celobrojnim težinama. Glani rezutat ove sekcije je dat u odeljku 2.2.2 gde je ustanovljen jednostavan i opšti uslov za postojanje težinskih integralnih cirkularnih grafova sa PST svojstvom, u funkciji od sopstvenih vrednosti matrice susedstva tog grafa. U daljem navodimo neka osnovna svojstva cirkularnih grafova.

Cirkularne kvantne spin mreže sa identičnom spregom kubitova se opisuju cirkularnim grafovima. *Cirkularni graf* $G(n;S)$ je je definisan skupom čvorova $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ takvih da su čvorovi i i j susedni ako i samo ako je $i-j \equiv s \mod n$ za neko $s \in S$. Skup S zovemo *simbol* skupom grafa $G(n;S)$. Kako ćemo težište našeg razmatranja zadržati na neusmerenim grafovima bez petlji, pretpostavićemo da je $S = n - S = \{n-s \mid s \in S\}$ i $0 \notin S$. Može se uočiti da je stepen grafa $G(n;S)$ jednak $|S|$. Sopstvene vrednosti i vektori grafa $G(n;S)$ dati su sledećim formulama

$$\lambda_j = \sum_{s\in S} \omega_n^{js}, \quad v_j = [1\ \omega_n^j\ \omega_n^{2j} \cdots \omega_n^{(n-1)j}]^T, \tag{2.11}$$

gde je $\omega_n = e^{i\frac{2\pi}{n}}$ n-ti koren jedinice.

Težinski cirkularni digraf $G(n;C)$ je težinski digraf reda n, čija je matrica susedstva cirkularna, sa prvom vrstom jednakom vektoru $C = (c_0,\ldots,c_{n-1}) \in \mathbb{R}^n$. Podsetimo da se svaka vrsta cirkularne matrice dobija pomeranjem prethodne za jedno mesto udesno. Sopstvene vrednosti i vektori grafa $G(n;C)$ dati su formulama

$$\lambda_j = \sum_{i=0}^{n-1} c_i \omega_n^{ji}, \quad v_j = [1\ \omega_n^j\ \omega_n^{2j} \cdots \omega_n^{(n-1)j}]^T. \tag{2.12}$$

Ako je matrica susedstva digrafa $G(n;C)$ simetrična sa nulama na glavnoj dijagonali, onda kažemo da je $G(n;C)$ težinski cirkularni graf. Drugim rečima, za težinski vektor C mora da važi $c_i = c_{n-i}$ za $1 \le i \le n-1$. Cirkularne kvantne mreže sa fiksnim ali različitim sparivanjem među kubitovima su opisane težinskim cirkularnim grafovima. Elementi vektora vrste C predstavljaju jačinu sparivanja među kubitovima u mreži i zato pretpostavlajmo da su elementi vektora C nenegativni. Međutim, rezultati u ovoj sekciji u najvećem broju slučajeva ne iziskuju ovaj uslov. Naime, ovakve vrsta mreža odgovaraju Hamiltonijanima datim u (**??**) gde su konstante sparivanja $J_{ij} > 0$ [**?**].

2.2.1 Kvantna periodičnost na težinskim cirkulantnim grafovima

Neka je $\mathbb{H}$ Hilbertov prostor koji je pridružen kvantnoj mreži. Kažemo da je dinamika sistema periodična ako za svako stanje $|\psi\rangle \in \mathbb{H}$, postoji $t \in \mathbb{R}^+$, takvo da je $|\langle\psi|e^{-\imath At}|\psi\rangle| = 1$, [**?**]. Broj t predstavlja periodu sistema.

Evolucija sistema u odnosu na Hamiltonijan (**??**), se može izraziti korišećenjem matrice susedstva A_G grafa G, tj.,

$$|\psi(t)\rangle = e^{itA_G}|\psi(0)\rangle.$$

Korišćenjem činjenice da je matrica A_G simetrična, jednostvanim računom možemo doći do sledećih relacija

$$|\psi(t)\rangle = \sum_{k=1}^{n} \alpha_k e^{it\lambda_k}|\lambda_k\rangle, \quad |\psi(0)\rangle = \sum_{k=1}^{n} \alpha_k|\lambda_k\rangle,$$

gde su $\lambda_k \in \mathbb{R}$, za $1 \leq k \leq n$, sopstvene vrednosti matrice A_G i $|\lambda_k\rangle$ njihovi odgovarajući sopstveni vektori.

Pretpostavimo da PST postoji između stanja sistema $|\psi(t_1)\rangle$ i $|\psi(t_2)\rangle$. Korišćenjem uslova periodičnosti $|\psi(t_1)\rangle = e^{i\phi}|\psi(t_2)\rangle$ imamo da je

$$\sum_{k=1}^{n} \alpha_k e^{it_1\lambda_j}|\lambda_j\rangle = |\psi(t_1)\rangle = e^{i\phi}|\psi(t_2)\rangle = \sum_{k=1}^{n} \alpha_k e^{i\phi}e^{it_2\lambda_j}|\lambda_j\rangle.$$

Kako su vektori $|\lambda_j\rangle$, za $1 \leq j \leq n$ linearno nezavisni, imamo

$$e^{i[(t_2-t_1)\lambda_j+\phi]} = 1, \quad \text{tj.} \quad (t_2-t_1)\lambda_j + \phi = 2k_j\pi,$$

za neko $k_j \in \mathbb{Z}$, $1 \leq j \leq n$. Eliminacijom $t_2 - t_1$, ϕ i $k_j \in \mathbb{Z}$, $j = 1, \ldots, n$, iz gornjeg sistema, za svaku četvorku λ_k,λ_j, λ_m, λ_h, (gde je $\lambda_m \neq \lambda_h$), dobijamo

$$\frac{\lambda_k - \lambda_j}{\lambda_m - \lambda_h} \in \mathbb{Q}. \tag{2.13}$$

U nastavku ćemo umesto termina kvantna mreža koristiti termin graf smatrajući ih ekvivalentnim.

Teorema 2.2.1. *Neka je $G = G(n, C)$ težinski cirkularni graf bez petlji, sa celobrojnim vektorom C pri čemu je suma koordinata vektora različita od nule. Tada G zadovoljava uslov (**??**) ako i samo ako je integralan.*

Dokaz. Pretpostavimo da G zadovoljava uslov (**??**). Dokazaćemo da su sve sopstvene vrednosti racionalni brojevi.

Iz relacije (**??**) direktno dobijamo $\lambda_0 = \sum_{i=0}^{n-1} c_i \in \mathbb{Z}$. Neka je λ_i proizvoljna sopstvena vrednost grafa G. Ako je $\lambda_i = \lambda_0$, očigledno je i $\lambda_i \in \mathbb{Z}$.

Pretpostavimo sada da je $\lambda_i \neq \lambda_0$. Koristeći (**??**), imamo $\frac{\lambda_j-\lambda_0}{\lambda_i-\lambda_0} = a_j \in \mathbb{Q}$ za $1 \leq j \leq n-1$, odakle sledi da je

$$\lambda_j = a_j\lambda_i + (1 - a_j)\lambda_0. \tag{2.14}$$

Kako G nema petlji, to je $c_0 = 0$, pa je suma sopstvenih vrednosti grafa G:

$$\sum_{j=0}^{n-1} \lambda_j = \sum_{j=0}^{n-1}\sum_{i=1}^{n-1} c_i\omega_n^{ji} = \sum_{i=1}^{n-1}\sum_{j=0}^{n-1} c_i\omega_n^{ji} = nc_0 + \sum_{i=1}^{n-1} c_i\frac{\omega_n^{in} - 1}{\omega_n^i - 1} = 0. \tag{2.15}$$

Pretpostavimo da je $\sum_{j=1}^{n-1} a_j = 0$. Iz relacije (**??**) proizilazi

$$\sum_{j=1}^{n-1} \lambda_j = \lambda_0 \sum_{j=1}^{n-1}(1 - a_j).$$

Korišćenjem (**??**) poslednja relacija se svodi na $-\lambda_0 = (n-1)\lambda_0$. Odavde dobijamo da je $\lambda_0 = 0$, što je kontradikcija.

Pretpostavimo da je $\sum_{j=1}^{n-1} a_j \neq 0$. Koristeći (**??**), relacija (**??**) se svodi na

$$\sum_{j=0}^{n-1} \lambda_j = \lambda_i \sum_{j=0}^{n-1} a_j + \lambda_0 \sum_{j=0}^{n-1} (1 - a_j) = 0,$$

odakle dalje imamo

$$\lambda_i = \frac{\lambda_0 (n - 1 - \sum_{j=0}^{n-1} a_j)}{\sum_{j=0}^{n-1} a_j} \in \mathbb{Q},$$

te zato iz (**??**), zaključujemo da je $\lambda_j \in \mathbb{Q}$ za svako $0 \leq j \leq n-1$. Dakle, kako su sve sopstvene vrednosti racionalne nule polinoma sa celobrojnim koeficijentima, zaključujeno da su i celobrojne.

Suprotan smer tvrđenja trivijalno važi. □

Posledica 2.2.2. *Neka je $G = G(n, C)$ težinski cirkularni graf zadat u odnosu na Hamiltonijan (**??**), čiji je vektor C celobrojan. Tada G zadovoljava uslov (**??**) ako i samo ako je integralan.*

Ova posledica nas navodi na zaključak da ako graf $G = G(n, C)$ poseduje svojstvo PST, onda mora biti integralan. Zato ćemo u nastavku dati karakterizaciju težinskih integralnih cirkularnih grafova, čije su težine celobrojne. Takođe, korišćenjem Ramanudžanovih suma, možemo dati eksplicitnu formulu za sopstvene vrednosti takvih grafova.

Neka je D_n skup svih pozitivnih delioca broja n, manjih od n. Označimo sa

$$G_n(d) = \{k \ : \ \gcd(k, n) = d, \ 1 \leq k \leq n-1\}.$$

Definišimo *ciklotomični polinom* stepena n (videti [**?**]),

$$\Phi_n(x) = \prod_{0<i<n, \ gcd(i,n)=1} (x - \omega_n^i),$$

čija će osnovna svojstva biti korišćenja u narednoj teoremi.

Teorema 2.2.3. *Težinski integralni cirkularni graf $G(n; C)$ sa celobrojnim težinama je integralan ako i samo je $c_i = c_j$ za svako $i, j \in G_n(d)$ i proizvoljni delilac $d \in D_n$.*

Dokaz. Za delilac d broja n, definišimo polinom

$$\Phi_{n,d}(x) = \prod_{i \in G_n(d)} (x - \omega_n^i).$$

Uočimo najpre da je uslov $gcd(i, n) = d$ ekvivalentan uslovu $gcd(i/d, n/d) = 1$. Na osnovu jednakosti $\omega_n^i = \omega_{n/d}^{i/d}$, za $i \in G_n(d)$, dobijamo da su monični polinomi $\Phi_{n,d}(x)$ i $\Phi_{n/d}(x)$ identični.

($\Leftarrow$:) Pretpostavimo da su brojevi c_i međusobno jednaki za svako $i \in G_n(d)$ i neki delilac $d \in D_n$. Primetimo da se j-ta sopstvena vrednost grafa $G(n; C)$ može zapisati na sledeći način

$$\lambda_j = \sum_{i=0}^{n-1} c_i \omega_n^{ji} = \sum_{d \in D_n} \sum_{i \in G_n(d)} c_i \omega_n^{ji} = \sum_{d \in D_n} c_d \sum_{i \in G_n(d)} \omega_n^{ji},$$

gde smo sa c_d označili vrednost c_i za svako $i \in G_n(d)$. U poslednjoj formuli smo iskoristili činjenicu da se skup Z_n može razbiti kao $\cup_{d\in D_n} G_n(d)$.

Označimo sa

$$\mu_{j,d} = \sum_{i\in G_n(d)} \omega_n^{ji} = \sum_{i\in G_{n/d}(1)} \omega_{n/d}^{ji}$$

i dokažimo da je $\mu_{j,d} \in \mathbb{Z}$ for $0 \le j \le n-1$.

Neka je skup $G_{n/d}(1) = \{i_1, \ldots, i_{\varphi(n/d)}\}$. Iz Vijetovih formula i svojstva da su svi koeficijenti ciklotomičnih polinoma celobrojni, zaključujemo da su koeficijenti polinoma $\Phi_{n/d}(x)$ jednaki

$$s_j(\omega_{n/d}^{i_1}, \ldots, \omega_{n/d}^{i_{\varphi(n/d)}}) \in \mathbb{Z},$$

gde je s_j, j-ti elementarni simetrčni polinom za $1 \le j \le \varphi(n/d)$.

Takođe, koristeći Newton–Girardove formule (videti [**?**]), dobijamo sledeće identitete

$$\mu_{j,d} = (-1)^{j+1} j s_j(\omega_{n/d}^{i_1}, \ldots, \omega_{n/d}^{i_{\varphi(n/d)}}) - \sum_{k=1}^{j-1} (-1)^{k+j} \mu_{k,d}\ s_{j-k}(\omega_{n/d}^{i_1}, \ldots, \omega_{n/d}^{i_{\varphi(n/d)}}).$$

Primenom matematičke indukcije imamo da je $\mu_{j,d} \in \mathbb{Z}$ for $1 \le j \le \varphi(n/d)$. Kako $\mu_{j,d}$ predstavlja sumu j-tih stepena $\varphi(n/d)$ promenljivih, možemo zaključiti da je $\mu_{j,d} \in \mathbb{Z}$ za svako $0 \le j \le n/d$.

($\Rightarrow$:) Pretpostavimo sada da su sve sopstvene vrednosti grafa $G(n; C)$ celobrojne,

$$\lambda_j = \sum_{i=0}^{n-1} c_i \omega_n^{ji} \in \mathbb{Z}$$

za svako $0 \leqslant j \leqslant n-1$. Kako vrednost λ_j predstavlja sumu j-tih stepena korena ω_n^i, zaključujemo da je $\lambda_j \in \mathbb{Z}$ za svako $j \ge n$, takođe. Prema Newton–Girardovim formulama dobijamo sledeće identitete

$$(-1)^j j s_j(\underbrace{1, \ldots, 1}_{c_0}, \underbrace{\omega_n, \ldots, \omega_n}_{c_1}, \ldots, \underbrace{\omega_n^{n-1}, \ldots \omega_n^{n-1}}_{c_{n-1}}) + \tag{2.16}$$

$$\sum_{k=1}^{j} (-1)^{k+j} \lambda_k\ s_{j-k}(\underbrace{1, \ldots, 1}_{c_0}, \underbrace{\omega_n, \ldots, \omega_n}_{c_1}, \ldots, \underbrace{\omega_n^{n-1}, \ldots \omega_n^{n-1}}_{c_{n-1}}) = 0$$

za svako $1 \le j \le n$, gde je s_j j-ti elementarni simetrični polinom. Primenom matematičke indukcije imamo

$$s_j(\underbrace{1, \ldots, 1}_{c_0}, \underbrace{\omega_n, \ldots, \omega_n}_{c_1}, \ldots, \underbrace{\omega_n^{n-1}, \ldots \omega_n^{n-1}}_{c_{n-1}}) \in \mathbb{Q}.$$

Dalje, korišćenjem Vietovih formula, sledi da je $p(x) = \prod_{i=0}^{n-1} (x - \omega_n^i)^{c_i} \in \mathbb{Q}[x]$, jer su koificijenti polinoma $p(x)$, do na znak, upravo jednaki $s_j(\underbrace{1, \ldots, 1}_{c_0}, \underbrace{\omega_n, \ldots, \omega_n}_{c_1}, \ldots, \underbrace{\omega_n^{n-1}, \ldots \omega_n^{n-1}}_{c_{n-1}})$.

Neka je i proizvoljan indeks $0 \le i \le n-1$ takav da je $c_i \ne 0$ za $i \in G_n(d)$. Na osnovu osnovnih svojstava ciklotomičnih polinoma [**?**], minimalan nenula polinom nad $\mathbb{Q}$, čija je nula ω_n^i, je $\Phi_{n,d}(x)$. Ovo dalje znači da $\Phi_{n,d}(x) \mid p(x)$, kao i da su brojevi c_i međusobno jednaki za svako $i \in G_n(d)$ i $d \in D_n$. $\square$

U slučaju netežinskih grafova ($c_i \in \{0,1\}$), iz Teoreme **??** može se videti da je $G(n;C)$ integralan ako i samo ako važi da su dva čvora a i b susedna ukoliko $a-b \in G_n(d)$ za neki $d \in D \subseteq D_n$. Odavde sledi da je cirkularni graf sa celobrojnim spektrom jednoznačno određen redom n i skupom delilaca $D \subseteq D_n$. Zato ih označavamo sa $\mathrm{ICG}_n(D)$.

Označimo sa $c(j,n) = \sum_{i \in G_n(1)} \omega_n^{ij}$. Izraz $c(j,n)$ poznat je pod nazivom *Ramanudžanova suma* ([**?**, p. 55]). Sopstvene vrednosti grafa $G(n,C)$ se mogu izraziti korišćenjem formula za Ramanudžanove sume:

$$c(j,n) = \mu(t_{n,j}) \frac{\varphi(n)}{\varphi(t_{n,j})}, \quad t_{n,j} = \frac{n}{\gcd(n,j)} \tag{2.17}$$

gde funkcija μ označava Mebijusovu funkciju definisanu kao

$$\mu(n) \;=\; \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{ako je } n \text{ deljiv kvadratom prostog broja} \\ (-1)^k, & \text{ako je } n \text{ proizvod } k \text{ različitih prostih brojeva.} \end{cases} \tag{2.18}$$

Prema notaciji korišćenoj u prethodnoj formuli, j-ta sopstvena vrednost grafa $G(n;C)$ data je sa

$$\lambda_j = \sum_{d \in D_n} c_d \sum_{i \in G_n(d)} \omega_n^{ji} = \sum_{d \in D_n} c_d \, c(j, n/d), \quad 0 \le j \le n-1. \tag{2.19}$$

Možemo uočiti sledeća osnovna svojstva Ramanudžanovih funkcija koja će biti korišćena u nastavku.

Propozicija 2.2.4. *Za proizvoljne prirodne brojeve n, j i d delilac broja n, važi*

$$c(n/2+1, n/d) \;=\; \begin{cases} -\mu(n/d), & n \in 4\mathbb{N}+2,\ d \in 2\mathbb{N}+1 \\ \mu(n/d), & \textit{u suprotnom} \end{cases} \tag{2.20}$$

$$c(0, n/d) \;=\; \varphi(n/d), \tag{2.21}$$

$$c(1, n/d) \;=\; \mu(n/d), \tag{2.22}$$

$$c(2, n/d) \;=\; \begin{cases} \mu(n/d), & n/d \in 2\mathbb{N}+1 \\ \mu(n/2d), & n/d \in 4\mathbb{N}+2 \\ 2\mu(n/2d), & n/d \in 4\mathbb{N} \end{cases} \tag{2.23}$$

$$c(n/2, n/d) \;=\; \begin{cases} \varphi(n/d), & d \in 2\mathbb{N} \\ -\varphi(n/d), & d \in 2\mathbb{N}+1 \end{cases} \tag{2.24}$$

$$c(n/2+1, n/d) \;=\; \begin{cases} -\mu(n/d), & n \in 4\mathbb{N}+2,\ d \in 2\mathbb{N}+1 \\ \mu(n/d), & \textit{u suprotnom} \end{cases} \tag{2.25}$$

$$c(j,2) \;=\; \begin{cases} -1, & j \in 2\mathbb{N}+1 \\ 1, & j \in 2\mathbb{N} \end{cases} \tag{2.26}$$

$$c(j,4) \;=\; \begin{cases} 0, & j \in 2\mathbb{N}+1 \\ -2, & j \in 4\mathbb{N}+2 \\ 2, & j \in 4\mathbb{N} \end{cases} . \tag{2.27}$$

Dokaz. Izvođenje se svodi na direktno korišćenje relacije (**??**). U cilju ilustracije izvođenja, dokazaćemo na primer relaciju (1.13). Za proizvoljan prost neparan delilac $p \mid n/d$ važi $p \mid n/2$ i zato $p \nmid n/2+1$. Na osnovu toga, zaključujemo da $gcd(n/2+1, n/d) \in \{1, 2\}$ i

$$\gcd(n/2+1, n/d) = \begin{cases} 2, & n \in 4\mathbb{N}+2,\ d \in 2\mathbb{N}+1 \\ 1, & \text{u suprotnom} \end{cases}, t_{n/d,n/2+1} = \begin{cases} n/2d, & n \in 4\mathbb{N}+2,\ d \in 2\mathbb{N}+1 \\ n/d, & \text{u suprotnom} \end{cases}. \tag{2.28}$$

Konačno dobijamo

$$c(n/2+1, n/d) = \begin{cases} \mu(n/2d) = -\mu(n/d), & n \in 4\mathbb{N}+2,\ d \in 2\mathbb{N}+1 \\ \mu(n/d), & \text{u suprotnom} \end{cases}. \tag{2.29}$$

□

2.2.2 PST na težinskim cirkularnim grafovima

U ovom delu ćemo dati opšti uslov za postojanje PST-a na težinskim cirkularnim grafovima sa celobrojnim težinama. Težinski integralni cirkularni graf reda n i sa skupom težina C označavaćemo sa WICG$(n; C)$. Prema notaciji iz Teoreme **??**, indeksiraćemo težine iz skupa C deliocima $d \in D_n$, tj. $C = \{c_d \mid d \in D_n\}$. Drugim rečima, stavljamo da je $c_i = c_d$, za svako $0 \le i \le n-1$ takvo da je $\gcd(i, n) = d$.

Za dati graf G kažemo da PST postoji između čvorova a i b ako postoji positivan realan broj t takav da je

$$|\langle a|e^{iAt}|b\rangle| = 1. \tag{2.30}$$

Za težinski cirkularni graf $G = G(n; C)$, neka je $v_j = [1, \omega_n^j, \ldots, \omega_n^{j(n-1)}]^T$ proizvoljan sopstveni vektor i $v_j^* = [1, \omega_n^{-j}, \ldots, \omega_n^{-j(n-1)}]$ konjugovano-transponovani vektor vektora v_j. Dalje važi da je $A = \frac{1}{n}\sum_{l=0}^{n-1} \lambda_l v_l v_l^*$ i $e^{iAt} = \frac{1}{n}\sum_{l=0}^{n-1} e^{i\lambda_l t} v_l v_l^*$, odakle sledi

$$|\langle a|e^{iAt}|b\rangle| = 1 \Leftrightarrow \left|\frac{1}{n}\sum_{l=0}^{n-1} e^{i\lambda_l t}\omega_n^{la}\omega_n^{-lb}\right| = \left|\frac{1}{n}\sum_{l=0}^{n-1} e^{i\lambda_l t}\omega_n^{l(a-b)}\right| = 1. \tag{2.31}$$

Iz nejednakosti trougla očigledno je $|\langle a|e^{iAt}|b\rangle| \le 1$, gde je jednakost zadovoljena ako i samo ako su svi sabirci u (**??**) jednaki, tj. imaju isti argument. Drugim rečima, PST postoji u G ako i samo ako je

$$e^{i\lambda_0 t} = e^{i\lambda_1 t + i\frac{2\pi}{n}(a-b)} = \cdots = e^{i\lambda_{n-1} t + i\frac{2(n-1)\pi}{n}(a-b)}. \tag{2.32}$$

Poslednji izraz ekvivalentan je sa

$$\lambda_0 t \equiv_{2\pi} \lambda_1 t + \frac{2\pi}{n}(a-b) \equiv_{2\pi} \cdots \equiv_{2\pi} \lambda_{n-1} t + \frac{2(n-1)\pi}{n}(a-b).$$

Relacija $\equiv_{2\pi}$ je definisana na sledeći na čin: $A \equiv_{2\pi} B$ ako $\frac{(A-B)}{2\pi} \in \mathbb{Z}$. Primetimo da (**??**) zavisi od a i b samo kao funkcija od $a-b$. Zato možemo, bez gubljenja opštosti, uzeti da je $b = 0$. Oduzimanjem susednih kongruencija u prethodnoj jednakosti i zamenom $b = 0$ dobijamo da je relacija (**??**) ekvivalentna sa sledećih $n-1$ uslova

$$(\lambda_{j+1} - \lambda_j)t_1 + \frac{a}{n} \in \mathbb{Z}, \quad j = 0, \ldots, n-2,$$

gde je $t_1 = t/(2\pi)$. Iz poslednjih izraza može se zaključiti da ako PST postoji u G, onda je t_1 racionalan, tj. postoje celi brojevi p i q takvi da je $t_1 = p/q$ i $\gcd(p, q) = 1$.

Ovom diskusijom dolazimo do sledećeg rezultata.

Teorema 2.2.5. *U težinskom cirkularnom grafu $G(n; C)$ postoji PST među čvorovima a i 0 ako i samo ako postoje celi brojevi p i q takvi da je $\gcd(p, q) = 1$ i*

$$\frac{p}{q}(\lambda_{j+1} - \lambda_j) + \frac{a}{n} \in \mathbb{Z}, \tag{2.33}$$

za svako $j = 0, \ldots, n-2$.

Takođe se može uočiti da ako PST postoji u $G(n; C)$, sledeći izrazi se mogu izvesti iz (**??**)

$$\frac{p}{q}(\lambda_{j+2} - \lambda_j) + \frac{2a}{n} \in \mathbb{Z}, \quad j = 0, 1, \ldots, n-3. \tag{2.34}$$

Naredna posledica proizilazi iz Teoreme **??** i biće korišćena kao kriterijum za nepostojanje PST u grafu.

Posledica 2.2.6. *Ako je $\lambda_j = \lambda_{j+1}$ za neko $0 \leq j \leq n-2$ onda PST ne postoji među proizvoljnim čvorovima a i b grafa $G(n; C)$.*

Dokaz. Bez gubljenja opštosti uzmimo da je $b = 0$. Iz Teoreme **??** imamo da je $a/n \in \mathbb{Z}$, t.j. $n \mid a$. A poslednje nije moguće jer je $0 < a < n$. □

Naredna tvrđenja se odnose na težinske integralne cirkularne grafove, koristeći prethodne rezultate dobijene za $G(n; C)$.

Teorema 2.2.7. *PST ne postoji u* WICG$(n; C)$ *ukoliko je za svaki $c_d \neq 0$, n/d neparan. Za n parno, ako postoji PST u* WICG$(n; C)$ *između čvorova a i 0, onda je $a = n/2$.*

Dokaz. Pretpostavimo da je n/d neparan za svaki $d \in D$, pri čemu je $c_d \neq 0$.

Koristeći relacije (1.10) i (1.11), Propozicije **??** lako se može dokazati da je

$$\lambda_1 = \lambda_2 = \sum_{d \in D_n} c_d \, \mu(n/d).$$

Na osnovu Posledice **??** imamo da ne postoji PST u WICG$(n; C)$.

Pretpostavimo sada da je n paran. Uočimo da je $\gcd(n/2+1, n/d) = \gcd(n/2-1, n/d) \in \{1, 2\}$. Odavde sledi da je $t_{n/d,n/2+1} = t_{n/d,n/2-1}$, tj. $c(n/2-1, n/d) = c(n/2+1, n/d)$. Korišćenjem poslednjeg izraza dokazujemo

$$\lambda_{n/2-1} = \sum_{d \in D_n} c_d \, c(n/2-1, n/d) = \sum_{d \in D_n} c_d \, c(n/2+1, n/d) = \lambda_{n/2+1}.$$

Korišćenjem (**??**) imamo da je $(2a)/n \in \mathbb{Z}$, što je moguće samo za $a = n/2$. □

Prema prethodnoj teoremi, PST može postojati u WICG$(n; C)$ samo za n parno i između čvorova 0 i $a = n/2$ (tj., između b i $n/2 + b$). Zato ćemo u ostatku poglavlja pretpostaviti da je n parno i $a = n/2$.

Takođe nećemo eksplicitno navoditi ulazne i izlazne čvorove, već ćemo samo reći da PST postoji u grafu WICG$(n; C)$. Relacija (**??**) sada postaje

$$\frac{p(\lambda_{j+1}-\lambda_j)}{q}+\frac{1}{2}\in\mathbb{Z}. \tag{2.35}$$

Za proizvoljan prost broj p i prirodan broj n, sa $S_p(n)$ označićemo mnajveći broj α takav da $p^\alpha \mid n$. Sledeća teorema daje kriterijum za egzistenciju PST u WICG$(n;C)$

Teorema 2.2.8. *PST postoji u grafu* WICG$(n;C)$ *ako i samo ako postoji* $m\in\mathbb{N}_0$ *takav da za svako* $j=0,1,\dots,n-2$ *važi*

$$S_2(\lambda_{j+1}-\lambda_j)=m. \tag{2.36}$$

Dokaz. Neka je $\lambda_{j+1}-\lambda_j=2^{s_j}m_j$ gde je $s_j=S_2(\lambda_{j+1}-\lambda_j)\geq 0$ i m_j neparan broj za svako $j=0,1,\dots,n-2$.
($\Rightarrow$:) Pretpostavimo da WICG$(n;C)$ ima PST. Na osnovu Teoreme **??**, postoje uzajamno prosti brojevi p,q takvi da važi (**??**). Napišimo pomenutu relaciju u sledećoj formi

$$\frac{2^{s_j+1}pm_j+q}{2q}\in\mathbb{Z}. \tag{2.37}$$

Iz poslednje jednakosti zaključujemo da $q \mid 2^{s_j+1}m_j$ $(\gcd(p,q)=1)$ i $2 \mid q$. Takođe, mora postojati nenegativan ceo broj s_q i $m_q\in 2\mathbb{N}+1$ takvi da je $q=2^{s_q+1}m_q$ gde je $s_q\leq s_j$ i $m_q \mid m_j$ za svako $j=0,1,\dots,n-2$. Zamenom u (**??**) dobijamo

$$\frac{2^{s_j-s_q}p\frac{m_j}{m_q}+1}{2}\in\mathbb{Z},$$

odakle direktno sledi da $s_j=s_q=S_2(q)-1$. Stavljajući da je $m=S_2(q)-1$ dobijamo (**??**).
($\Leftarrow$:) Pretpostavimo da važi (**??**). Neka je $q=2^{m+1}$ i $p=1$. Tada je

$$\frac{p(\lambda_{j+1}-\lambda_j)}{q}+\frac{1}{2}=\frac{m_j+1}{2}\in\mathbb{Z},$$

za svaki $j=0,1,\dots,n-2$. Prema Teoremi **??** imamo da PST postoji u WICG$(n;C)$. □

Sledeće tvrđenje direktno sledi iz Teoreme **??**.

Posledica 2.2.9. *Neka je* WICG$(n;C)$ *graf sa PST svojstvom. Jedno od sledeća dva tvrđenja mora da važi*

1. $\lambda_j\equiv\lambda_{j+1} \mod 2$ *za* $0\leq j\leq n-1$ *(sve sopstvene vrednosti* λ_j *su iste parnosti).*
2. $\lambda_j\equiv\lambda_{j+1}+1 \mod 2$ *za* $0\leq j\leq n-1$ *(sopstvene vrednosti niza* λ_j *,* $0\leq j\leq n-1$ *naizmenično menjaju parnost.*

PST može postojati na mreži samo ako je mreža (graf) povezana. Graf ICG$_n(D)$ je povezan ako i samo ako je

$$\gcd(n,d_1,d_2,\dots d_t)=1,$$

za svako $d_i\in D$ i $1\leq i\leq t$ (videti Teoremu **??**). Zato ćemo do kraja odeljka pretpostaviti da su grafovi ICG$_n(D)$ i WICG$(n;C)$ povezani. Naglasimo, da je WICG$(n;C)$ povezan ako je njemu odgovarajući netežinski graf ICG$_n(D)$ gde je $D=\{d \mid n \ : \ c_d\neq 0\}$, takođe povezan.

Kako se unitarni Kejlijevi grafovi proučavaju kao posebna klasa grafova, ilustrovaćemo primenu uslova datih u Teoremama **??**, **??** i Posledici **??**, i dokazati negzistenciju PST na njima.

2.2.3 PST na unitarnim Kejlijevim grafovima

Unitarni Kejlijevi grafovi se mogu tretirati kao podklasa integralnih cirkularnih grafova kada je $D = \{1\}$. Primetimo da ako je $D = \{d\}$ onda je $\mathrm{ICG}_n(D)$ povezan ako i samo ako je $d = 1$. Dakle, jedini integralni cirkularni grafovi sa skupom delioca $D = \{d\}$ koji bi mogli imati PST su unitarni Kejlijevi grafovi. Glavi rezultat ove podsekcije je nepostojanje PST na unitarnim Kejlijevim grafovima, osim u slučajevim za K_2 i C_4.

Sledeće tvrđenje rešava slučaj kada su n i $n/2$ deljivi kvadratom prostog broja.

Propozicija 2.2.10. *Ako su n i $n/2$ deljivi nekim kvadratima prostih brojeva, tada PST ne postoji u* $\mathrm{ICG}_n(1)$.

Dokaz. Na osnovu Propozicije **??** imamo da je $\lambda_1 = \lambda_2 = 0$, jer važi $\mu(n) = \mu(n/2) = 0$. Primenom Posledice **??** dobijamo da PST ne postoji u $\mathrm{ICG}_n(1)$. □

Razmotrimo slučaj kada je $n = 2s$ gde s nije deljiv kvadratom prostog broja.

Lema 2.2.11. *Ako je $n = 2s$ gde s nije deljiv kvadratom prostog broja, jedini unitarni Kejlijevi grafovi koji imaju PST su K_2 i C_4.*

Dokaz. Pretpostavimo da $\mathrm{ICG}_n(1)$ ima PST. Tada je $\lambda_1 = \mu(n)$ i

$$\lambda_2 = \begin{cases} \mu(s), & s \in 2\mathbb{N}+1 \\ 2\mu(s), & s \in 2\mathbb{N} \end{cases}.$$

Štaviše, kako je $\mu(s) = -\mu(n)$ za $s \in 2\mathbb{N}+1$ i $\mu(n) = 0$ za $s \in 2\mathbb{N}$ zaključujemo da je $|\lambda_1 - \lambda_2| = 2$. Iz relacije (**??**), zamenom $a = n/2$ dobijamo

$$\frac{2p}{q} + \frac{1}{2} \in \mathbb{Z} \quad \text{or} \quad -\frac{2p}{q} + \frac{1}{2} \in \mathbb{Z}. \tag{2.38}$$

Pretpostavimo da je prvi iskaz tačan. Onda je $\frac{4p+q}{2q} \in \mathbb{Z}$, te stoga važi $q \mid 4p$, odakle sledi da $q \mid 4$. Sa druge strane imamo da $2 \mid q$, pa zato postoje dve mogućnosti za q, $q = 2$ i $q = 4$. Slučaj $q = 2$ je nemoguć jer $(2p+1)/2 \notin \mathbb{Z}$ za svako $p \in \mathbb{Z}$. Ostaje da mora biti $q = 4$. Isti zaključak se može izvesti analogno ako se pretpostavi da je drugi iskaz u (**??**) tačan.

Neka je $n \geq 3$ i $s \in 2\mathbb{N}+1$. Uočimo da je $\lambda_s = -\varphi(n)$ i $\lambda_{s-1} = -\mu(n)$, gde je $\varphi(n)$ paran i $\mu(n)$ neparan ($n = 2s$ nije deljiv kvadratom prostog broja). Odavde sledi da je $|\lambda_{s-1} - \lambda_s|$ neparan. Ovo je u kontradikciji sa Teoremom **??** jer je $S_2(|\lambda_1 - \lambda_2|) \neq S_2(|\lambda_{s-1} - \lambda_s|)$.

Neka je $n > 4$ i $s \in 2\mathbb{N}$. Tada je $\lambda_s = -\varphi(n) \in 4\mathbb{N}$ i $\lambda_{s-1} = 0$. Odavde sledi da je $S_2(|\lambda_{s-1} - \lambda_s|) \geq 2$, a kako je $S_2(|\lambda_1 - \lambda_2|) = 1$ ovo je ponovo kontradikcija sa Teoremom **??**.

Uslovi $n \leq 2$ i $s \in 2\mathbb{N}+1$ su zadovoljeni samo ako je $n = 2$, odakle direktnim izračunavanjem sopstvenih vrednosti i proverom u (**??**) dobijamo da $\mathrm{ICG}_2(1)$ ima PST. Primetio da je $\mathrm{ICG}_2(1) = K_2$.

Konačno, uslovi $n \leq 4$ and $s \in 2\mathbb{N}$ su zadovoljeni samo ako je $n = 4$. Takođe, direktnom proverom dobijamo da $\mathrm{ICG}_4(1)$ ima PST. U ovom slučaju je $\mathrm{ICG}_4(1) = C_4$. □

Na osnovu Teoreme **??**, Propozicije **??** i Leme **??** glavni rezultat sekcije se izvodi direktno.

Teorema 2.2.12. *Jedini unitarni Kejlijevi grafovi koji imaju PST su K_2 i C_4.*

2.3 Karakterizacija cirkularnih grafova sa PST svojstvom

U ovom delu proučavamo cirkularne mreže u kojima postoji PST, na osnovu rezultata datih u [**?**, **?**, **?**, **?**, **?**, **?**, **?**]. Najpre ćemo opisati relevantna svojstva spektra grafa $\mathrm{ICG}_n(\widetilde{D_1})$ gde je $\widetilde{D_1} = \{d \in D \mid 4 \nmid n/d\}$, koja se koriste u nastavku. Glavni rezultat sekcije predstavlja karakterizaciju grafova $\mathrm{ICG}_n(D)$ koji imaju PST. Dokazujemo da takvi grafovi imaju PST ako i samo ako $n \in 4\mathbb{N}$ i $D = \widetilde{D_3} \cup D_2 \cup 2D_2 \cup 4D_2 \cup \{n/2^a\}$, gde $\widetilde{D_3} = \{d \in D \mid n/d \in 8\mathbb{N}\}$, $D_2 = \{d \in D \mid n/d \in 8\mathbb{N}+4\} \setminus \{n/4\}$ i $a \in \{1,2\}$. Koristeći prethodni rezultat dokazujemo da je kvantno komunikaciono rastojanje (rastojanje čvorova između kojih postoji PST) jednako jedan ako je $n/2 \in D$ ili jednako dva ako je $n/4 \in D$. Takođe ćemo opisati spektar integralnih cirkularnih grafova koji imaju PST. Sekciju završavamo formulom za broj grafova $\mathrm{ICG}_n(D)$ koji imaju PST u funkciji reda grafa n. Pomenuti rezultati daju odgovore na neka od otvorenih pitanja postavljenih u [**?**, **?**, **?**]. U daljem, navodimo neke osnovne terminološke postavke koje će se koristiti u nastavku sekcije.

Neka je $\mathrm{ICG}_n(D)$ proizvoljan integralni cirkularni graf. Definišimo skupove $D_i \subseteq D$ za $0 \leq i \leq l$, gde je $l = S_2(n)$, na sledeći način

$$D_i = \{d \in D \mid S_2(n/d) = i\}.$$

Zbog jednostavnijeg izlaganja takođe definišemo skupove:
$\widetilde{D_1} = D_0 \cup D_1$ i $\widetilde{D_3} = \cup_{i \geq 3} D_i$.
Uvedimo i notaciju kD za skup $\{kd \mid d \in D\}$ gde je k prirodan broj.

2.3.1 Spektar integralnih cirkularnih grafova $\mathrm{ICG}_n(\widetilde{D_1})$

U ovom delu se bavimo integralnim cirkularnim grafovima $\mathrm{ICG}_n(D)$ takvim da za svaki delilac $d \in D$ važi da $4 \nmid \frac{n}{d}$. U ostatku ove sekcije razmatraćemo samo ovakve klase grafova, ukoliko se ne naglasi drugačije.

U Lemama **??** i **??** pokazujemo neka svojstva Ramanudžanovih funkcija.

Tokom sekcije, pretpostavljamo da n ima sledeću kanonsku reprezentaciju $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gde su $p_1 < p_2 < \ldots < p_k$ različiti prosti faktori, i $\alpha_i \geqslant 1$ za $1 \leq i \leq k$ i $\alpha_0 \geq 0$.

Lema 2.3.1. *Za $n \geq 2$ je $c(j,n) \in 2\mathbb{N}+1$ ako i samo ako $4 \nmid n$ i $j = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1} J$ za neki J takav da je $\gcd(J,n) \in \{1,2\}$.*

Dokaz.

($\Rightarrow$:) Pretpostavimo da je $c(j,n)$ neparan. Kako je $c(j,n) = \mu(t_{n,j})\varphi(n)/\varphi(t_{n,j})$, sledi da je $\mu(t_{n,j}) = \pm 1$, tj. $t_{n,j}$ nije deljiv kvadratom prostog broja i $\varphi(n)/\varphi(t_{n,j})$ je takođe neparan.

Pretpostavimo da za naki neparan prost broj p_i važi da $p_i \nmid t_{n,j}$. Neka je takođe $n' = n/p_i^{\alpha_i}$. Kako važi da $t_{n,j} \mid n'$ i na taj način $\varphi(t_{n,j}) \mid \varphi(n')$ dobijamo da

$$c(j,n) = \pm\frac{\varphi(n)}{\varphi(t_{n,j})} = \pm\frac{\varphi(p_i^{\alpha_i})\varphi(n')}{\varphi(t_{n,j})} = \pm p_i^{\alpha_i - 1}(p_i - 1)\frac{\varphi(n')}{\varphi(t_{n,j})}.$$

Iz poslednje jednakosti sleduje da je $c(j,n)$ paran, jer je i $p_i - 1$ takođe paran. Ovo je kontradikcija i zato zaključujemo da $p_i \mid t_{n,j}$ za svaki $1 \leq i \leq k$.

Sada imamo da je $\varphi(t_{n,j}) = (p_1 - 1)(p_2 - 1)\cdots(p_k - 1)$ i zbog toga

$$c(j,n) = 2^{\alpha_0 - 1} p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}.$$

Pošto je $c(j,n)$ neparan, onda važi $0 \leq \alpha_0 \leq 1$, to jest $4 \nmid n$.

Ako je $n \in 2\mathbb{N}+1$ tada je $t_{n,j} = p_1 \cdots p_k$, jer $t_{n,j}$ nije deljiv kvadratom prostog broja. Ako je $n \in 4\mathbb{N}+2$, imamo dve mogućnosti za $t_{n,j}$, $t_{n,j} = p_1 \cdots p_k$ ili $t_{n,j} = 2p_1 \cdots p_k$ zavisno od parnosti indeksa j.

Štaviše, koristeći $n = \gcd(n,j)t_{n,j}$ dobijamo da je $\gcd(n,j) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}$ ($t_{n,j}$ i n su iste parnosti) ili $\gcd(n,j) = 2p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}$ (u suprotnom). Iz poslednjeg je tvrđenje ovog smera dokaza jasno.

($\Leftarrow$:) Kako je $\gcd(n,j) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1} \gcd(J,n)$ i $\gcd(J,n) = \{1,2\}$, imamo da je $t_{n,j} = p_1 \cdots p_k$ ili $t_{n,j} = 2p_1 \cdots p_k$. U oba slučaja je $\varphi(t_{n,j}) = (p_1 - 1)\cdots(p_k - 1)$. Na osnovu formule

$$c(j,n) = \mu(t_{n,j}) \frac{\varphi(n)}{\varphi(t_{n,j})} = \pm p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1},$$

zaključujemo da $c(j,n) \in 2\mathbb{N}+1$. □

Lema 2.3.2. *Neka je d proizvoljan delilac broja n takav da je $n/d \in 2\mathbb{N}+1$ i $0 \leq j \leq n-1$ proizvoljan prirodan broj. Tada je $c(j,n/d) = -c(j,2n/d)$ za $j \in 2\mathbb{N}+1$ i $c(j,n/d) = c(j,2n/d)$ za $j \in 2\mathbb{N}$.*

Dokaz. Iz $n/d \in 2\mathbb{N}+1$ zaključujemo da je $\varphi(2n/d) = \varphi(n/d)$.

Neka je $j \in 2\mathbb{N}+1$. Tada je $\gcd(2n/d, j) = \gcd(n/d, j)$ i

$$t_{2n/d,j} = \frac{2n}{d\gcd(2n/d,j)} = 2\frac{n}{d\gcd(n/d,j)} = 2t_{n/d,j}.$$

Takođe je $\varphi(t_{2n/d,j}) = \varphi(t_{n/d,j})$ jer je $t_{n/d,j}$ neparan. Dalje iz činjenice da $t_{2n/d,j}$ nije deljiv nekim kvadratom prostog broja ako i samo ako ista činjenica važi za $t_{n/d,j}$, zaključujemo da je $\mu(t_{2n/d,j}) = -\mu(t_{n/d,j})$. Sada odavde direktno sledi da je

$$c(j,2n/d) = \mu(t_{2n/d,j}) \frac{\varphi(2n/d)}{\varphi(t_{2n/d,j})} = -\mu(t_{n/d,j}) \frac{\varphi(n/d)}{\varphi(t_{n/d,j})} = -c(j,n/d).$$

Neka je sada $j \in 2\mathbb{N}$. Sličnim razmatranjem imamo da je $\gcd(2n/d, j) = 2\gcd(n/d, j)$, kao i $t_{2n/d,j} = t_{n/d,j}$. Iz poslednjih činjenica direktno izvodimo da je $c(j,2n/d) = c(j,n/d)$. □

Teorema 2.3.3. *Za proizvoljni integralni cirkularni graf $ICG_n(D)$ postoji neparan broj $0 \leq j \leq n-1$ gde je λ_j takođe neparan ako i samo ako postoji delilac $d \in D$ takav da $d/2 \notin D$ i $2d \notin D$.*

Dokaz.

($\Rightarrow$:) Pretpostavimo da za svaki $d \in D$ važi da je ili $2d \in D$ ili $d/2 \in D$. Odavde sledi $D = D_1 \cup 2D_1$. Neka je $j \in 2\mathbb{N}+1$. Prema Lemi **??** imamo $c(j,n/d) = -c(j,2n/d)$ za proizvoljni $d \in D$ takav da je $n/d \in 2\mathbb{N}+1$ i zato

$$\lambda_j = \sum_{d \in D_1 \cup 2D_1} c(j,n/d) = \sum_{d \in D_1} c(j,n/d) + c(j,2n/d) = 0 \in 2\mathbb{N}.$$

Odavde zaključujemo da su sve sopstvene vrednosti sa neparnim indeksima parne.

($\Leftarrow$:) Neka je $D_1'' = \{d \in D \mid n/d \in 4\mathbb{N}+2 \Rightarrow\ 2d \in D\}$ i $D'' = D_1'' \cup 2D_1''$.

Neka je $D' = D \setminus D''$. Prema pretpostavci, D' je neprazan skup. Na osnovu Leme **??** važi da je $c(j, n/d) + c(j, 2n/d) \in 2\mathbb{N}$ za svaki $d \in D''$ takav da je $n/d \in 2\mathbb{N}+1$. Označimo sa $d'_{max} = \max D'$. Kako je d'_{max} delilac broja n, tada se može zapisati u formi $d'_{max} = 2^{\beta_0} p_1^{\beta_1} \cdots p_k^{\beta_k}$ gde je $0 \leq \beta_i \leq \alpha_i$ za svako $i = 1, \ldots, k$. Bez gubljenja opštosi, pretpostavićemo da postoji $1 \leq s \leq k$ takav da je $\beta_i < \alpha_i$ za svako $i = 1, \ldots, s$ i $\beta_i = \alpha_i$, za $i = s+1, \ldots, k$. Tada možemo pisati $n/d'_{max} = 2^{\alpha_0-\beta_0} p_1^{\alpha_1-\beta_1} \cdots p_s^{\alpha_s-\beta_s}$. Neka je

$$j_0 = p_1^{\alpha_1-\beta_1-1} \cdots p_s^{\alpha_s-\beta_s-1} p_{s+1}^{\alpha_{s+1}} \cdots p_k^{\alpha_k}.$$

Jasno je da važi $0 \leq j_0 \leq n-1$. Iz Leme **??** direktno proizilazi da je $c(j_0, n/d'_{max})$ neparan jer je $n/d'_{max} \geq 2$.

Pretpostavimo da je $D' \setminus \{d'_{max}\} \neq \emptyset$ i neka je $d \in D' \setminus \{d'_{max}\}$ proizvoljan delilac čija je kanonska faktorizacija $d = 2^{\gamma_0} p_1^{\gamma_1} \cdots p_k^{\gamma_k}$.

Pokazaćemo da postoji $1 \leq i \leq k$ takav da je $0 \leq \gamma_i < \beta_i \leq \alpha_i$. Pretpostavimo da ovo nije slučaj, to jest da je $0 \leq \beta_i \leq \gamma_i \leq \alpha_i$ za svaki $1 \leq i \leq k$. Ako je $\beta_0 \leq \gamma_0$ onda $d'_{max} \mid d$, što dovodi do kontradikcije. Slično, ako je $\beta_0 = \gamma_0 + 1$ onda važi da je $d'_{max} \mid 2d$, odakle sledi $d = d'_{max}/2$, što je ponovo kontradikcija sa definicijom skupa D'.

Neka je i proizvoljan indeks takav da je $\gamma_i < \beta_i$. Pretpostavimo da je $\alpha_i - \beta_i \geq 1$. Tada je $i \leq s$ i $S_{p_i}(n/d) = \alpha_i - \gamma_i \geq 2$. Kako je $S_{p_i}(j_0) = \alpha_i - \beta_i - 1 > \alpha_i - \gamma_i - 1 = S_{p_i}(n/d) - 1$, iz Leme **??** zaključujemo da je $c(j_0, n/d)$ paran.

Pretpostavimo da je $\alpha_i = \beta_i$. Tada je $i > s$ i $S_{p_i}(n/d) = \alpha_i - \gamma_i \geq 1$. Ponovo, kako je $S_{p_i}(j_0) = \alpha_i > \alpha_i - \gamma_i - 1 = S_{p_i}(n/d) - 1$, iz Leme **??** proizilazi da je $c(j_0, n/d)$ paran.

Iz celokupnog razmatranja zaključujemo da postoji neparan indeks j_0 takav da je $c(j_0, n/d'_{max})$ neparan i $c(j_0, n/d)$ je paran za svaki $d \in D' \setminus \{d'_{max}\}$. Sada imamo da je

$$\lambda_{j_0} = c(j_0, n/d'_{max}) + \sum_{d \in D' \setminus \{d'_{max}\}} c(j_0, n/d) + \sum_{d \in D''} c(j_0, n/d) \in 2\mathbb{N}+1,$$

pošto su obe sume u poslednjem izrazu parne.

Ako je d_{max} jedini delilac koji je sadržan u D, gornja suma se svodi na

$$\lambda_{j_0} = c(j_0, n/d'_{max}) + \sum_{d \in D''} c(j_0, n/d) \in 2\mathbb{N}+1,$$

i ponovo je neparna. □

Pomenimo i dve direktne posledice prethodne teoreme. Prva zapravo predstavlja kontrapoziciju tvrđenja prethodne teoreme.

Lema 2.3.4. *Sve sopstvene vrednosti grafa* $\mathrm{ICG}_n(D)$ *na neparnim pozicijama su parne ako i samo ako je* $D = D_1 \cup 2D_1$.

Lema 2.3.5. *Neka je* $n/2 \in D$. *Sve sopstvene vrednosti grafa* $\mathrm{ICG}_n(D)$ *na neparnim pozicijama su neparne ako i samo ako* $D = D_1^* \cup 2D_1^* \cup \{n/2\}$ *gde je* $D_1^* = D_1 \setminus \{n/2\}$.

Dokaz. Pretpostavimo da su sve sopstvene vrednosti grafa $\mathrm{ICG}_n(D)$ na neparnim pozicijama neparne. Označimo sa λ_j sopstvene vrednosti grafa. Posmatrajmo integralni cirkularni graf

$\mathrm{ICG}_n(D')$ gde je $D' = D \setminus \{n/2\}$. Označimo sa λ'_j sopstvene vrednosti integralnog cirkularnog grafa $\mathrm{ICG}_n(D')$. Kako je

$$t_{2,j} = \frac{2}{\gcd(2,j)} = \begin{cases} 2, & 2 \nmid j \\ 1, & 2 \mid j \end{cases}, \quad c(j,2) = \begin{cases} -1, & 2 \nmid j \\ 1, & 2 \mid j \end{cases}. \tag{2.39}$$

važi

$$\lambda_j = \begin{cases} \lambda'_j + 1, & 2 \mid j \\ \lambda'_j - 1, & 2 \nmid j \end{cases}. \tag{2.40}$$

Odavde dobijamo da su sve sopstvene vrednosti grafa $\mathrm{ICG}(D')$ na neparnin pozicijama parne. Prema Lemi **??** imamo da je $D' = D_1^* \cup 2D_1^*$ gde $D_1^* = D_1 \setminus \{n/2\}$, čime kompletiramo prvi deo dokaza.

Suprotan smer tvrđenja se može dokazati analogno. Neka je $D = D_1^* \cup 2D_1^* \cup \{n/2\}$ i $D' = D \setminus \{n/2\}$. Prema Lemi **??** sve sopstvene vrednosti grafa $\mathrm{ICG}_n(D')$ na neparnim pozicijama su parne. Takođe, korišćenjem relacije (**??**) imamo da su sopstvene vrednosti $\mathrm{ICG}_n(D)$ na neparnim pozicijama neparne. □

Sada možemo dokazati glavni rezultat ovog dela.

Teorema 2.3.6. *U* $\mathrm{ICG}_n(D)$ *ne postoji PST za* $n \in 4\mathbb{N}+2$ *i proizvoljan skup delilaca* D.

Dokaz.

Korišćenjem **??** imamo da je $\lambda_1 = \sum_{d\in D_0\cup D_1} \mu(n/d)$ i $\lambda_2 = \sum_{d\in D_0} \mu(n/d) + \sum_{d\in D_1} \mu(n/(2d))$. Odavde dobijamo da je $\lambda_2 - \lambda_1 = \sum_{d\in D_1}(\mu(n/(2d)) - \mu(n/d))$. Kako n/d nije deljiv kvadratom prostog broja ako i samo ako $n/(2d)$ nije deljiv kvadratom prostog broja, imamo da $2 \mid \lambda_2 - \lambda_1$ ili, ekvivalentno, $S_2(\lambda_2 - \lambda_1) \geq 1$. Sada razlikujemo sledeća dva slučaja.

Slučaj 1. $n/2 \notin D$. Tada je po Propoziciji **??** $\lambda_0 \in 2\mathbb{N}$. Pretpostavimo takođe da $\mathrm{ICG}_n(D)$ ima PST. Prema Posledici **??**, sve sopstvene vrednosti λ_j su parne, gde je $0 \leq j \leq n-1$. Ali iz Leme **??** sledi da je $D = D_1 \cup 2D_1$. Posmatrajmo sada graf $\mathrm{ICG}_{n_1}(D')$ gde $n_1 = n/2$. Označimo sopstvene vrednosti ovog grafa sa λ'_j za $j = 0, \ldots, n_1 - 1$. Kako je n_1/d neparan za svaki $d \in D_1$, zaključujemo $c(2j, n_1/d) = c(j, n_1/d)$ za svaki $0 \leq j \leq n_1 - 1$. Takođe, iz Leme **??** imamo da je $c(2j, n/d) = c(2j, n/(2d))$ za svako $d \in D_1$. Iz poslednjih razmatranja proizilazi

$$\begin{aligned} \lambda_{2j} &= \sum_{d\in D} c(2j, n/d) = 2\sum_{d\in D'} c(2j, n/(2d)) \\ &= 2\sum_{d\in D'} c(2j, n_1/d) = 2\sum_{d\in D'} c(j, n_1/d) = 2\lambda'_j. \end{aligned}$$

Kako je $n_1/2 \notin D_1$ važi da je $\lambda'_0 \in 2\mathbb{N}$ odakle sledi da je $S_2(\lambda_0) \geq 2$. Sa druge strane, prema Teoremi **??** postoji j_0 takav da je λ'_{j_0} neparan, pa je i $S_2(\lambda_{2j_0}) = 1$.

Ako je $0 \leq j \leq n-1$ neparan, prema Lemi **??** imamo da je $c(j, n/(2d)) = -c(j, n/d)$ za bilo koji $d \in D$, odakle sledi da je $\lambda_j = 0$. Odavde zaključujemo da je $S_2(\lambda_1 - \lambda_0) \geq 2$ i $S_2(\lambda_{2j_0} - \lambda_{2j_0-1}) = 1$, što je u kontradikciji sa Teoremom **??**.

Slučaj 2. $n/2 \in D$. Sada je $\lambda_0 \in 2\mathbb{N}+1$. Pretpostavimo da PST postoji u $\mathrm{ICG}_n(D)$. Kako je $\lambda_2 - \lambda_1 \in 2\mathbb{N}$ prema Posledici **??**, sve sopstvene vrednosti λ_j, za $0 \leq j \leq n-1$ su neparne. Iz Leme **??** proizilazi da $D' = D_1^* \cap 2D_1^* \cap \{n/2\}$ gde je $D_1^* = D_1 \setminus \{n/2\}$. Analogno prethodnom **Slučaju 1**, dokazujemo da je $S_2(\lambda_1 - \lambda_0) = S_2(\lambda'_1 - \lambda'_0 + 2) = 1$ i $S_2(\lambda_{2j_0} - \lambda_{2j_0-1}) = S_2(\lambda'_{2j_0} - \lambda'_{2j_0-1} + 2) \geq 2$, što je kontradikcija sa Teoremom **??**. □

2.3.2 Spektar i karakterizacija $\mathrm{ICG}_n(D)$ sa PST svojstvom

Glavni rezultat ovog odeljka je karakterizacija netežinskih integralnih cirkularnih grafova $\mathrm{ICG}_n(D)$ sa PST. Takođe ćemo na ovim grafovima izračunati savršeno kvantno rastojanje. Na osnovu ovih rezultat može se izračunati i broj grafova reda n, sa PST svojstvom, u funkciji od n. Prema Teoremi **??** pretpostavljamo da za graf $\mathrm{ICG}_n(D)$ važi da je n deljivo sa 4.

Teorema 2.3.7. *Neka* $\mathrm{ICG}_n(D)$ *ima PST. Ako je* $n/2 \in D$ *onda su sve sopstvene vrednosti neparne, u suprotnom su sve parne. Štaviše, u prvom slučaju su sopstvene na neparnim pozicijama jednake* -1*, a u drugom slučaju su sopstvene vrednosti na neparnim pozicijam jednake* 0*.*

Dokaz. Prema Propoziciji **??** imamo da je $\lambda_1 = \sum_{d\in D}\mu(n/d)$. Kako $4 \mid n/d$ za $d \in D_2 \cup \widetilde{D_3}$ zaključujemo da je $\mu(n/d) = 0$ i zbog toga $\lambda_1 = \sum_{d\in \widetilde{D_1}}\mu(n/d)$. Koristeći Propoziciju **??** jos jednom, vidimo da je $\lambda_2 = \sum_{d\in D_0}\mu(n/d) + \sum_{d\in D_1}\mu(n/2d) + \sum_{d\in D_2\cup\widetilde{D_3}} 2\mu(n/2d)$. Za $d \in \widetilde{D_3}$ važi $4 \mid n/2d$, odakle proizilazi da je

$$\lambda_2 - \lambda_1 = \sum_{d\in D_1}(\mu(n/2d) - \mu(n/d)) + 2\sum_{d\in D_2}\mu(n/2d) \in 2\mathbb{N}.$$

Po Teoremi **??** sve razlike oblika $\lambda_{i+1} - \lambda_i \in 2\mathbb{N}$ za $0 \le i \le n-2$, posšto $\mathrm{ICG}_n(D)$ ima PST. Ako $n/2 \notin D$ onda je $\lambda_0 \in 2N$ pa su sve sopstvene vrednosti takođe parne. U suprotnom je $\lambda_0 \in 2N+1$ pa su zato i sve ostale sopstvene vrednosti neparne.

Neka je $j \in 2\mathbb{N}+1$. Za $d \in D_2 \cup \widetilde{D_3}$ imamo da $4 \mid t_{n/d,j}$ i zato je $c(j, n/d) = 0$. Poslednjim zaključkom formulu za j-tu sopstvenu vrednost svodimo na

$$\lambda_j = \sum_{d\in\widetilde{D_1}} c(j, n/d).$$

Iz uslova $n/2 \notin D$ proizilazi da je $\lambda_0 \in 2\mathbb{N}$ i prema prvom delu dokaza sve sopstvene vrednosti su parne.

Neka su μ_j, $0 \le j \le n-1$, sopstvene vrednosti grafa $\mathrm{ICG}_n(\widetilde{D_1})$. Tada je $\lambda_j = \mu_j$ za svaki neparan $0 \le j \le n-1$, pa je $\mu_j \in 2\mathbb{N}$ za $j \in 2\mathbb{N}+1$. Iz Leme **??** zaključujemo da su sve sopstvene vrednosti μ_j na neparnim pozicijama parne ako i samo ako je $D_0 = 2D_1$ i $\widetilde{D_1} = D_1 \cup 2D_1$. Na osnovu prvog dela dokaza Teoreme **??** izvodimo zaključak da je $\mu_j = 0$ za $j \in 2\mathbb{N}+1$ i stoga $\lambda_j = 0$ za $j \in 2\mathbb{N}+1$.

Analogno, ako je $n/2 \in D$ dobijamo da je $\lambda_j \in 2\mathbb{N}+1$ za $0 \le j \le n-1$ pa je i $\mu_j \in 2\mathbb{N}+1$ za neparne $0 \le j \le n-1$. Sada, prema Lemi **??** imamo da je $D = D_1^* \cup 2D_1^* \cup \{n/2\}$ gde je $D_1^* = D_1 \setminus \{n/2\}$.

Posmatrajmo dalje graf $\mathrm{ICG}_n(D')$ gde je $D' = D \setminus \{n/2\} = D_1^* \cup 2D_1^*$. Označimo sa λ'_j sopstvene vrednosti grafa $\mathrm{ICG}_n(D')$. Iz (**??**) dobijamo da je $\lambda_j = \lambda'_j - 1$ za $j \in 2\mathbb{N}+1$. Međutim, na osnovu prvog dela dokaza imamo da je $\lambda'_j = 0$ za $j \in 2\mathbb{N}+1$ i zato je $\lambda_j = -1$ za $j \in 2\mathbb{N}+1$.
□

Iz dokaza poslednje teoreme možemo izvesti sledeću značajnu posledicu

Posledica 2.3.8. *Ako* $\mathrm{ICG}_n(D)$ *ima PST onda je* $D_0 = 2(D_1 \setminus \{n/2\})$.

Koristeći Teoremu **??** možemo ustanoviti precizniji kriterijum za karakterizaciju integralnih cirkularnih grafova koji imaju PST, od kriterijuma datog u Posledici **??**.

Lema 2.3.9. $\mathrm{ICG}_n(D)$ *ima PST ako i samo ako postoji prirodan broj* $k \geq 1$ *takav da je jedan od sledeća dva uslova zadovoljen*

i) $S_2(\lambda_{2j}) = k \ i \ \lambda_{2j+1} = 0$, *if* $n/2 \notin D$

ii) $S_2(\lambda_{2j}+1) = k \ i \ \lambda_{2j+1} = -1$, *if* $n/2 \in D$

za $0 \leq j \leq n/2$.

Lema 2.3.10. *Neka je* n *paran,* d *delilac od* n *i* $n_1 = n/2$. *Za paran broj* $0 \leq j \leq n-1$, *sledeće jednakosti su zadovoljene*

1. $c(j, n/d) = c(j/2, \frac{n_1}{d/2})$, *ako* $d \in D_0$

2. $c(j, n/d) = c(j/2, n_1/d)$, *ako* $d \in D_1$

3. $c(j, n/d) = 2c(j/2, n_1/d)$, *ako* $d \in D_2 \cup \widetilde{D_3}$.

Dokaz.

1. Pretpostavimo da je $d \in D_0$. Tada je $\gcd(n/d, j) = \gcd(\frac{n_1}{d/2}, j/2)$ i

$$t_{n/d,j} = \frac{n}{d\gcd(n/d,j)} = \frac{2n_1}{2\frac{d}{2}\gcd(\frac{n_1}{d/2}, j/2)} = t_{\frac{n_1}{d/2}, j/2}.$$

Osim toga, važi da je $\varphi(n/d) = \varphi(\frac{n_1}{d/2})$ pa je i $c(j, n/d) = c(j/2, \frac{n_1}{d/2})$.

2. Pretpostavimo sada da je $d \in D_1$. Tada je $\gcd(n/d, j) = 2\gcd(n_1/d, j/2)$ i

$$t_{n/d,j} = \frac{n}{d\gcd(n/d,j)} = \frac{2n_1}{d\ 2\gcd(n_1/d, j/2)} = t_{n_1/d, j/2}.$$

Takođe zaključujemo da je $\varphi(n/d) = \varphi(2\frac{n_1}{d}) = \varphi(n_1/d)$ odakle je $c(n/d, j) = c(n_1/d, j/2)$.

3. Pretpostavimo da je $d \in D_2 \cup \widetilde{D_3}$. Kao i u prethodnom slučaju dobijamo $\gcd(n/d, j) = 2\gcd(n_1/d, j/2)$ i $t_{n/d,j} = t_{n_1/d,j/2}$. Neka je $k = S_2(n/d)$ i n' ceo broj takav da je $n/d = 2^k\ n'/d$. Primetimo da je $k \geq 2$, pošto je $d \in D_2 \cup \widetilde{D_3}$. Takođe je n'/d neparan pa je zato i $\gcd(2^k, n'/d) = 1$, odakle sledi da je $\varphi(n/d) = \varphi(2^k\frac{n'}{d}) = 2^{k-1}\varphi(\frac{n'}{d})$.

Osim toga, imamo da je

$$\varphi(n/d) = 2^{k-1}\varphi(\frac{n'}{d}) = 2\varphi(2^{k-1})\varphi(\frac{n'}{d}) = 2\varphi(2^{k-1}\frac{n'}{d}) = 2\varphi(n_1/d)$$

odakle je konačno $c(j, n/d) = 2c(j/2, n_1/d)$, ako je $d \in D_2 \cup \widetilde{D_3}$.

□

Lema 2.3.11. *Ako* $\mathrm{ICG}_n(D)$ *ima PST tada je* $D_1 = 2(D_2 \setminus \{n/4\})$.

Dokaz.

Neka su λ_j sopstvene vrednosti grafa $\mathrm{ICG}_n(D)$ za $0 \leq j \leq n-1$.

Prema Posledici **??** važi da je $D_0 = 2(D_1 \setminus \{n/2\})$, pa je zato

$$\lambda_j = \sum_{d \in 2(D_1 \setminus \{n/2\})} c(j, n/d) + \sum_{d \in D_1} c(j, n/d) + \sum_{d \in D_2 \cup \widetilde{D_3}} c(j, n/d).$$

Primetimo da iz relacije (**??**) imamo da je $c(j, 2) = 1$ for $j \in 2\mathbb{N}$.

Za $d \in 2(D_1 \setminus \{n/2\})$, neka je $d = 2d'$ gde je $d' \in D_1 \setminus \{n/2\}$. Tada je $c(j, n/d) = c(j, n_1/d')$, pa na osnovu Leme **??** (deo 1.), dobijamo da je $c(j, n_1/d') = c(j/2, \frac{n_1/2}{d'/2}) = c(j/2, n1/d')$.

Ako je $d \in D_1$, korišćenjem Leme **??** (deo 2.) važi da je $c(j, n/d) = c(j/2, n1/d)$.

Konačno ako je $d \in D_2 \cup \widetilde{D_3}$, prema Lemi **??** (deo 3.) važi da je $c(j, n/d) = 2c(j/2, n1/d)$.

Uzimajući prethodnu diskusiju u obzir dobijamo

$$\lambda_j = \begin{cases} c(j,2) + 2\sum_{d \in D_1 \setminus \{n/2\} \cup D_2 \cup \widetilde{D_3}} c(j/2, n_1/d) = 2\lambda'_{j/2} + 1, & n/2 \in D \\ 2\sum_{d \in D_1 \setminus \{n/2\} \cup D_2 \cup \widetilde{D_3}} c(j/2, n_1/d) = 2\lambda'_{j/2}, & n/2 \notin D \end{cases} \tag{2.41}$$

gde je $n_1 = n/2$ i λ'_i sopstvene vrednosti grafa $\mathrm{ICG}_{n_1}(D')$ gde je $D' = (D_1 \setminus \{n/2\}) \cup D_2 \cup \widetilde{D_3}$.

Zaključujemo da je $\gcd(n/d, j) = 2$ za $j \in 4\mathbb{N}+2$ i $d \in \widetilde{D_3}$, te je stoga $4 \mid t_{n/d,j}$, što konačno dovodi do $c(j, n/d) = 0$. Odavde dobijamo da je

$$\lambda_j = \sum_{d \in \widetilde{D_1}} c(j, n/d) + \sum_{d \in D_2} c(j, n/d) = \begin{cases} 2\lambda'_{j/2} + 1, & n/2 \in D \\ 2\lambda'_{j/2}, & n/2 \notin D \end{cases} \tag{2.42}$$

gde je $\lambda'_j = \sum_{d \in D_1 \setminus \{n/2\}} c(j, n_1/d) + \sum_{d \in D_2} c(j, n_1/d)$. Ovo znači da su sopstvene vrednosti λ'_j, za neparno $0 \leq j \leq n_1 - 1$, jednake sopstvenim vrednostima na neparnim pozicijama grafa $\mathrm{ICG}_{n_1}(D_1 \cup D_2 \setminus \{n/2\})$. Označimao sa μ_j sopstvene vrednosti grafa $\mathrm{ICG}_{n_1}(D_1 \cup D_2 \setminus \{n/2\})$, za $0 \leq j \leq n_1 - 1$.

Iz Leme **??** sledi da je $S_2(\lambda_j) = k$ ili $S_2(\lambda_j + 1) = k$, za $j \in 4\mathbb{N} + 2$ i neki prirodan broj $k \geq 1$, u zavisnosti od toga da li je $n/2 \notin D$ ili $n/2 \in D$. Takođe imamo da je $S_2(\lambda'_{j/2}) = k - 1$ ili $S_2(\lambda'_{j/2} + 1) = k - 1$ za neparne $0 \leq j/2 \leq n_1 - 1$. Kako je $\mu_j = \lambda'_j$ za neparne $0 \leq j \leq n_1 - 1$ (sopstvene vrednosti μ_j na neparnim pozicijama imaju istu parnost), to Leme **??** i **??** pokazuju da je $D_1 = 2(D_2 \setminus \{n_1/2\})$, čime je dokaz kompletiran.

□

Teorema 2.3.12. *Ako* $\mathrm{ICG}_n(D)$ *ima PST onda je ili* $n/2 \in D$ *ili* $n/4 \in D$.

Dokaz.

Slučaj 1. $n/2 \notin D$. Pretpostavimo takođe da $n/4 \notin D$. Kako $n/2 \notin D$, prema Posledici **??** važi da je $D_0 = 2D_1$. Koristeći Propoziciju **??** imamo da je $\lambda_2 = \sum_{d \in 2D_1} \mu(n/d) + \sum_{d \in D_1} \mu(n/2d) + 2\sum_{d \in D_2 \cup \widetilde{D_3}} \mu(n/2d)$. Za $d \in \widetilde{D_3}$ zaključujemo da je $4 \mid n/2d$, te je zato $\sum_{d \in \widetilde{D_3}} \mu(n/2d) = 0$. Sada formula za sopstvenu vrednost λ_2 postaje $\lambda_2 = \sum_{d \in D_1} \mu(n/2d) + \sum_{d \in D_1} \mu(n/2d) + 2\sum_{d \in D_2} \mu(n/2d)$. Kako $n/4 \notin D$, Lema **??** nas dovodi do zaključka

$$\lambda_2 = 2\Big(\sum_{d \in 2D_2} \mu(n/2d) + \sum_{d \in D_2} \mu(n/2d)\Big) = 2\Big(\sum_{d \in D_2} \mu(n/4d) + \sum_{d \in D_2} \mu(n/2d)\Big) = 0.$$

Slučaj 2. $n/2 \in D$. Pretpostavimo takođe da je $n/4 \in D$. Iz poslednje pretpostavke, kao i Posledice **??** i Leme **??**, dobijamo da je $D_0 = 2(D_1 \setminus \{n/2\})$ i $D_1 = 2(D_2 \setminus \{n/4\})$. U ovom slučaju λ_2 može biti zapisana na sledeći način

$$\lambda_2 = \sum_{d \in D_1'} \mu(n/d) + \sum_{d \in D_1 \setminus \{n/2\}} \mu(n/2d) + 2 \sum_{d \in D_2 \setminus \{n/4\}} \mu(n/2d) + \mu(1) + 2\mu(2) = 0 + 1 - 2 = -1.$$

Primetimo da je $\sum_{d \in D_0} \mu(n/d) + \sum_{d \in D_1 \setminus \{n/2\}} \mu(n/2d) + 2 \sum_{d \in D_2 \setminus \{n/4\}} = 0$ prema Slučaju 1 dokaza. U oba slučaja zaključujemo da je $\lambda_1 = \lambda_2$ (prema Lemi **??**), a poslednje je kontradikcija prema Posledici **??**. □

Savršeno kvantno komunikaciono rastojanje (PQCD) za proizvoljan par čvorova a i b predstavlja rastojanje $d(a, b)$ u grafu, ako PST postoji između njih. Ukoliko uzmemo u razmatranje cirkularnu mrežu sa identičnim načinom sparivanja kubitova, PST se pojavljuje samo između čvorova b i $b + n/2$ za svako $0 \leq b \leq n/2 - 1$ (Teorema **??**). Za integralni cirkularni graf $\mathrm{ICG}_n(D)$, PQCD čvorova b i $b + n/2$ je jednak jedan, ako $n/2 \in D$. U suprotnom, imamo da je $n/4 \in D$ (Teorema **??**) pa put $b, b + n/4, b + n/2$ pokazuje da je PQCD jednak dva. U oba slučaja je PQCD nezavisno od reda grafa.

Sledećim tvrđenjem opisujemo spektar integralnih cirkularnih grafova. Kriterijum za egzistenciju PST u integralnim cirkularnim grafovima dat sledećom lemom, biće korišćen i u narednim teoremama.

Lema 2.3.13. $\mathrm{ICG}_n(D)$ *ima PST ako i samo ako važi jedan od sledećih uslova*

i) $\lambda_{2j} \in 4\mathbb{N} + 2$ *i* $\lambda_{2j+1} = 0$, *ako* $n/2 \notin D$

ii) $\lambda_{2j} \in 4\mathbb{N} + 1$ *i* $\lambda_{2j+1} = -1$, *ako* $n/2 \in D$

za svako $0 \leq j \leq n/2$.

Dokaz. U dokazu ćemo koristiti istu notaciju kao u dokazu Leme **??**. Pretpostavimo da je $\mathrm{ICG}_n(D)$ ima PST.

Iz Leme **??** sledi da je $\lambda_j = 0$ ili $\lambda_j = -1$ u zavisnosti od toga da li $n/2 \notin D$ ili $n/2 \in D$, za svaki neparan $0 \leq j \leq n - 1$.

Sada pretpostavimo da je $n/4 \in D$. Prema Teoremi **??** imamo da $n/2 \notin D$. Odavde sledi da je $\lambda_0 \in 2\mathbb{N}$, te su sopstvene vrednosti grafa $\mathrm{ICG}_n(D)$ parne za $j \in 2\mathbb{N}$, što sledi iz Leme **??**. Sada ćemo nastaviti razmatrnje prema dokazu Leme **??**, to jest

$$\lambda_j = 2\lambda'_{j/2}$$

gde su λ'_i sopstvene vrednosti grafa $\mathrm{ICG}_{n_1}(D')$, pri čemu je $D' = D_1 \cup D_2 \cup \widetilde{D_3} \setminus \{n/2\}$ i $n_1 = n/2$.

Kako je $n/4 = n_1/2 \in D$, sledi da je $\lambda'_0 \in 2\mathbb{N} + 1$, odakle dalje imamo da je $\lambda_0 \in 4\mathbb{N} + 2$. Konačno, iz Leme **??** zaključujemo da je $\lambda_j \in 4\mathbb{N} + 2$ za $j \in 2\mathbb{N}$.

Ako je $n/2 \in D$ onda je $\lambda_0 \in 2\mathbb{N} + 1$, pa otuda važi da je $\lambda_j \in 2\mathbb{N} + 1$ za $j \in 2\mathbb{N}$. Odavde dalje sledi da je $\lambda_j = 2\lambda'_{j/2} + 1$. Prema Teoremi **??** je $n/4 = n_1/2 \notin D$, pa je zato i $\lambda'_0 \in 2\mathbb{N}$.

Odavde sledi da je $\lambda_0 \in 4\mathbb{N}+1$. Konačno, korišćenjem Leme **??** zaključujemo da je $\lambda_j \in 4\mathbb{N}+1$ za $j \in 2\mathbb{N}$.

Ako bilo koji od uslova **i)** ili **ii)** važi, može se lako videti da je $\lambda_{j+1} - \lambda_j \in 4\mathbb{N}+2$ iz čega dalje proizilazi da $\mathrm{ICG}_n(D)$ ima PST, prema Teoremi **??**.

□

Teorema 2.3.14. *Neka je D skup delilaca broja n takvih da $n/2, n/4 \notin D$. Tada* $\mathrm{ICG}_n(D \cup \{n/4\})$ *ima PST ako i samo ako* $\mathrm{ICG}_n(D \cup \{n/2\})$ *ima PST.*

Dokaz.

Neka su λ_j, μ_j i ν_j sopstvene vrednosti grafova $\mathrm{ICG}_n(D \cup \{n/4\})$, $\mathrm{ICG}_n(D \cup \{n/2\})$ i $\mathrm{ICG}_n(D)$, redom. Sada imamo sledeće relacije između pomenutih sopstvenih vrednosti: $\lambda_j = \nu_j + c(j,4)$ i $\mu_j = \nu_j + c(j,2)$. Odavde sledi da je $\mu_j = \lambda_j - c(j,4) + c(j,2)$ za svako $0 \le j \le n-1$.

Direktnim izračunavanjem pokazuju se sledeće relacije

$$t_{4,j} = \frac{4}{\gcd(4,j)} = \begin{cases} 4, & 2 \nmid j \\ 2, & S_2(j) = 1 \\ 1, & 4 \mid j \end{cases}, \quad c(j,4) = \begin{cases} 0, & j \in 2\mathbb{N}+1 \\ -2, & j \in 4\mathbb{N}+2 \\ 2, & j \in 4\mathbb{N} \end{cases}. \tag{2.43}$$

Odavde sledi da je

$$\mu_j = \begin{cases} \lambda_j - 1, & j \in 2\mathbb{N}+1 \\ \lambda_j + 3, & j \in 4\mathbb{N}+2 \\ \lambda_j - 1, & j \in 4\mathbb{N} \end{cases}, \tag{2.44}$$

Sledeće dve činjenice se sada lako izvode: za $j \in 2\mathbb{N}+1$, $\lambda_j = 0$ ako i samo ako je $\mu_j = -1$ i za $j \in 2\mathbb{N}$, $\lambda_j \in 4\mathbb{N}+2$ ako i samo ako je $\mu_j \in 4\mathbb{N}+1$. Konačno, primenom Leme **??** kompletiramo dokaz.

□

Sada možemo iskazati jedan od glavnih rezultata poglavlja.

Teorema 2.3.15. $\mathrm{ICG}_n(D)$ *ima PST ako i samo ako je $n \in 4\mathbb{N}$, $D_1^* = 2D_2^*$, $D_0 = 4D_2^*$ i važi jedan od uslova $n/4 \in D$ ili $n/2 \in D$, pri čemu je $D_2^* = D_2 \setminus \{n/4\}$ i $D_1^* = D_1 \setminus \{n/2\}$.*

Dokaz.

($\Rightarrow$:) Tvrđenje ovog smera teoreme predstavlja posledicu Teoreme **??**, Leme **??**, Posledice **??** i Teoreme **??**.

($\Leftarrow$:) Prema Teoremi **??**, ovaj smer je dovoljno dokazati za $n/4 \in D$. Takođe, iz Teoreme **??** imamo da $n/2 \notin D$.

Neka je $0 \le j \le n-1$ neparan. Za $d \in D_2 \cup \widetilde{D_3}$, zaključujemo da je $c(j, n/d) = 0$, jer važi da $4 \mid t_{n/d,j}$. Odavde sledi da je

$$\lambda_j = \sum_{d \in 2D_1} c(j, n/d) + \sum_{d \in D_1} c(j, n/d) = \sum_{d \in D_1} c(j, n/2d) + c(j, n/d) = 0.$$

Poslednja jednakost važi iz Leme **??**.

Neka je $0 \le j \le n-1$ paran. Tada je

$$\lambda_j = \sum_{d\in 2D_1} c(j,n/d) + \sum_{d\in D_1} c(j,n/d) + \sum_{d\in D_2\setminus\{n/4\}} c(j,n/d) + c(j,4) + \sum_{d\in \widetilde{D_3}} c(j,n/d).$$

Iz Leme **??** i relacije (**??**) dobijamo

$$\lambda_j = 2\sum_{d\in D_1} c(j,n/d) + \sum_{d\in D_2\setminus\{n/4\}} c(j,n/d) + \sum_{d\in \widetilde{D_3}} c(j,n/d) \pm 2.$$

Sada primenom Leme **??** dalje izvodimo

$$\begin{aligned}\lambda_j &= 2\sum_{d\in D_1=2(D_2\setminus\{n/4\})} c(j/2,n_1/d) + 2\sum_{d\in D_2\setminus\{n/4\}} c(j/2,n_1/d) + 2\sum_{d\in \widetilde{D_3}} c(j/2,n_1/d) \pm 2\\ &= 2\sum_{d\in D_2\setminus\{n/4\}} (c(j/2,n_1/d) + c(j/2,n_1/2d)) + 2\sum_{d\in \widetilde{D_3}} c(j/2,n_1/d) \pm 2,\end{aligned}$$

gde je $n1 = n/2$.

Neka je $j \in 4\mathbb{N}+2$. Iz Leme **??** sledi da je $c(j/2,n_1/d) + c(j/2,n_1/2d) = 0$, pošto važi $j/2 \in 2\mathbb{N}+1$. Za $d \in \widetilde{D_3}$ imamo da $4 \mid t_{n_1/d,j/2}$, pa je zato $c(j/2,n_1/d) = 0$. Konačno izvodimo zaključak da je $\lambda_j = c(j,4) = -2$.

Ako je $j \in 4\mathbb{N}$, prema Lemi **??** pokazujemo da je

$$\lambda_j = 4\sum_{d\in D_2\setminus\{n/4\}} c(j/2,n_1/d) + 2\sum_{d\in \widetilde{D_3}} c(j/2,n_1/d) + 2.$$

Takođe, na osnovu Leme **??** imamo da je $c(j/2,n_1/d) = 2c(j/4,n_1/2d)$. U oba slučaja je $\lambda_j \in 4\mathbb{N}+2$ za $j \in 2\mathbb{N}$. Sada, direktnom primenom Leme **??** dokazujemo tvrđenje.

□

Poslednjom teoremom smo odgovorili na pitanje kada cirkularne mreže imaju PST, karakterišući sve integralne cirkularne grafove sa tom osobinom. Iz ove karakterizacije možemo izračunati broj integralnih cirkularnih grafova koji imaju PST, datog reda n. Ako je $n \in 8\mathbb{N}$, korišćenjem pravila proizvoda, ovaj broj je jednak dvostrukom proizvodu kardinalnosti partetivnih skupova $\{d : d \mid n,\ n/d \in 8\mathbb{N}\}$ i $\{d : d \mid n,\ n/d \in 8\mathbb{N}+4\}\setminus\{n/4\}$. Ako je $n \in 8\mathbb{N}+4$ onda je jednak samo dvostrukoj kardinalnosti partetivnog skupa $\{d : d \mid n,\ n/d \in 8\mathbb{N}+4\}\setminus\{n/4\}$. U oba slučaja smo imali dve mogućnosti jer ili $n/2 \in D$ ili $n/4 \in D$. Prema tome, za dati prirodan broj n, broj integralnih cirkularnih grafova $\mathrm{ICG}_n(D)$ koji imaju PST dat je sledećom formulom

$$|\mathrm{ICG}_n(D)| = \begin{cases} 2^{\tau(\frac{n}{4})}, & n \in 8\mathbb{N}+4 \\ 2^{\tau(\frac{n}{8})\tau(\frac{n}{2^{S_2(n)}})}, & n \in 8\mathbb{N} \end{cases}, \tag{2.45}$$

gde $\tau(n)$ označava ukupan broj delioca broja n. Rezultati prethodne formule su prikazani u tabeli ispod.

n	4	8	12	16	20	24	28	32	36	40	44	48	52
# ICG sa PST	1	2	2	4	2	10	2	8	4	10	2	44	2

n	56	60	64	68	72	76	80	84	88	92	96	100
# ICG sa PST	10	10	16	2	44	2	44	10	10	2	184	4

n	104	108	112	116	120	124	128	132	136	140
# ICG sa PST	10	8	44	2	218	2	32	10	10	10

n	144	148	152	156	160	164	168	172	176	180	184
# ICG sa PST	400	2	10	10	184	2	218	2	44	44	10

n	188	192	196	200
# ICG sa PST	2	752	4	44

Napomenimo da je stastički prikaz podataka u ovoj tabeli proveren u programskom paketu MATHEMATICA (videti kod u prilogu). Iz tabele vidimo da za pojedine vrednosti $n \in 8\mathbb{N}$ (na primer $n = 96, 120, 144, 160, 168, 192, \ldots$) imamo veliki broj grafova koji imaju PST, dok za neke vrednosti $n \in 8\mathbb{N}+4$, postoje samo 2 takva grafa. Ipak, broj grafova $\mathrm{ICG}_n(D)$ koji imaju PST je asimptotski jednak broju $\mathrm{ICG}_n(D)$ datog reda n. Poslednji zaključak se može izvesti iz Posledice 7.2 date u [**?**], gde je pokazano da postoji najviše $2^{\tau(n)-1}$ integralnih cirkularnih grafova sa n čvorova.

Takođe, vredi pomenuti da je maksimalna vrednost PQCD jednaka 2 na cirkularnim mrežama reda $n \in 4\mathbb{N}$. To znači da još uvek ostaje kao otvoreno pitanje o mogućnosti konstrukcije mreža sa identičnim načinom sparivanja, gde se svako kvantno stanje može savršeno preneti na rastojanju većem od $2\log_3 n$, dobijenom u [**?**, **?**] za kocke sa dvostrukim linkovima reda n.

Takođe se povećanje PQCD može postići uzimajući u razmatranje mreže sa fiksnim ali različitim načinom sparivanja [**?**]. Sličan prilaz može biti korišćen na circularnim grafovima sa težinskom matricom susedstva sa ciljem da se uveća PQCD. Štaviše, mnogi nedavno objavljeni radovi na ovu temu predlažu ovakav pristup [**?**, **?**, **?**, **?**]. Neki rezultati vezani za karakterizaciju i pronalaženje novih klasa težinskih cirkularnih grafova biće tema sledećeg poglavlja (videti [**?**]). Karakterizacija cirkularnih grafova koji imaju PST je prvi korak u opisivanju opštije klase težinskih cirkularnih grafova koji imaju PST.

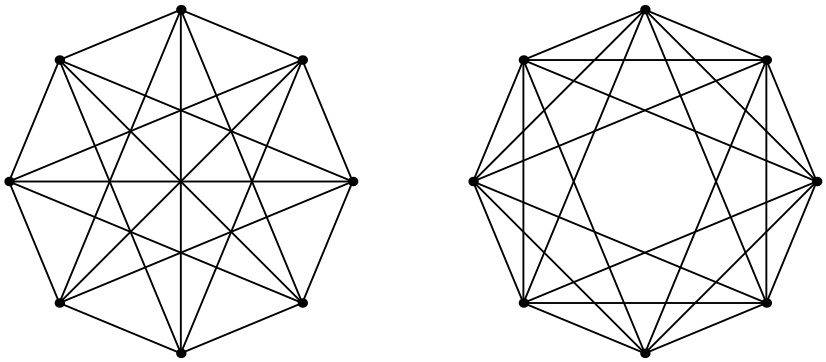
U nastavku ćemo navesti nekoliko karakterističnih klasa grafova $\mathrm{ICG}_n(D)$ sa PST (D je dvoelementni skup, $n \in 8\mathbb{N}+4$, $n \in 8\mathbb{N}$,...), kao i onih koje to svojstvo poseduju. Navedene klase PST grafova će biti korišćene i u narednoj sekciji. Sve ove klase biće izvedene iz Teoreme (**??**). Naime, za $\widetilde{D_3} = \{1\}$ i $D_2 = \emptyset$ dobijamo sledeće dve posledice pomenute teoreme.

Posledica 2.3.16. *Integralni cirkularni grafovi* $\mathrm{ICG}_n(\{1, n/4\})$ *i* $\mathrm{ICG}_n(\{1, n/2\})$ *imaju PST ako i samo ako je* $S_2(n) \geq 3$.

Posledica 2.3.17. *Integralni cirkularni graf* $\mathrm{ICG}_n(D)$*, pri čemu* D *sadrži dva delioca, ima PST ako i samo ako je if* $S_2(n) \geq 3$ *i* $D = \{1, n/2\}$, $D = \{1, n/4\}$.

Propozicija 2.3.18. *Minimalni broj čvorova integralnog cirkularnog grafa (koji nije unitarni Kejlijev)* $\mathrm{ICG}_n(D)$ *sa PST, jednak je* $n = 8$.

Sada možemo konstruisati klasu grafa za $n \in 8\mathbb{N}+4$. Primetimo da su u ovom slučaju ne postoji klasa grafova $\mathrm{ICG}_n(D)$ koji imaju PST, sa brojem elemenata u D manjim od 4. Graf $\mathrm{ICG}_n(D)$ gde je $n \in 8\mathbb{N}+4$, a D četvoroelementni skup se dobija kada je $\widetilde{D_3} = \emptyset$ i $D_2 = \{1\}$.



Slika 2.1: Integralni cirkularni grafovi (koji nisu unitarni Kejlijevi) sa minimalnim brojem čvorova ($\mathrm{ICG}_8(\{1,4\})$ sa leve strane i $\mathrm{ICG}_8(\{1,2\})$ sa desne) koji imaju PST

Posledica 2.3.19. *Neka je n prirodan broj takav da je $S_2(n) = 2$. Tada grafovi $\mathrm{ICG}_n(\{1,2,4,n/4\})$ i $\mathrm{ICG}_n(\{1,2,4,n/2\})$ imaju PST.*

Takođe, možemo konstruisati klasu grafova $\mathrm{ICG}_n(D)$ koji imaju PST, sa troelementnim skupom D, ali tada n mora biti deljiv brojem 16. Zaista, za $\widetilde{D_3} = \{1,2\}$ i $D_2 = \emptyset$ dobijamo grafove navedene sledećom posledicom.

Posledica 2.3.20. *Integralni cirkularni grafovi $\mathrm{ICG}_n(\{1,2,n/4\})$ i $\mathrm{ICG}_n(\{1,2,n/2\})$ imaju PST ako i samo ako je $S_2(n) \geq 4$.*

Sada možemo navesti neke klase grafova koji nemaju PST. Direktno iz Teoreme **??** zaključujemo da nema PST u grafu $\mathrm{ICG}_n(D)$ ako je n broj koji nije deljiv kvadratom prostog broja, budući da takvi brojevi nisu deljivi sa 4.

Propozicija 2.3.21. *Neka skup delioca D sadrži samo neparne delioce. Tada ne postoji PST u $\mathrm{ICG}_n(D)$.*

Dokaz. Ako je $n \in 8\mathbb{N}$ tada za svaki delilac $d \in D$ važi da je $n/d \in 8\mathbb{N}$, tj. $D = \widetilde{D_3}$, odakle sledi da $n/2, n/4 \notin D$. Poslednje je kontradikcija sa Teoremom **??**.

Ako je $n \in 8\mathbb{N} + 4$, slično prethodnom dobijamo da je $D = D_2$. Međutim, $2D_2$ i $4D_2$ nisu u D, te dobijamo da PST ne postoji u $\mathrm{ICG}_n(D)$ □

Slično dokazu prethodnog tvrđenja može se dokazati i sledeće.

Posledica 2.3.22. *Neka je $S_2(n) = 2$ i D sadrži tačno jedan paran delilac. Tada u $\mathrm{ICG}_n(D)$ nema PST.*

Propozicija 2.3.23. *Neka je $\mathrm{ICG}_n(D)$ graf takav da je $S_2(n) \geq 3$. Pretpostavimo da postoji paran delilac $d_0 \in D$ uzajamno prost sa svim ostalim deliocima $d \in D \backslash \{d_0\}$. Tada $\mathrm{ICG}_n(D)$ ima PST ako i samo ako je $D = \{1, n/2\}$ ili $D = \{1, n/4\}$.*

Iz tvrđenja **??**, **??** i **??** proizilazi sledeća posledica.

Posledica 2.3.24. *Graf $\mathrm{ICG}_n(D)$, gde D sadrži paran broj uzajamno prost sa svim ostalima u D, ima PST ako i samo ako je $S_2(n) \geq 3$ i $D = \{1, n/2\}$, $D = \{1, n/4\}$.*

2.3.3 PST između neantipodalnih čvorova u cirkularnim grafovima

U ovom delu nastavljamo sa ispitivanjem cirkularnih mreža koje poseduju PST. Korisno je izučavati određenje parametre grafova vezane za kvantnu dinamiku, imajući, pre svega, u vidu primenu u PST. Posebno bi bilo interesantno znati koliki bi bio put informacije koja bi se mogla potencijalno preneti između delova sistema modeliranih grafovima. Zato je važno znati dijametar grafova, kao i PQCD, o čemu je već bilo reči u prethodnim sekcijama. Specijalno, interesantno je znati da li je rastojanje PQCD uvek jednako dijametru grafa. Drugim rečima, da li su čvorovi između kojih se odvija PST, uvek antipodalni? Ovo pitanje je postavio Godsil u [**?**], a mi dajemo negativan odgovor određivanjem dijametra svih integralnih cirkularnih grafova sa dvoelementnim skupom deliocima, koji imaju PST.

Najpre ćemo odrediti dijametar integralnih cirkularnih grafova $\mathrm{ICG}_n(D)$ sa jednoelementnim skupom D. Ovaj rezultat je od suštinske važnosti za izračunavanje dijametra integralnih cirkularnih grafova sa dva delioca. Karakterizacijom svih integralnih cirkularnih grafova sa dvoelementnim skupom delioca koji imaju PST, pronašli smo dve klase grafova gde se PST odvija među neantipodalnih čvorova. Ove klase grafova imaju red koji je deljiv sa osam. Takođe, se moze pronaći klasa grafova $\mathrm{ICG}_n(D)$ koji imaju red oblika $8k+4$. Na ovaj način smo dokazali da za svako $n \in 4\mathbb{N}$ postoji integralni cirkularni graf reda n, takav da je PST odvija među neantipodalnih čvorova. Primetomo još da PST postoji na integralnim cirkularnim grafovima reda koji je deljiv sa četiri. Ovom metodom se takođe može naći klasa $\mathrm{ICG}_n(D)$, gde je $n \in 8\mathbb{N}+4$ takva da je PST javlja među antipodalnim čvorovima.

Dijametar integralnih cirkularnih grafova sa jednim deliocem

Rastojanje $d(u,v)$ između čvorova u i v u grafu G predstavlja broj ivica najkraćeg puta među njima (dužina grafovske geodeze među čvorovima u i v). Dijametar grafa je maksimalno rastojanje među parovima cvorova grafa.

Definicija 2.3.1. *Neka su l i N dati prirodni brojevi. Ukoliko postoje celi brojevi $s_1, s_2, \dots s_k$ takvi da je $gcd(s_i, N) = 1$, za $1 \leqslant i \leqslant k$ i $l \equiv s_1 + s_2 + \ldots + s_k \mod N$, onda k-torku $(s_1, s_2, \dots, s_k)$ nazivamo redukovanom kompozicijom broja l po modulu N ($RD_N(l)$) od k elemenata.*

Lema 2.3.25. *Za prirodne brojeve m i l takve da je $l < m$ i $gcd(l,m) = 1$, važe sledeći uslovi:*

(i) *Postoji $RD_m(l)$ od tri elemenata.*

(ii) *Ako je m neparan onda postoji $RD_m(l)$ od dva elementa.*

(iii) *Ako je m paran onda ne postoji $RD_m(l)$ od dva elementa.*

Dokaz.

(i) Kako je $gcd(l,m) = 1$ dobijamo da je $gcd(m-l, m) = 1$, pa je prema tome i $l \equiv (m-l)+l+l \mod m$.

(ii) Ako je m neparan onda je $gcd(2l, m) = 1$, te je zato $l \equiv (m-l) + 2l \mod m$.

(iii) Pretostavimo da postoji dvoelementno razlaganje $RD_m(l)$, broja l. Odavde sledi da postoje brojevi a i b koji su relativno prosti sa m i pri tome je $l \equiv a + b \mod m$. Kako je m paran, iz poslednje jednakosti proizilazi da je $l - a - b$ takođe paran. Sa druge

strane, pošto su a, b i l relativno prosti sa m, oni su neparni pa je i $l-a-b$ neparan, što nas dovodi do kontradikcije.

□

Lema 2.3.26. *Neka je $m = p^\alpha$, gde je p prost broj i $\alpha > 1$. Za prirodan broj $l < m$ deljiv sa p, postoji razlaganje $RD_m(l)$ od dva elementa, a ako je $p > 2$ postoji razlaganje $RD_m(l)$ od tri elementa.*

Dokaz. Brojevi m i $m-1$ su uzajamno prosti, a za $p > 2$ broj $m-2$ nije deljiv sa p. Dakle, na osnovu uslova leme, dvojka $((m-1), 1)$ i trojka $((m-2), 1, 1)$ predstavljaju razlaganje $RD_m(l)$ od dva i tri elementa, redom. □

Lema 2.3.27. *Za svaki prirodan broj l manji od datog broja N, postoji $RD_N(l)$ od najviše tri elementa.*

Dokaz.

(i) Neka je N prost. Kako su svi prirodni brojevi manji od N i relativno prosti sa N, svaki od njih trivijalno zadovoljava uslove tvrđenja leme.

(ii) Sada neka je $N = p^\alpha$ za proizvoljni prost broj $p \geq 2$ i $\alpha > 1$. Tada za sve brojeve koji nisu uzajamno prosti sa N postoji $RD_N(l)$ od dva elementa na osnovu Leme **??**.

(iii) Pretpostavimo da je $N = nm$, gde su $n, m > 1$ uzajamno prosti. Takođe pretpostavimo da je $m = p^\alpha$ za proizvoljni prost neparan broj p i $\alpha \geq 1$. Posmatrajmo klase kongruencije po modulu m, $C_i = \{tm + i \mid 0 \leq t \leq n-1\}$ za $0 \leq i \leq m-1$.

Dokaz dalje izvodimo koristeći indukciju po N. Za $N = p^\alpha$ gde je p prost, tvrđenje važi prema delovima (i) i (ii) dokaza. Pretpostavimo da tvrđenje važi za svako $n < N$.

Posmatrajmo proizvoljnu klasu C_k za $0 \leq k \leq m-1$. Prema pretpostavci, za svaki element $l \in C_k$ postoji prirodan broj $1 \leq x \leq 3$ takav da je

$$l \equiv s_1 + s_2 + \cdots + s_x \mod n, \tag{2.46}$$

i $gcd(s_i, n) = 1$ za svaki $1 \leq i \leq x$.

U slučaju kada je $2 \leq x \leq 3$ na osnovu Leme **??** (delovi (i) i (ii)) i Leme **??** postoje brojevi $r_1, r_2, \ldots, r_x$ takvi da je

$$l \equiv k \equiv r_1 + r_2 + \cdots + r_x \mod m, \tag{2.47}$$

i $gcd(r_i, m) = 1$ za $1 \leq i \leq x$.

Dokaz tvrđenja za $x = 1$, tj. $gcd(l, n) = 1$, se lako može svesti na slučaj kada je $x = 3$, koristeći deo (i) Leme **??**.

Kako je $gcd(n, m) = 1$, elementi proizvoljne klase formiraju potpun sistem ostataka po modulu n. Odavde sledi da za svaki element s_i postoji prirodan broj $s_i' \in C_{r_i}$, takav da je $s_i' \equiv s_i \mod n$ za svaki $1 \leq i \leq x$. To znači da na osnovu (**??**) i (**??**) dobijamo $l \equiv s_1' + s_2' + \cdots + s_x' \mod n, m$ ili ekvivalentno $l \equiv s_1' + s_2' + \cdots + s_x' \mod N = nm$, jer je $gcd(n, m) = 1$. Na osnovu izbora brojeva s_i' imamo da su oni relativno prosti sa n i m, a time sa $N = nm$.

□

Sada možemo dokazati rezultat koji se odnosi na dijametar integralnih cirkulantnih grafova sa skupom delioca $D = \{1\}$.

Teorema 2.3.28. *Za integralni cirkularni graf* $\mathrm{ICG}_n(1)$ *takav da je* $n \geqslant 2$*, važi*

$$diam\ (\mathrm{ICG}_n(1)) \quad = \quad \begin{cases} 1, & n \text{ je prost} \\ 2, & n \text{ je neparan složen ili je stepen dvojke} \\ 3, & u \text{ suprotnom.} \end{cases} \tag{2.48}$$

Dokaz. Posmatrajmo dva proizvoljna čvora $u, v \in \mathbb{Z}_n$ takva da je $u < v$ i neka je $l = v - u$. Prema Lemi **??** postoji razlaganje $RD_n(l)$ od najviše tri elementa, odakle sledi da je $diam\ (\mathrm{ICG}_n(1)) \leq 3$.

(i) Dijametar grafa je jednak jedan ako i samo ako je kompletan. Ekvivalentno, stepen regularnosti $\varphi(n)$ mora biti jednak $n - 1$. Poslednja jednakost je zadovoljena ako i samo ako je n prost broj. Stoga ćemo u nastavku pretpostaviti da je n složen i $diam(\mathrm{ICG}_n(1)) \geqslant 2$.

(ii) Ako je n stepen dvojke, prema delu (ii) Leme **??**, imamo da je $diam(\mathrm{ICG}_n(1)) = 2$. Sada ćemo pretpostaviti da je n neparan složen broj. Neka je $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ kanonska faktorizacija broja n. Koristeći indukciju po k, kao u dokazu Leme **??**, zaključujemo da postoji razlaganje $RD_{p_i^{\alpha_i}}(l)$ od dva elementa (prema delu (ii) Leme **??**), za $1 \leq i \leq k$. Dakle, postoji razlaganje $RD_n(l)$ od dva elementa, a time je i $diam\ (\mathrm{ICG}_n(1)) = 2$.

(iii) Neka je n paran broj deljiv nekim prostim neparnim brojem. To znači da se on može zapisati kao $n = 2^{\alpha_1} m$, gde je m neparan broj veći od jedan. Pretpostavimo da je $diam\ (\mathrm{ICG}_n(1)) = 2$. Izaberimo čvorove u i v takve da je l neparan i nije uzajamno prost sa m. Kako je m neparan, prema delu (ii) postoji razlaganje $RD_m(l)$ od dva elementa. Sa druge strane, prema delu (iii) Leme **??** ne postoji $RD_{2^{\alpha_1}}(l)$ od dva elementa. Zaključujemo, da ne postoji $RD_n(l)$ od dva elementa ili ekvivalentno $diam\ (\mathrm{ICG}_n(1)) \neq 2$, što je kontradikcija. Jedina preostala mogućnost je $diam\ (\mathrm{ICG}_n(1)) = 3$, čime je dokaz kompletiran.

□

PQCD i dijametar integralnih circkularnih grafova

U prvom delu sekcije razmatramo dijametar grafa $\mathrm{ICG}_n(D)$ za $D = \{1, d\}$. Izračunavamo dijametar u Teoremi **??**, gde je dokaz prirodno podeljen po lemama. Pretpostavljamo da je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gde su $p_1 < p_2 < \ldots < p_k$ različiti prosti brojevi i $\alpha_i \geq 1$.

Lema 2.3.29. *Graf* $\mathrm{ICG}_n(D)$ *je kompletan ako i samo ako je* $n = p^2$ *i* $d = p$ *gde je* p *proizvoljni prost broj.*

Dokaz. Integralni cirkularni graf $\mathrm{ICG}_n(D)$ je kompletan ako i samo ako je $D = D_n \setminus \{n\}$.

($\Rightarrow$:) Pretpostavimo da je $\mathrm{ICG}_n(D)$ kompletan. Odavde imamo da je $|D| = |D_n \setminus \{n\}|$. Poslednja jednakost implicira da je $\tau(n) - 1 = 2$, gde funkcija $\tau(n)$ označava broj delioca broja n, kao što smo ranije već naveli. Odavde je

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) - 1 = 2.$$

Kako je $\alpha_i + 1 \geq 2$ za $1 \leq i \leq k$ zaključujemo da je $k = 1$ i $\alpha_1 = 2$. Ovaj smer leme je sad očigledan.
($\Leftarrow$:) Za $n = p^2$ i $d = p$ imamo da je $D = \{1, p\} = D_n \setminus \{n\}$, čime je dokaz kompletiran. □

Lema 2.3.30. *Neka je n paran broj i $k \geq 2$. Tada je $diam(\mathrm{ICG}_n(D)) = 2$ ako je jedan od sledeća dva uslova zadovoljen*

(i) d je stepen dvojke

(ii) $n = 2^{\alpha_1} p$ i $d = p$ za neparan prost broj p.

Dokaz. Neka su $u, v \in \mathbb{Z}_n$ dva proizvoljna čvora i $l = v - u$.

(i) Pretpostavimo takođe da je $d = 2^\alpha$ gde je $1 \leq \alpha \leq \alpha_1$. Dokazaćemo da postoje brojevi $s_1, s_2 \in \mathbb{Z}_n$ takvi da je $l \equiv s_1 + s_2 \mod n$ i $s_1, s_2 \in G_n(D)$.

Ako je $l \in 2\mathbb{N}$ onda ćemo naći $s_1, s_2 \in \mathbb{Z}_n$ takve da postoji razlaganje $RD_n(l)$ od dva elementa. Neka je $n = 2^{\alpha_1} m$ gde je m neparan. Deo (ii) Teoreme **??**, garantuje postojanje $RD_m(l)$ od dva elementa. Sa druge strane, iz Leme **??** (part (ii)) sledi egzistencija razlaganja $RD_{2^{\alpha_1}}(l)$ od dva elementa, pa prema tome imamo i razlaganje $RD_n(l)$ od dva elementa. Primetimo da postoji $RD_n(l)$ od x elemenata ako i samo ako postoji $RD_n(l')$ od x elemenata, gde je l' ostatak broja l po modulu n. Poslednje je tačno jer je $l \equiv l' \equiv s_1 + s_2 + \ldots + s_x \mod n$, gde je $\gcd(s_i, n) = 1$. Odavde sledi da gornje razmatranje takođe stoji i kada je $l > m$ ili $l > 2^{\alpha_1}$.

Ako je $l \in 2\mathbb{N} + 1$ tada bez gubljenja opštosti, pretpostavimo da je $s_1 \in 2\mathbb{N} + 1$ i $s_2 \in 2\mathbb{N}$. Odavde sledi da je $gcd(s_1, n) = 1$ i $gcd(s_2, n) = 2^\alpha$. Iz poslednjeg zaključujemo da $p_i \nmid s_1$ za svako $1 \leq i \leq k$ i ako je $\alpha < \alpha_1$ takođe mora biti $2^\alpha \mid s_2$, $2^{\alpha+1} \nmid s_2$ i $p_i \nmid s_2$ za svako $2 \leq i \leq k$. Poslednje relacije mogu biti zapisane na sledeći način : $s_1 \not\equiv 0 \mod p_i$ za svako $1 \leq i \leq k$, $s_2 \equiv 0 \mod 2^\alpha$, $s_2 \not\equiv 0 \mod 2^{\alpha+1}$ i $s_2 \not\equiv 0 \mod p_i$ za svako $2 \leq i \leq k$. Kako još važi da je $s_1 \equiv l - s_2 \mod n$, koristeći gornje relacije dobijamo da je $s_2 \equiv 0 \mod 2^\alpha$, $s_2 \not\equiv 0 \mod 2^{\alpha+1}$ i $s_2 \not\equiv \{0, l\} \mod p_i$ for $2 \leq i \leq k$. Konačno, udruživanjem prve dve relacije dobijamo sledeći sistem

$$\begin{aligned} s_2 &\equiv 2^\alpha \mod 2^{\alpha+1} \\ s_2 &\not\equiv \{0, l\} \mod p_i \text{ za svako } 2 \leq i \leq k. \end{aligned}$$

Prema Kineskoj teoremi o ostacima postoji rešenje s gornjeg sistema takvo da je $0 \leq s < M$ i $s_2 \equiv s \mod M$, gde je $M = 2^{\alpha+1} p_2 \dots p_k$. Primetino da je $M \leq n$, jer je $\alpha < \alpha_1$.

Ako je $\alpha = \alpha_1$ onda je uslov $gcd(s_2, n) = 2^\alpha$ ekvivalentan sa $s_2 \equiv 0 \mod 2^{\alpha_1}$ i $s_2 \not\equiv 0 \mod p_i$ za svako $2 \leq i \leq k$. To znači da se gornji sistem redukuje na

$$\begin{aligned} s_2 &\equiv 0 \mod 2^{\alpha_1} \\ s_2 &\not\equiv \{0, l\} \mod p_i \text{ za svako } 2 \leq i \leq k. \end{aligned}$$

Koristeći ponovo Kinesku teoremu o ostacima, sistem ima rešenje s takvo da je $0 \leq s < M$ i $s_2 \equiv s \mod M$ gde je $M = 2^{\alpha_1} p_2 \dots p_k$.

(ii) Pretpostavimo da je $n = 2^{\alpha_1}p$ i $d = p$. Ako je $l \in 2\mathbb{N}+1$ imamo da je tačno jedan od uslova zadovoljen: $p \mid l$ ili $p \nmid l$. Odavde sledi da je onda, za dato l, tačno jedan od sledećih uslova zadovoljen $gcd(l,n) = p$ ili $gcd(l,n) = 1$. U oba slučaja zaključujemo da mora biti $l \in G_n(D)$.

Kada je $l \in 2\mathbb{N}$ postoji razlaganje $RD_n(l)$ od dva elementa kao što je već pokazano u (i).

□

Lema 2.3.31. *Neka je p_i proizvoljan prost delilac broja n gde je $2 \leq i \leq k$. Tada imamo da je $k = i = 2$ i $\alpha_2 = 1$ ako i samo ako za svako neparno $l \in \mathbb{Z}_n$ važi da je $l \in G_n(1, p_i)$.*

Dokaz.
($\Rightarrow$:) Za $l \in 2\mathbb{N}+1$ imamo da je $gcd(l,n) = p_i$ ili $gcd(l,n) = 1$,u zavisnosti od toga da li $p_i \mid l$ ili $p_i \nmid l$. U oba slučaja zaključujemo da je $l \in G_n(D)$.

($\Leftarrow$:) Pretpostavimo da za sve neparne $l \in \mathbb{Z}_n$ imamo da je $l \in G_n(1, p_i)$, tj. ili je $gcd(l,n) = 1$ ili $gcd(l,n) = p_i$. Kako je broj neparnih $l \in \mathbb{Z}_n$ takvih da je $gcd(l,n) = 1$ jednak je $\varphi(n)$, dok je broj neparnih $l \in \mathbb{Z}_n$ takvih da je $gcd(l,n) = p_i$ jednak je $\varphi(n/p_i)$, imamo da je

$$\varphi(n) + \varphi(n/p_i) = \frac{n}{2}. \tag{2.49}$$

Neka je $\alpha_i \geq 2$. Koristeći Ojlerovu formulu dobijamo

$$\begin{aligned} 2^{\alpha_1-1}p_2^{\alpha_2}\dots p_k^{\alpha_k} &= 2^{\alpha_1-1}p_2^{\alpha_2-1}(p_2-1)\dots p_k^{\alpha_k-1}(p_k-1) \\ &+ 2^{\alpha_1-1}p_2^{\alpha_2-1}(p_2-1)\dots p_i^{\alpha_i-2}(p_i-1)\dots p_k^{\alpha_k-1}(p_k-1) \Leftrightarrow \\ p_2\dots p_i^2\dots p_k &= (p_2-1)\dots(p_i-1)\dots(p_k-1)(p_i+1) \\ &= (p_2-1)\dots(p_i^2-1)\dots(p_k-1). \end{aligned}$$

Vidimo da ova jednačina nema rešenja, jer je leva strana jednakosti očigledno veća od desne. Pretpostavimo sada da je $\alpha_i = 1$. Relacija (**??**) sada izgleda

$$\begin{aligned} 2^{\alpha_1-1}p_2^{\alpha_2}\dots p_i\dots p_k^{\alpha_k} &= 2^{\alpha_1-1}p_2^{\alpha_2-1}(p_2-1)\dots(p_i-1)\dots p_k^{\alpha_k-1}(p_k-1) \\ &+ 2^{\alpha_1-1}p_2^{\alpha_2-1}(p_2-1)\dots p_{i-1}^{\alpha_{i-1}-1}(p_{i-1}-1)p_{i+1}^{\alpha_{i+1}-1}(p_{i+1}-1)\dots p_k^{\alpha_k-1}(p_k-1) \Leftrightarrow \\ p_2\dots p_i\dots p_k &= (p_2-1)\dots(p_{i-1}-1)(p_{i+1}-1)\dots(p_k-1)p_i. \end{aligned}$$

Zaključujemo da jednakost važi ako i samo ako je $k = 2$, jer za $k \geq 3$ leva strana je očigledno veća od desne. Dakle $i = 2$, te je $\alpha_2 = 1$.
□

Lema 2.3.32. *Neka je $n > 4$ paran broj i $k \geq 2$. Tada je $diam(\mathrm{ICG}_n(D)) = 3$ ako i samo ako su sledeći uslovi zadovoljeni*

(i) *d nije stepen dvojke*

(ii) *$n \neq 2^{\alpha_1}p$ ili $d \neq p$ za bilo koji prost broj p.*

Dokaz.
($\Rightarrow$:) Pretpostavimo da je $diam(\mathrm{ICG}_n(D)) = 3$ i da je bar jedan od delova leme (i) ili (ii) netačan. Odavde sledi da su zadovoljeni uslovi Leme **??** odakle je $diam(\mathrm{ICG}_n(D)) = 2$. Ovo je kontradikcija sa pretpostavkom.
($\Leftarrow$:) Pretpostavimo sada da su zadovoljeni delovi (i) i (ii). Odavde sledi da za $2 \leq i \leq k$ postoji neparan prost delilac p_i brojeva n i d.

Ako je $d \neq p_i$ onda je $gcd(p_i, n) = p_i \notin \{1, d\}$, tj. $p_i \notin G_n(D)$. Neka su $u, v \in \mathbb{Z}_n$ dva proizvoljna čvora takva da je $p_i = v - u$. Pretpostavimo da je rastojanje čvorova u i v jednako dva. To znači da postoje brojevi $s_1, s_2 \in G_n(D)$ takvi da je $s_1 + s_2 \equiv p_i \mod n$. Kako je $p_i \in 2\mathbb{N} + 1$ i $n \in 2\mathbb{N}$ onda su s_1 i s_2 različite parnosti, te je $gcd(s_1, n) \neq gcd(s_2, n)$. Bez gubljenja opštosti, pretpostavimo da je $gcd(s_1, n) = 1$ i $gcd(s_2, n) = d$. Dalje dobijamo da $p_i \nmid s_1$ i $p_i \mid s_2$, pa $p_i \nmid s_1 + s_2$, što je nemoguće. Dakle, zaključujemo da je rastojanje među čvorovima u i v veće od dva.

Ako je $d = p_i$, prema Lemi **??**, postoji neparan $l \in \mathbb{Z}_n$ takav da je $gcd(l, n) \notin \{1, p_i\}$. Posmatrajmo čvorove u i v takve da je $l = v - u$ i $v > u$. Pretpostavimo da je rastojanje čvorova u i v jednako dva. To znači da postoje $s_1, s_2 \in G_n(D)$ takvi da je $s_1 + s_2 \equiv l \mod n$. Kako je $l \in 2\mathbb{N}+1$, s_1 i s_2 su različite parnosti, pa bez gubljenja opštosti možemo pretpostaviti da je $s_1 \in 2\mathbb{N}$. Sa druge strane, imamo da je $gcd(s_1, n) \in \{1, p_i\}$ odakle sledi da je $s_1 \in 2\mathbb{N}+1$. Ovo je kontradikcija, pa je rastojanje među čvorovima u i v veće od dva.

U oba slučaja su nađena dva čvora čije je rastojanje veće ili jednako tri, odakle je $diam(\mathrm{ICG}_n(D)) \geq 3$. Prema Teoremi **??** zaključujemo da je $diam(\mathrm{ICG}_n(D)) \leq diam(\mathrm{ICG}_n(1)) \leq 3$, čime je dokaz teoreme završen. □

Sada možemo formulisati glavni rezultat ovog odeljka koji ima važnu primenu u Teoremi **??**. Ovaj rezultat je direktna posledica Lema **??**, **??** i **??**.

Teorema 2.3.33. *Za dati graf* $\mathrm{ICG}_n(1, d)$ *i* $n \geqslant 4$ *imamo da je*

$$diam(\mathrm{ICG}_n(1,d)) = \begin{cases} 1, & n = p^2,\ d = p,\ p \text{ je prost} \\ 2, & n \text{ neparan različit od prostog broja ili} \\ & n \text{ je paran i } d \text{ je stepen broja 2 ili} \\ & n \text{ je paran, } k = 2, \alpha_2 = 1 \text{ i } d = p_2 \\ 3, & \text{u suprotnom.} \end{cases} \tag{2.50}$$

Već smo iskomentarisali da je PQCD integralnog cirkularnog grafa $\mathrm{ICG}_n(D)$ jednako jedan ili dva u zavisno od toga da li $n/2 \in D$ ili $n/4 \in D$. To znači da PST postoji između antipodalnih čvorova ako i samo ako je $1 \leq diam(\mathrm{ICG}_n(1, d)) \leq 2$.

Teorema 2.3.34. *PST postoji između neantipodalnih čvorova u* $\mathrm{ICG}_n(D)$ *za* $|D| = 2$ *ako i samo ako je jedan od uslova zadovoljen*

(i) $n \in 8\mathbb{N}$ *i* $D = \{1, n/2\}$

(ii) $n \in 8\mathbb{N}$ *i nije stepen broja* 2 *i* $D = \{1, n/4\}$.

Dokaz.

(i) PST postoji u $\mathrm{ICG}_n(1, n/2)$ između antipodalnih čvorova b i $b + n/2$ za $0 \leq b \leq n/2 - 1$ ako i samo ako je $diam(\mathrm{ICG}_n(1, n/2)) = d(b, b + n/2) = 1$. Odavde sledi da $\mathrm{ICG}_n(1, n/2)$ za $n \in 8\mathbb{N}$ mora biti kompletan. Međutim, na osnovu Teoreme **??** imamo da je poslednje tačno ako je n kvadrat prostog broja. Ponovo ovo je kontradikcija pošto $8 \mid n$. Odavde zaključujemo da ne postoje antipodalni čvorovi b i $b+n/2$ za $0 \leq b \leq n/2-1$ u $\mathrm{ICG}_n(1, n/2)$ za $8 \mid n$, čime je završen prvi deo dokaza.

(ii) Slično se može zaključiti da PST postoji u $\mathrm{ICG}_n(1, n/4)$ između antipodalnih čvorova b i $b + n/2$ za $0 \leq b \leq n/2 - 1$ ako i samo ako je dijametar grafa $\mathrm{ICG}_n(1, n/4)$ za $n \in 8\mathbb{N}$ jednak dva. Kako je n paran, koristeći Teoremu **??** imamo dve mogućnosti takve da je $diam(\mathrm{ICG}_n(1, n/4)) = 2$.

Ako je $d = n/4$ stepen dvojke, tada je i broj n takođe stepen dvojke. Odavde zaključujemo da su čvorovi b i $b + n/2$ antipodalni za $0 \leq b \leq n/2 - 1$ u $\mathrm{ICG}_n(1, n/4)$ za $n = 2^{\alpha_1}$ i $\alpha_1 \geq 3$.

Ako je $n = 2^{\alpha_1} p_2$ i $d = p_2$, sledi da je $d = n/4 = p_2$ i zato je $n = 4p_2$. Prema pretpostavci imamo da je $n \in 8\mathbb{N}$ što je kontradikcija pa je zbog toga $diam(\mathrm{ICG}_n(1, n/4)) \neq 2$. Odavde zaključujemo da ne postoje antipodalni čvorovi b i $b + n/2$ za $0 \leq b \leq n/2 - 1$ u $\mathrm{ICG}_n(1, n/4)$ za $8 \mid n$.

□

Nađene su dakle dve klase integralnih cirkularnih grafova $\mathrm{ICG}_n(D)$ koji imaju PST među parovima neantipodalnih čvorova za $n \in 8\mathbb{N}$. Sa druge strane znamo da postoji integralni cirkularni graf sa n čvorova koji ima PST ako i samo ako je $n \in 4\mathbb{N}$. Zato ćemo ispitati klase grafove date u Posledici **??** i odgovoriti na pitanje o postojanju PST među neantipodalnim čvorovima za svako $n \in 4\mathbb{N}$.

Koristeći sličan pristup kao u dokazu Leme **??** možemo pokazati da je $\mathrm{ICG}_n(1, d_1, d_2, d_3)$ kompletan ako i samo ako je $n = p^4$ i $d_i = p^i$ za $1 \leq i \leq 3$ i proizvoljan prost broj p. Odavde sledi da $\mathrm{ICG}_n(1, 2, 4, n/2)$ za $n \in 8\mathbb{N} + 4$ nije kompletan, pa PST postoji samo između neanitpodalnih čvorova.

Kako je $diam(\mathrm{ICG}_n(1, 2, 4, n/4)) \leq diam(\mathrm{ICG}_n(1, 2)) = 2$ na osnovu Leme **??** (deo (i)), može se zaključiti da je $diam(\mathrm{ICG}_n(1, 2, 4, n/4)) = 2$ za $n \in 8\mathbb{N} + 4$. Ovo nas dovodi do konačnog zaključka da PST postoji samo između antipodalnih čvorova u $\mathrm{ICG}_n(1, 2, 4, n/4)$ za $n \in 8\mathbb{N} + 4$. Na koncu ove diskusije, možemo formulisati završni rezultat.

Teorema 2.3.35. *Postoji graf* $\mathrm{ICG}_n(D)$ *koji ima PST između neantipodalnih čvorova ako i samo ako je* $n \in 4\mathbb{N}$.

Ispostavilo se da je problem karakterizacije integralnih cirkularnih grafova dijametra dva (kao i onih koji imaju PST) je interesantan. Čak i u nekim specijalnim slučajevima kada se skup delioca sastoji od nekoliko elemenata, nemoguće je elegantno rešiti ovaj problem. Grafovi sa malim dijametrom imaju takođe primenu u hemiskoj teoriji grafova. Takođe, klasu samokomplementarnih integralnih cirkularnih grafova treba tražiti među onima koji imaju dijametar dva.

2.4 PST na klasama težinskih cirkularnih grafova

U ovoj sekciji ćemo predstaviti nove klase težinskih cirkularnih grafova koji imaju PST. Ove klase obuhvataju nađene integralne cirularne grafove sa PST svojstvom u netežinskom slučaju. Šta više, pokazaćemo postojanje težinskih integralnih cirkularnih grafova reda n koji ima PST ako i samo ako je n paran. U Teoremi **??** ćemo dokazati nepostojanje PST u klasi težinskin integralnih cirkularnih grafova $\mathrm{WICG}(n;C)$ za koje je $c_{n/4} = c_{n/2} = 0$.

Neka je k proizvoljan prirodan broj. Primetimo da $\mathrm{WICG}(n;C)$ ima PST ako i samo ako $\mathrm{WICG}(n;2^kC)$ ima PST. Zaista, neka su $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ i $\mu_0, \mu_1, \ldots, \mu_{n-1}$ sopstvene vrednosti $\mathrm{WICG}(n;C)$ i $\mathrm{WICG}(n;2^kC)$, redom. Sada možemo uočiti sledeće relacije, za svako $1 \leq j \leq n-1$,

$$\mu_j - \mu_{j-1} = \sum_{d \in D_n} 2^k c_d (c(j, n/d) - c(j-1, n/d)) = 2^k (\lambda_j - \lambda_{j-1}).$$

Odavde sledi da je $S_2(\mu_j - \mu_{j-1}) = S_2(\lambda_j - \lambda_{j-1}) + k$, te prema Teoremi **??** važi pomenuto tvrđenje.

Poslednja opaska nam omogućava da pretpostavimo da $\mathrm{WICG}(n;C)$ sa PST, ima bar jednu neparnu težinu iz C. U suprotnom, ako bi sve težine c_d za $d \in D_n$ bile parne, onda bi mogli da ih podelimo dovoljan broj puta dvojkom, čime bi dobili da je bar jedna od težina c_d neparna, a graf sa novim težinama bi i dalje posedovao PST. Zato ćemo u ostatku poglavlja pretpostaviti da postoji bar jedno $c_d \in 2\mathbb{N}+1$ za $d \in D_n$.

Teorema 2.4.1. *Graf* $\mathrm{WICG}(n;C)$ *ima PST ako je* $c_{n/2^a}$ *neparan i* $c_d \in 4\mathbb{N}$ *za* $d \in D_n \backslash \{n/2^a\}$, *gde je* $1 \leq a \leq 2$.

Dokaz. Za $a \in \{1,2\}$ i $1 \leq j \leq n-1$, razlika uzastopnih sopstvenih vrednosti je

$$\lambda_j - \lambda_{j-1} = \sum_{d \in D_n \backslash \{n/2^a\}} c_d (c(j, n/d) - c(j-1, n/d)) + c_{n/2^a}(c(j, 2^a) - c(j-1, 2^a)).$$

Ako je $a = 1$, prema relaciji (16) Propozicije **??** zaključujemo da je $|c(j,2) - c(j-1,2)| = 2$, pa je otuda $c_{n/2}(c(j,2) - c(j-1,2)) \in 4\mathbb{N}+2$. Ako je $a = 2$, za oba slučaja $j \in 4\mathbb{N}+2$ i $j \in 4\mathbb{N}$ takođe imamo da je $|c(j,4) - c(j-1,4)| = 2$, te je zato $c_{n/4}(c(j,4) - c(j-1,4)) \in 4\mathbb{N}+2$.

Koristeći dalje uslove teoreme, direktno dobijamo da je $\sum_{d \in D_n \backslash \{n/2^a\}} c_d (c(j, n/d) - c(j-1, n/d)) \in 4\mathbb{N}$. Konačno zaključujemo da je $\lambda_j - \lambda_{j-1} \in 4\mathbb{N}+2$ za $1 \leq j \leq n-1$, odakle je sledi postojanje PST u $\mathrm{WICG}(n;C)$ prema Teoremi **??**. □

Primetimo da tvrđenje i dalje važi ako je $S_2(c_d) \geq S_2(c_{n/2^a}) + 2$ za $d \in D_n \backslash \{n/2^a\}$ i $a \in \{1,2\}$.

Iz prethodne teoreme vidimo da pridruživanjem opisanih težina ivicama grafa $\mathrm{ICG}_n(D)$ tako da je $n/2 \in D$ or $n/4 \in D$ možemo dobiti težinski graf koji ima PST. Ovaj rezultat očigledno generalizuje Teoremu **??**, jer u ovom slučaju oba delioca $n/4$ i $n/2$ mogu pripadati D, bez ikakvih dodatnih uslova za ostale delioce iz D, pri čemu je n parno. Zato ćemo se u ostatku poglavlja fokusirati na traženje $\mathrm{WICG}(n;C)$ sa PST takvih da je $c_{n/4} = c_{n/2} = 0$. Zapravo, nalazimo da ne postoji celobrojni vektor težina C grafa $\mathrm{WICG}(n;C)$ koji ima PST, takav da su tačno dve težine c_{d_1} i c_{d_2} pozitivne. To znači da je nemoguće dodeliti težine ivicama odgovarajućeg netežinskog grafa $\mathrm{ICG}_n(D)$ takvog da $n/2, n/4 \notin D$ i $|D| = 2$ koji bi imao PST.

Primetimo takođe da u slučaju kada je tačno jedna težina $c_d \in C$ različita od nule za neko $d \in D_n$, tada $\mathrm{WICG}(n;C)$ ima PST ako i samo ako $\mathrm{ICG}_n(\{d\})$ ima PST. Ovaj zaključak je jasan

budući da važi relacija $\mu_i = c_d\lambda_i$ za $0 \leq i \leq n-1$, gde su μ_i i λ_i sopstvene vrednosti grafova $\mathrm{WICG}(n;C)$ i $\mathrm{ICG}_n(d)$, redom. Tada, na osnovu Teoreme **??** zaključujemo da ne postoji PST u $\mathrm{WICG}(n;C)$ izuzev trivijalnih slučajeva za hiperkocke K_2 i C_4.

Lema 2.4.2. *Neka su* $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ *sopstvene vrednosti grafa* $\mathrm{WICG}(n;C)$. *Tada važi da je* $\lambda_2 - \lambda_1$ *parno.*

Dokaz.

Prema relaciji (1.13) Propozicije **??** imamo da je $\lambda_1 = \sum_{d\in D} c_d\mu(n/d)$. Kako $4 \mid n/d$ za svaki $d \in D_2 \cup \widetilde{D_3}$ zaključujemo da je $\mu(n/d) = 0$ te je zato $\lambda_1 = \sum_{d\in D_0\cup D_1} c_d\mu(n/d)$. Koristeći Propoziciju **??** (1.14) još jednom, vidimo da je $\lambda_2 = \sum_{d\in D_0} c_d\mu(n/d) + \sum_{d\in D_1} c_d\mu(n/2d) + \sum_{d\in D_2\cup\widetilde{D_3}} 2c_d\mu(n/2d)$. Za $d \in \widetilde{D_3}$ dobija se da $4 \mid n/2d$, odakle prozilazi da je $\mu(n/2d) = 0$ i

$$\lambda_2 - \lambda_1 = \sum_{d\in D_1} c_d(\mu(n/2d) - \mu(n/d)) + 2\sum_{d\in D_2} c_d\mu(n/2d) = 2\sum_{d\in D_1\cup D_2} c_d\mu(n/2d) \in 2\mathbb{N}. \quad (2.51)$$

□

Teorema 2.4.3. *Neka je* $\mathrm{WICG}(n;C)$ *težinski integralni cirkularni graf takav da n nije deljiv kvadratom prostog broja i* $c_{n/4} = c_{n/2} = 0$. *Ako postoje* $d_1, d_2 \in D_n$ *takvi da je* $c_{d_1}, c_{d_2} > 0$ *i* $c_d = 0$ *za svako* $d \in D_n \setminus \{d_1, d_2\}$ *tada nema PST u* $\mathrm{WICG}(n;C)$.

Dokaz. Pretpostavimo da $\mathrm{WICG}(n;C)$ ima PST. Prema Propoziciji **??** imamo

$$\lambda_1 - \lambda_0 = c_{d_1}(\mu(n/d_1) - \varphi(n/d_1)) + c_{d_2}(\mu(n/d_2) - \varphi(n/d_2)). \quad (2.52)$$

Kako $\mathrm{WICG}(n;C)$ ima PST, koristeći Teoremu **??** i Lemu **??** važi da je $\lambda_1 - \lambda_0 \in 2\mathbb{N}$. Takođe, oba broja n/d_1 i n/d_2 nisu deljivi kvadratom prostog broja pa je $\mu(n/d_i) \in \{-1, 1\}$ za $1 \leq i \leq 2$. Sa druge strane je $d_i \neq n/2$, odakle sledi da je $\varphi(n/d_i) \in 2\mathbb{N}$ za $1 \leq i \leq 2$. Konačno se može zaključiti da su oba člana $\varphi(n/d_1) - \mu(n/d_1)$ i $\varphi(n/d_2) - \mu(n/d_2)$ neparni i kako jedna od težina c_{d_1} i c_{d_2} mora biti neparna, to onda obe težine moraju biti neparne da bi $\lambda_1 - \lambda_2$ bilo parno.

Kako je $\mathrm{WICG}(n;C)$ povezan tada je $\gcd(d_1, d_2) = 1$ odakle proizilazi da d_1 i d_2 ne mogu biti oba parna. Posmatrajmo slučaj kada su d_1 i d_2 različite parnosti i bez gubljena opštosti pretpostavimo da je $d_1 \in 2\mathbb{N}$ i $d_2 \in 2\mathbb{N}+1$. Kako n nije deljiv kvadratom prostog broja to je $n \in 4\mathbb{N}+2$, što znači da je $d_1 \in D_0$ i $d_2 \in D_1$. Relacija (**??**) se sada svodi na

$$\lambda_2 - \lambda_1 = c_{d_2}(\mu(n/2d_2) - \mu(n/d_2)) = -2c_{d_2}\mu(n/d_2) \in 4\mathbb{N}+2.$$

Prema Teoremi **??** imamo da su sve razlike $\lambda_i - \lambda_{i-1} \in 4\mathbb{N}+2$ za $1 \leq i \leq n-1$. Sa druge strane, koristeći relacije (1.15) and (1.16) Propozicije **??** imamo da je

$$\lambda_{n/2+1} - \lambda_{n/2} = c_{d_1}(\mu(n/d_1) - \varphi(n/d_1)) + c_{d_2}(-\mu(n/d_2) + \varphi(n/d_2)).$$

Osim toga, oduzimajući razlike $\lambda_1 - \lambda_0$ i $\lambda_{n/2+1} - \lambda_{n/2}$

$$(\lambda_1 - \lambda_0) - (\lambda_{n/2+1} - \lambda_{n/2}) = 2c_{d_2}(\mu(n/d_2) - \varphi(n/d_2)).$$

Kako su $\lambda_1 - \lambda_0, \lambda_{n/2+1} - \lambda_{n/2} \in 4\mathbb{N}+2$, leva strana gornje relacije je deljiva sa četiri. Međutim poslednja činjenica predstavlja kontradikciju pošto je desna strana jednakosti $2c_{d_2}(\mu(n/d_2) - \varphi(n/d_2)) \in 4\mathbb{N}+2$.

Kako smo eliminisali prethodni slučaj, sada istražujemo slučaj kada su oba delioca d_1 i d_2 neparni. Neka su $r_1, r_2, \ldots, r_s$ svi neparni prosti delioci broja n, koji ne dele d_1 i $q_1, q_2, \ldots, q_l$ neparni prosti delioci od n, koji ne dele d_2. Bez gubljenja opštosti možemo pretpostaviti da je $d_1 > d_2$ odakle sledi da postoji prost neapran delilac p takav da $p \mid d_1$. Otuda, dobijamo da $p \notin \{r_1, r_2, \ldots, r_s\}$. Kako je $\gcd(d_1, d_2) = 1$ onda $p \nmid d_2$, pa je zato $p \in \{q_1, q_2, \ldots, q_l\}$. Sada možemo uzeti $0 \leq j_0 \leq n-1$ takvo da je

$$\begin{aligned} j_0 &\not\equiv \{0,1\} \mod r_i \text{ for } 1 \leq i \leq s. \\ j_0 &\equiv 0 \mod p \\ j_0 &\not\equiv 1 \mod q_i \text{ for } 1 \leq i \leq l \text{ such that } q_i \neq p. \end{aligned}$$

Na osonovu Kinseke teoreme o ostacima, važi da postoji $0 \leq j_0 \leq n-1$ koje je rešenje gornjeg sistema, po modulu $n/2$.

Zaključujemo da je $\gcd(j_0, n/d_1) \in \{1, 2\}$ i $p \mid \gcd(j_0, n/d_2)$, pa je zato $c(j_0, n/d_1) \in 2\mathbb{N}+1$ i $c(j_0, n/d_2) \in 2\mathbb{N}$, prema Lemi **??**. Sada imamo da je

$$\lambda_{j_0} = c_{d_1} c(j_0, n/d_1) + c_{d_2} c(j_0, n/d_2) \in 2\mathbb{N}+1.$$

Slično, važi $\gcd(j_0 - 1, n/d_1) \in \{1, 2\}$ i $\gcd(j_0 - 1, n/d_2) \in \{1, 2\}$ odakle je $c(j_0 - 1, n/d_1) \in 2\mathbb{N}+1$ i $c(j_0 - 1, n/d_2) \in 2\mathbb{N}+1$. Tada je

$$\lambda_{j_0-1} = c_{d_1} c(j_0 - 1, n/d_1) + c_{d_2} c(j_0 - 1, n/d_2) \in 2\mathbb{N}$$

i $\lambda_{j_0} - \lambda_{j_0-1} \in 2\mathbb{N}+1$ što nas dovodi do kontradikcije.

□

Teorema 2.4.4. *Neka je* $\mathrm{WICG}(n; C)$ *težinski integralni cirkularni graf takav da je* $S_2(n) = 2$ *i* n *nije deljiv kvadratom prostog neparnog broja, pri čemu važi* $c_{n/4} = c_{n/2} = 0$. *Ako postoje delioci* $d_1, d_2 \in D_n$ *takvi da je* $c_{d_1}, c_{d_2} > 0$ *i* $c_d = 0$ *za svako* $d \in D_n \setminus \{d_1, d_2\}$ *onda PST ne postoji u grafu* $\mathrm{WICG}(n; C)$.

Dokaz. Pretpostavimo da $\mathrm{WICG}(n; C)$ ima PST. Kao i u prethodnoj teoremi razlikujemo dva slučaja.

Slučaj 1. Delioci d_1 i d_2 su različite parnosti i bez gubljenja opštosti pretpostavimo da je $d_1 \in 2\mathbb{N}$ i $d_2 \in 2\mathbb{N}+1$. Koristeći relaciju (**??**) dobijamo

$$\lambda_1 - \lambda_0 = c_{d_1}(\mu(n/d_1) - \varphi(n/d_1)) - c_{d_2}\varphi(n/d_2).$$

Kako $\mathrm{WICG}(n; C)$ ima PST, prema Teoremi **??** i Lemi **??** važi da je $\lambda_1 - \lambda_0 \in 2\mathbb{N}$, kao i da su sve razlike $\lambda_i - \lambda_{i-1} \in 2\mathbb{N}$ za svako $1 \leq i \leq n-1$. Činjenice da su $\mu(n/d_1) - \varphi(n/d_1) \in 2\mathbb{N}+1$ i $\varphi(n/d_2) \in 2\mathbb{N}$ dovode do zaključaka da je $c_{d_1} \in 2\mathbb{N}$ i $c_{d_2} \in 2\mathbb{N}+1$ (jedna od težina iz C mora biti neparan broj).

Iz uslova parnosti delilaca d_1 i d_2 sledi da je $d_1 \in D_0 \cup D_1$ i $d_2 \in D_2$, pa je

$$\lambda_2 - \lambda_1 = \begin{cases} c_{d_1}(\mu(n/2d_1) - \mu(n/d_1)) + 2c_{d_2}\mu(n/2d_2), & d_1 \in D_1 \\ 2c_{d_2}\mu(n/2d_2), & d_1 \in D_0 \end{cases}. \tag{2.53}$$

U oba slučaja imamo da je $\lambda_2 - \lambda_1 \in 4\mathbb{N}+2$, zbog činjenica da je $c_{d_1}(\mu(n/2d_1) - \mu(n/d_1)) \in 4\mathbb{N}$ i $2c_{d_2}\mu(n/2d_2) \in 4\mathbb{N}+2$. Korisreći Teoremu **??** još jednom, dobijamo da je $\lambda_1 - \lambda_0 \in 4\mathbb{N}+2$.

Poslednja relacija je tačna ako i samo ako je zadovoljen uslov $c_{d_1} \in 4\mathbb{N}$ i $\varphi(n/d_2) \in 4\mathbb{N}+2$ ili uslov $c_{d_1} \in 4\mathbb{N}+2$ i $\varphi(n/d_2) \in 4\mathbb{N}$.

Ako je $\varphi(n/d_2) \in 4\mathbb{N}+2$ onda je lako videti da je $n/d_2 \in \{p^\alpha, 2p^\alpha\}$ za neki neparan prost broj p i $\alpha \geq 1$. Međutim, imamo da je $n/d_2 \in 4\mathbb{N}$, pa je zato $\varphi(n/d_2) \notin 4\mathbb{N}+2$. Pošto smo eliminisali prethodni slučaj, sada možemo pretpostaviti da je $c_{d_1} \in 4\mathbb{N}+2$.

Pretpostavimo takođe da je $d_2 > 1$. Tada postoji neparan prost broj p takav da $p \mid d_2$ i pošto je $\gcd(d_1, d_2) = 1$ onda $p \nmid d_1$. Neka su $r_1, r_2, \ldots, r_s$ svi neparni prosti delioci broja n, koji ne dele d_1 i $q_1, q_2, \ldots, q_l$ svi neparni prosti delioci broja n, koji ne dele d_2. Sada možemo odabrati takvo $0 \leq j_0 \leq n-1$ da je

$$\begin{aligned} j_0 &\equiv 0 \mod p \\ j_0 &\not\equiv 1 \mod r_i \text{ za } 1 \leq i \leq s \text{ tako da je } r_i \neq p \\ j_0 &\not\equiv 0 \mod q_i \text{ za } 1 \leq i \leq l. \end{aligned}$$

Primetimo da $p \notin \{q_1, q_2, \ldots, q_l\}$ jer $p \mid d_2$. Prema Kineskoj teoremi o ostacima, sledi da postoji ovakvo $0 \leq j_0 \leq n-1$ koje je rešenje sistema kongruencija, po modulu $n/4$. To znači da možemo odabrati takvo $j_0 \in 4\mathbb{N}+2$.

Zaključujemo da $p \mid \gcd(j_0, n/d_1)$ i $\gcd(j_0-1, n/d_1) = 1$, te je zato $c(j_0, n/d_1) \in 2\mathbb{N}$ i $c(j_0-1, n/d_1) \in 2\mathbb{N}+1$, prema Lemi **??**. Kako je $j_0 \in 4\mathbb{N}+2$ takođe imamo da je $\gcd(j_0-1, n/d_2) \in 2\mathbb{N}+1$ pa je $4 \mid t_{n/d_2, j_0-1}$ odakle sledi da je $c(j_0-1, n/d_2) = \mu(t_{n/d_2, j_0-1}) = 0$. Sa druge strane, na osnovu gornjeg sistema kongruencija imamo da je $\gcd(j_0, n/d_2) = 2$. Odavde je $t_{n/d_2, j_0} = n/2d_2$ i $c(j_0, n/d_2) = 2\mu(n/2d_2) \in 4\mathbb{N}+2$. Osim toga, može se zaključiti da je $c(j_0, n/d_1) - c(j_0-1, n/d_1) \in 2\mathbb{N}+1$ i $c(j_0, n/d_2) - c(j_0-1, n/d_2) = c(j_0, n/d_2) \in 4\mathbb{N}+2$. Konačno, imamo da je

$$\lambda_{j_0} - \lambda_{j_0-1} = c_{d_1}(c(j_0, n/d_1) - c(j_0-1, n/d_1)) + c_{d_2}(c(j_0, n/d_2) - c(j_0-1, n/d_2)) \in 4\mathbb{N}$$

pošto za obe sume važi $c_{d_1}(c(j_0, n/d_1) - c(j_0-1, n/d_1)), c_{d_2}(c(j_0, n/d_2) - c(j_0-1, n/d_2)) \in 4\mathbb{N}+2$, što nas dovodi do kontradikcije.

Neka je sada $d_2 = 1$. Kako $d_1 \notin \{n/4, n/2\}$ i $n \in 8\mathbb{N}+4$, pri čemu nije deljiv kvadratom prostog neparnog broja, to znači da postoji neparan prost broj p takav da $p \nmid d_1$. Neka su $p_2, \ldots, p_k$ svi prosti neparni delioci broja n. Uzmimo sada $0 \leq j_0 \leq n-1$ takvo da je

$$\begin{aligned} j_0 &\equiv 1 \mod p \\ j_0 &\not\equiv 0 \mod p_i \text{ for } 2 \leq i \leq k \text{ such that } p_i \neq p. \end{aligned}$$

Na osnovu Kineske teoreme o ostacima, postoji $0 \leq j_0 \leq n-1$ koje je rešenje gonjeg sistema kongruencija, po modulu $n/4$. Odavde sledi da možemo izabrati $j_0 \in 4\mathbb{N}+2$.

Kako je $\gcd(j_0, n/d_1) \in \{1, 2\}$ i $p \mid \gcd(j_0-1, n/d_1)$, otuda je i $c(j_0, n/d_1) \in 2\mathbb{N}+1$ i $c(j_0-1, n/d_1) \in 2\mathbb{N}$, prema Lemi **??**. Iz činjenice da je $j_0 \in 4\mathbb{N}+2$ zaključujemo da je $\gcd(j_0-1, n) \in 2\mathbb{N}+1$, te zato $4 \mid t_{n, j_0-1}$ odakle sledi da je $c(j_0-1, n) = \mu(t_{n, j_0-1}) = 0$. Sa druge strane, na osnovu uslova datih gornjim sistemom kongruencija imamo da je $\gcd(j_0, n) = 2$. Odavde sledi da je $t_{n, j_0} = n/2$ i $c(j_0, n) = 2\mu(n/2) \in 4\mathbb{N}+2$. Štaviše, zaključujemo da je $c(j_0, n/d_1) - c(j_0-1, n/d_1) \in 2\mathbb{N}+1$ i $c(j_0, n) - c(j_0-1, n) = c(j_0, n) \in 4\mathbb{N}+2$. Konačno, imamo da je

$$\lambda_{j_0} - \lambda_{j_0-1} = c_{d_1}(c(j_0, n/d_1) - c(j_0-1, n/d_1)) + c_{d_2}(c(j_0, n) - c(j_0-1, n)) \in 4\mathbb{N}$$

jer za oba sabirka važi da je $c_{d_1}(c(j_0, n/d_1) - c(j_0 - 1, n/d_1)), c_{d_2}(c(j_0, n) - c(j_0 - 1, n)) \in 4\mathbb{N} + 2$, što nas dovodi do kontradikcije.

Slučaj 2. d_1, d_2 su oba neparni. Odavde sledi da je $d_1, d_2 \in D_2$. Prema (**??**) dobijamo da je

$$\lambda_1 - \lambda_0 = -c_{d_1}\varphi(n/d_1) - c_{d_2}\varphi(n/d_2)$$
$$\lambda_2 - \lambda_1 = 2c_{d_1}\mu(n/2d_1) + 2c_{d_2}\mu(n/2d_2).$$

Kako su oba delicoa d_1 i d_2 različita od $n/4$, tada postoje prosti neparni brojevi p i q koji dele n/d_1 i n/d_2, redom. Odavde sledi da $\varphi(n/d_1), \varphi(n/d_2) \in 4\mathbb{N}$, odakle dalje imamo da je $\lambda_1 - \lambda_0 \in 4\mathbb{N}$. Ako pretpostavimo da su c_{d_1} i c_{d_2} brojevi različite parnosti zaključujemo da je $\lambda_2 - \lambda_1 \in 4\mathbb{N} + 2$, što je kontradikcija sa Teoremom **??**. To znači da su obe težine c_{d_1} i c_{d_2} neparne, pošto bar jedna težina mora biti neparna.

Kako su oba delioca d_1 i d_2 neparna, bez gubljenja opštosti pretpostavimo da je $d_1 > d_2$. Ovo znači da postoji neparan prost broj p takav da $p \mid d_1$. Pošto važi i da je $\gcd(d_1, d_2) = 1$ onda $p \nmid d_2$. Izaberimo $0 \leq j_0 \leq n-1$ takvo da je $j_0 = 2p$. Sada imamo da je $\gcd(j_0, n/d_1) = 2$, odakle je $t_{n/d_1, j_0} = n/2d_1$, što konačno dovodi do $c(j_0, n/d_1) = 2\mu(n/2d_1) \in 4\mathbb{N} + 2$. Sa druge strane možemo zaključiti da je $\gcd(j_0 - 1, n/d_1) \in 2\mathbb{N} + 1$, iz čega sledi da je $t_{n/d_1, j_0 - 1} \in 4\mathbb{N}$, te je $c(j_0 - 1, n/d_1) = \mu(t_{n/d_1, j_0 - 1}) = 0$. Koristeći prethodna razmatranja važi da je

$$c_{d_1}(c(j_0, n/d_1) - c(j_0 - 1, n/d_1)) = 2c_{d_1}\mu(n/2d_1) \in 4\mathbb{N} + 2. \tag{2.54}$$

Takođe, iz $\gcd(j_0, n/d_2) = 2p$ sledi da je $t_{n/d_2, j_0} = n/(2pd_2)$. Odavde dalje sledi da je $c(j_0, n/d_2) = 2(p-1)\mu(n/2pd_2) \in 4\mathbb{N}$. Sa druge strane je $\gcd(j_0 - 1, n/d_2) \in 2\mathbb{N} + 1$, pa je i $t_{n/d_2, j_0 - 1} \in 4\mathbb{N}$, odakle konačno sledi da je $c(j_0 - 1, n/d_2) = \mu(t_{n/d_2, j_0 - 1}) = 0$. Prethodnim razmatranjem dobijamo da je

$$c_{d_2}(c(j_0, n/d_2) - c(j_0 - 1, n/d_2)) = 2c_{d_2}(p-1)\mu(n/2pd_2) \in 4\mathbb{N}. \tag{2.55}$$

Konačno, koristeći (**??**) i (**??**) imamo da je

$$\lambda_{j_0} - \lambda_{j_0 - 1} \in 4\mathbb{N} + 2,$$

što je u kontradikciji sa Teoremom **??**. □

Sada možemo nastaviti sa razmatranjem opšteg slučaja.

Teorema 2.4.5. *Neka je* WICG$(n; C)$ *težinski integralni cirkularni graf takav da je* $c_{n/4} = c_{n/2} = 0$. *Ako postoje delioci* $d_1, d_2 \in D_n$ *takvi da je* $c_{d_1}, c_{d_2} > 0$ *i* $c_d = 0$ *za svako* $d \in D_n \setminus \{d_1, d_2\}$ *onda PST ne postoji u* WICG$(n; C)$.

Dokaz. Pretpostavimo da $8 \mid n/d_i$ ili $p_i^2 \mid n/d_i$ za neke proste delioce p_i od n/d_i, $1 \leq i \leq 2$. Odavde sledi da je $\mu(n/d_i) = \mu(n/2d_i) = 0$, za $1 \leq i \leq 2$, pa je otuda $\lambda_1 = \lambda_2 = 0$ na osnovu Propozicije **??**, (relacije (1.13) i (1.14)). Sada, korišćenjem Posledice **??** tada ne postoji PST u WICG$(n; C)$. Prema tome, može se zaključiti da je bar jedan od delioca d_1 ili d_2 takav da n/d_i nije deljiv kvadratom neparnog prostog broja i $8 \nmid n$. Neka navedenu osobinu ima delilac d_2 i prema njoj ćemo razdvojiti dva slučaja.

Case 1. n/d_2 nije deljiv kvadratom prostog broja. Pretpostavimo da graf WICG$(n; C)$ ima PST. Prema Propoziciji **??** imamo da je

$$\lambda_1 - \lambda_0 = c_{d_1}(\mu(n/d_1) - \varphi(n/d_1)) + c_{d_2}(\pm 1 - \varphi(n/d_2)). \tag{2.56}$$

Kako WICG$(n; C)$ ima PST, korišćenjem Teoreme **??** i Leme **??** važi da je $\lambda_1 - \lambda_0 \in 2\mathbb{N}$.

Pretpostavimo da je $c_{d_2} \in 2\mathbb{N}+1$. Kako $d_2 \neq n/2$ imamo da je $\varphi(n/d_2) \in 2\mathbb{N}$. Iz poslednjeg sledi da je $c_{d_2}(\mu(n/d_2) - \varphi(n/d_2)) \in 2\mathbb{N} + 1$, pa iz činjenice $\lambda_1 - \lambda_0 \in 2\mathbb{N}$ vidimo da je $c_{d_1}(\mu(n/d_1) - \varphi(n/d_1)) \in 2\mathbb{N} + 1$. Poslednja relacija je tačna ako i samo ako $c_{d_1} \in 2\mathbb{N} + 1$ i $\mu(n/d_1) \in 2N + 1$ ($\varphi(n/d_1)$ je parno). To znači da n/d_1 nije deljiv kvadratom prostog broja.

Pretpostavimo da postoji prost delilac p takav da $p^2 \mid n$. Odavde sledi $p \mid d_1$ i $p \mid d_2$, pošto oba broja n/d_1 i n/d_2 nisu deljiva nekim kvadratom prostog broja. Međutim, graf WICG$(n; C)$ je povezan tj. $\gcd(d_1, d_2) = 1$, što je kontradikcija. Ovo znači da n nije deljiv kvadratom prostog broja, pa prema Teoremi **??** nemamo postojanje PST u WICG$(n; C)$.

Pretpostavimo sada da je $c_{d_2} \in 2\mathbb{N}$. Pošto jedna od težina mora biti neparna imamo da je $c_{d_1} \in 2\mathbb{N} + 1$. Kako je $\lambda_1 - \lambda_0 \in 2\mathbb{N}$, $c_{d_2} \in 2\mathbb{N}$ i $c_{d_1} \in 2\mathbb{N} + 1$ zaključujemo da je $\mu(n/d_1) - \varphi(n/d_1) \in 2\mathbb{N}$ tj. $\mu(n/d_1) \in 2\mathbb{N}$. To znači da je n/d_1 deljiv kvadratom nekog prostog broja i $\mu(n/d_1) = 0$. Relacija (**??**) se sada svodi

$$\lambda_1 - \lambda_0 = -c_{d_1}\varphi(n/d_1) + c_{d_2}(\pm 1 - \varphi(n/d_2)). \tag{2.57}$$

Pretpostavimo da $n/2d_1$ nije deljiv kvadratom prostog broja. Korišćenjem uslova da je n/d_1 deljiv kvadratom prostog broja zaključujemo da je $n/d_1 \in 8\mathbb{N}+4$ i nije deljiv kvadratom prostog neparnog broja. Zbog poslednjeg uslova, kao i uslova da n/d_2 nije deljiv kvadratom prostog broja, lako se može pokazati da je $n \in 8\mathbb{N} + 4$ i nije deljiv kvadratom neparnog prostog broja. Međutim, prema Teoremi **??** PST ne postoji u WICG$(n; C)$. Dakle, $n/2d_1$ je deljiv kvadratom prostog broja, pa je $\mu(n/2d_1) = 0$. Takođe, pošto n/d_2 nije deljiv kvadratom prostog broja to je $d_2 \in D_0 \cup D_1$. Odavde sledi da se relacija (**??**) svodi na

$$\lambda_2 - \lambda_1 \;=\; \begin{cases} -2c_{d_2}\mu(n/d_2), & d_2 \in D_1 \\ 0, & d_2 \in D_0 \end{cases}. \tag{2.58}$$

Ukoliko je $d_2 \in D_0$ tada je $\lambda_1 = \lambda_2$, pa na osnovu Posledice **??** nema PST u WICG$(n; C)$, što je kontradikcija. Zato, pretpostavimo da je $d_2 \in D_1$. Iz poslednje relacije imamo da je $S_2(\lambda_2 - \lambda_1) = S_2(c_{d_2}) + 1$, pa na osnovu Teoreme **??** važi $S_2(\lambda_i - \lambda_{i-1}) = S_2(c_{d_2}) + 1$ za svako $1 \leq i \leq n - 1$. Kako je onda $S_2(\lambda_1 - \lambda_0) = S_2(c_{d_2}) + 1$ i $S_2(c_{d_2}(\pm 1 - \varphi(n/d_2))) = S_2(c_{d_2})$ dobija se da za prvi sabirak u (**??**) važi da je $S_2(c_{d_1}\varphi(n/d_1)) = S_2(c_{d_2})$. Iz činjenice da je t $c_{d_1} \in 2\mathbb{N} + 1$ konačno imamo

$$S_2(\varphi(n/d_1)) = S_2(c_{d_2}). \tag{2.59}$$

Neka su $q_1, q_2, \ldots, q_l$ svi neparni prosti delioci broja n/d_2. Kako je $d_2 \neq n/2$ i n/d_2 nije deljiv kvadratom prostog broja važi da je $n/d_2 > 2$ i $l \geq 1$.

Neka je $p \in \{q_1, q_2, \ldots, q_l\}$. Posmatrajmo $0 \leq j_0 \leq n - 1$ takav da je

$$\begin{aligned} j_0 &\equiv 1 \mod p \\ j_0 &\not\equiv 0 \mod q_i \text{ for } 1 \leq i \leq l \text{ takav da je } q_i \neq p. \end{aligned} \tag{2.60}$$

Na osnovu Kineske teoreme o ostacima sledi da ovakvo j_0 zaista postoji i predstavlja jedinstveno rešenje sistema po modulu n/d_2. Takođe, kako je $\gcd(j_0, n/d_2) = 1$ i $p \mid \gcd(j_0 - 1, n/d_2)$ dobijamo da je $c(j_0, n/d_2) \in 2\mathbb{N} + 1$ i $c(j_0 - 1, n/d_2) \in 2\mathbb{N}$, prema Lemi **??**.

Pretpostavimo takođe da postoji neparan prost broj r_0 takav da $r_0^2 \mid n/d_1$. Ako je $r_0 \neq p$ gornjem sistemu kongruencija (**??**) možemo pridodati uslov $j_0 \not\equiv \{0,1\} \mod r_0$ i na taj način dobiti da oba broja $\gcd(j_0, n/d_1)$ i $\gcd(j_0-1, n/d_1)$ nisu deljiva sa r_0. Ovo dalje znači da je $r_0^2 \mid t_{n/d_1,j_0}$ i $r_0^2 \mid t_{n/d_1,j_0-1}$, odakle sledi da je $c(j_0, n/d_1) = \mu(t_{n/d_1,j_0}) = 0$ i $c(j_0-1, n/d_1) = \mu(t_{n/d_1,j_0-1}) = 0$. Konačno imamo da je

$$S_2(\lambda_{j_0} - \lambda_{j_0-1}) = S_2(c_{d_2}(c(j_0, n/d_2) - c(j_0-1, n/d_2))) = S_2(c_{d_2}) < S_2(c_{d_2}) + 1,$$

što je kontradikcija.

Ako je $r_0 = p$ možemo naći takvo $0 \leq j_0 \leq n-1$ koje predstavlja rešenje sledećeg sistema kongruencija

$$\begin{aligned} j_0 &\equiv p+1 \mod p^2 \\ j_0 &\not\equiv 0 \mod q_i \text{ za svako } 1 \leq i \leq l \text{ takvo da je } q_i \neq p. \end{aligned} \tag{2.61}$$

Iz prve relacije sistema se vidi da je $j_0 \equiv 1 \mod p$, te zato kao i u prethodnom slučaju zaključujemo da je $c(j_0, n/d_2) \in 2\mathbb{N}+1$ i $c(j_0-1, n/d_2) \in 2\mathbb{N}$, prema Lemi **??**. Kako $p \nmid \gcd(j_0, n/d_1)$, to imamo $p^2 \mid t_{n/d_1,j_0}$. Odavde sledi da je $c(j_0, n/d_1) = \mu(t_{n/d_1,j_0}) = 0$. Ako bi $t_{n/d_1,j_0-1}$ bio deljiv kvadratom nekog prostog broja, imali bi da je $c(j_0-1, n/d_1) = 0$, pa na osnovu prethodnog slučaja dobijamo da je $S_2(\lambda_{j_0} - \lambda_{j_0-1}) < S_2(c_{d_2}) + 1$.

Pretpostavimo sada da $t_{n/d_1,j_0-1}$ nije deljiv kvadratom prostog broja. Kako je $S_p(j_0 - 1) = 1$, dolazimo do zaključka da je takođe $S_p(\gcd(j_0-1, n/d_1)) = 1$. Kako $p^2 \mid n/d_1$ važi da $p \mid t_{n/d_1,j_0-1}$. Odavde sledi da $p-1 \nmid \varphi(n/d_1)/\varphi(t_{n/d_1,j_0-1})$, a pošto $p-1 \mid \varphi(n/d_1)$ zaključujemo da $S_2(c(j_0-1, n/d_1)) < S_2(\varphi(n/d_1))$. Na osnovu relacije (**??**) dobijamo da je $S_2(c(j_0-1, n/d_1)) < S_2(c_{d_2})$.

Iz gornje diskusije zaključujemo da je $S_2(c_{d_2}(c(j_0, n/d_2) - c(j_0-1, n/d_2))) = S_2(c_{d_2})$. Štaviše, iz $S_2(c_{d_1} c(j_0-1, n/d_1)) < S_2(c_{d_2})$ konačno dobijamo da je

$$S_2(\lambda_{j_0} - \lambda_{j_0-1}) < S_2(c_{d_2})$$

što je čigledno kontradikcija.

Ako ne postoji neparan prost broj r_0 takav da $r_0^2 \mid n/d_1$ tada je $n = 2^\alpha M$ gde je $\alpha \geq 3$ i M neparan broj koji nije deljiv kvadratom prostog broja. Zaista, pretpostavimo da poslednji zaključak nije tačan. To znači da postoji prost neparan broj p takav da je $S_p(n) \geq 2$ ili $0 \leq S_2(n) \leq 1$. Pretpostavimo najpre da je $p^2 \mid n$. Kako $p^2 \nmid n/d_1$ važi da $p \mid d_1$. Sa druge strane, imamo da $p \mid d_2$ pošto n/d_2 nije deljiv kvadratom prostog broja. Iz poslednjeg zaključka dalje proizilazi da $p \mid \gcd(d_1, d_2)$, što je kontradikcija jer je $\mathrm{WICG}(n; C)$ povezan. Sada, pretpostavimo da je $0 \leq S_2(n) \leq 1$. To znači da je n nije deljiv kvadratom ni kojim kvadratom prostog broja ili je $n \in 8\mathbb{N}+4$ i nije deljiv kvadratom prostog neparnog broja. Ali u ovim slučajevima imamo da PST ne postoji u $\mathrm{WICG}(n; C)$.

Izaberimo $0 \leq j_0 \leq n-1$ takvo da je rešenje sistema kongruencija (**??**) i $j_0 \equiv 2 \mod 4$. Kao i u prethodnom slučaju, imamo da je $c(j_0, n/d_2) \in 2\mathbb{N}+1$ i $c(j_0-1, n/d_2) \in 2\mathbb{N}$. Takođe, kako je $j_0 - 1 \in 2\mathbb{N}+1$ imamo da je $\gcd(j_0-1, n/d_1) \in 2\mathbb{N}+1$, pa je zato $2^\alpha \mid t_{n/d_1,j_0-1}$. Iz uslova $\alpha \geq 3$ imamo da važi da je $c(j_0-1, n/d_1) = \mu(t_{n/d_1,j_0-1}) = 0$. Dalje, kako je $j_0 \in 4\mathbb{N}+2$ može se zaključiti da je $\gcd(j_0, n/d_1) \in 4\mathbb{N}+2$ i $2^{\alpha-1} \mid t_{n/d_1,j_0}$. Korišćenjem uslova da je $\alpha \geq 3$ dobijamo da je $c(j_0, n/d_1) = \mu(t_{n/d_1,j_0}) = 0$. Sada, kao i u prethodnom slučaju imamo da je

$$S_2(\lambda_{j_0} - \lambda_{j_0-1}) = S_2(c_{d_2}(c(j_0, n/d_2) - c(j_0-1, n/d_2))) = S_2(c_{d_2}) < S_2(c_{d_2}) + 1$$

.

Case 2. $n/d_2 \in 8\mathbb{N}+4$ i nije deljiv kvadratom neparnog prostog broja. Pošto je $\mu(n/d_2)=0$ onda je prema Propoziciji **??**

$$\lambda_1-\lambda_0 = c_{d_1}(\mu(n/d_1)-\varphi(n/d_1)) - c_{d_2}\varphi(n/d_2).$$

Ako n/d_1 nije deljiv kvadratom prostog broja, onda za svaki neparni prost delilac p od n takav da je $S_p(n)\geq 2$ imamo da p deli oba delioca d_1 i d_2, što je nemoguće jer je $\gcd(d_1,d_2)=1$. Slično, zaključujemo da je $S_2(n)=2$. Znači, n nije deljiv kvadratom prostog neparnog broja odakle prema Teoremi (**??**) proizilazi da ne postoji PST u WICG$(n;C)$. Dakle, n/d_1 mora biti deljiv kvadratom prostog broja, odakle sledi da je

$$\lambda_1-\lambda_0 = -c_{d_1}\varphi(n/d_1) - c_{d_2}\varphi(n/d_2).$$

Primetimo da je $d_2\in D_2$. Ako je $d_1\in D_1$, onda postoji neparan prost broj p takav da $p^2 \mid n/d_1$. To znači da je $\mu(n/2d_1)=0$. Ako je $d_1\in D_2$ tada je $n/2d_1$ nije deljiv kvadratom prostog broja ako i samo ako $8\nmid n/d_1$ i n/d_1 nije deljiv kvadratom prostog neparnog broja. A ako je poslednji iskaz tačan, iz činjenice da je $\gcd(d_1,d_2)=1$ zaključujemo da je $n\in 8\mathbb{N}+4$ i nije deljiv kvadratom prostog neparnog broja. Na osnovu Teoreme **??** ne postoji PST u WICG$(n;C)$. Na taj način, možemo pretpostaviti da $n/2d_1$ deljiv kvadratom prostog broja. Iz prethodnog razmatranja relacija (**??**) se svodi na

$$\lambda_2-\lambda_1 = 2c_{d_2}\mu(n/2d_2).$$

Iz poslednje relacije imamo da je $S_2(\lambda_2-\lambda_1)=S_2(c_{d_2})+1$, pa na osnovu Teoreme **??** važi da je $S_2(\lambda_j-\lambda_{j-1})=S_2(c_{d_2})+1$ za svako $1\leq j\leq n-1$. Posmatrajmo uslov $S_2(\lambda_1-\lambda_0)=S_2(c_{d_2})+1$. Kako $n/d_2\in 8\mathbb{N}+4$ i nije deljiv kvadratom neparnog prostog broja, to postoji neparan prost broj p takav da $p\mid n/d_2$, jer $d_2\neq n/4$. Odavde sledi da $\varphi(4p)\mid\varphi(n/d_2)$, odakle je $\varphi(n/d_2)\in 4\mathbb{N}$. Ovo dalje implicira da je $S_2(c_{d_2}\varphi(n/d_2))\geq S_2(c_{d_2})+2$ te je zato $S_2(c_{d_1}\varphi(n/d_1))=S_2(c_{d_2})+1$. Iz činjenice da je $d_1\neq n/2$ zaključujemo da je $\varphi(n/d_1)\in 2\mathbb{N}$ odakle proizilazi

$$S_2(c_{d_1})+1\leq S_2(c_{d_1}\varphi(n/d_1)) = S_2(c_{d_2})+1.$$

Kako je bar jedan od koeficijenata c_{d_1} ili c_{d_2} neparan, zaključujemo da je $c_{d_1}\in 2\mathbb{N}+1$. Osim toga, odavde sledi

$$S_2(\varphi(n/d_1)) = S_2(c_{d_2})+1. \tag{2.62}$$

Neka su $r_1,r_2,\dots r_s$ svi neparni prosti delioci broja n/d_1 takvih da je $S_{r_i}(n/d_1)\geq 2$. Primetimo da je $s\geq 1$ i neka je $\beta_i = S_{r_i}(n/d_1)$ za svako $1\leq i\leq s$.

Posmatrajmo $0\leq j_0\leq n-1$ takvo da je $j_0 = 2r_1^{\beta_1-1}r_2^{\beta_2-1}\dots r_s^{\beta_s-1}$. Kako je $n/d_2\in 4\mathbb{N}$, koristeći Lemu **??** dobijamo da je $c(j_0,n/d_2)\in 2\mathbb{N}$. Sa druge strane, iz $\gcd(j_0-1,n/d_2)\in 2\mathbb{N}+1$ imamo da je $t_{n/d_2,j_0-1}\in 4\mathbb{N}$, pa je zato $c(j_0-1,n/d_2)=\mu(t_{n/d_2,j_0-1})=0$. Na osnovu ove diskusije možemo zaključiti da je

$$S_2(c_{d_2}(c(j_0,n/d_2)-c(j_0-1,n/d_2)))\geq S_2(c_{d_2})+1. \tag{2.63}$$

Lako se može videti da $r_i\nmid\gcd(j_0-1,n/d_1)$ za svaki $1\leq i\leq s$, te je zato $r_i^2\mid t_{n/d_1,j_0-1}$. Odavde sledi da je $c(j_0-1,n/d_1)=\mu(t_{n/d_1,j_0-1})=0$. Takođe, iz činjenice da $r_1^{\beta_1-1}r_2^{\beta_2-1}\dots r_s^{\beta_s-1}\mid$

$\gcd(j_0, n/d_1)$ zaključujemo da $t_{n/d_1,j_0}$ nije deljiv kvadratom prostog broja i $r_1 r_2 \dots r_s \mid t_{n/d_1,j_0}$. Odavde je

$$S_2(c(j_0, n/d_1)) = S_2(\varphi(n/d_1)) - S_2(\varphi(t_{n/d_1,j_0})) < S_2(\varphi(n/d_1)). \tag{2.64}$$

Sada, na osnovu relacija (**??**) i (**??**) imamo da je

$$S_2(c_{d_1}(c(j_0, n/d_1) - c(j_0 - 1, n/d_1))) = S_2(c(j_0, n/d_1)) < S_2(\varphi(n/d_1)) = S_2(c_{d_2}) + 1. \tag{2.65}$$

Konačno, koristeći (**??**) i (**??**) dobijamo

$$S_2(\lambda_{j_0} - \lambda_{j_0-1}) < S_2(c_{d_2}) + 1$$

što je kontradikcija. □

Iz poslednje teoreme možemo izvesti zaključak da se ivicama grafa $\mathrm{ICG}_n(D)$, gde je $D = \{d_1, d_2\}$ i $d_1 < d_2$, mogu pridružiti težine c_{d_1} i c_{d_2} da bi imao PST ako i samo je n parno i $d_2 \in \{n/4, n/2\}$. To znači da za dati broj $n \in 4\mathbb{N} + 2$ imamo $\tau(n) - 2$ grafova, dok za $n \in 4\mathbb{N}$ imamo $2\tau(n) - 5$ grafova (toliko je broj mogućnosti za d_1 pri fiksiranom $d_2 \in \{n/4, n/2\}$). Primetimo da smo Posledicom **??** u netežinskom slučaju našli samo dva grafa $\mathrm{ICG}_n(D)$ sa dvoelementnim skupom D koji imaju PST za dato n, i to kad je $n \in 8\mathbb{N}$ i $D = \{1, n/2^a\}$, gde je $1 \le a \le 2$. Naime, ako sa $S(G; N)$ označimo broj grafova reda ne većeg od N, zaključujemo da je $S(\mathrm{ICG}_n(D); N) = 2N$, za dato N. Sa druge strane, na osnovu sledeće jednakosti

$$\sum_{n \le N} \tau(n) \sim N \log N.$$

imamo da je $S(W(C; N)) \sim N \log N$.

U Teoremi **??** smo pokazali da ne postoji težinski integralni cirkularni graf neparnog reda koji poseduje svojsto PST. Kombinovanjem ovog rezultata sa Toremom **??** dobijamo jedan od glavnih rezultata ovog poglavlja koji se može formulisati na sledeći način: Za proizvoljno $n \in N$, postoji težinski integralni cirkularni graf reda n koji ima PST ako i samo ako je n parno. Štaviše, ovaj rezultat očigledno uopštava odgovarajući rezultat za netežinske graafove, dat Teoremom **??**. Zaista, u težinskom slučaju delioci $n/4$ i $n/2$ mogu oba biti elementi od D, bez ikakvih dodatnih uslova za ostale delioce iz D. Takođe, red grafa n može biti i iz $4\mathbb{N} + 2$, za razliku od netežinskog slučaja. Korišćenjem ovog rezultata možemo izračunati broj nađenih cirkularnih mreža u kojima postoji PST. Taj broj je jednak broju integralnih cirkularnih grafova takvih da $n/4 \in D$ ili $n/2 \in D$, pri čemu se lako može pokazati da je jednak $3 \cdot 2^{\tau(n)-3}$. Pošto je broj integralnih cirkularnih grafova sa n čvorova najviše jednak broju $2^{\tau(n)-1}$, zaključujemo da je broj integralnih cirkularnih mreža koje imaju PST asimptotski jedna broju integralnih cirkularnih grafova datog reda n.

Teoremom **??** smo pokazali nepostojanje PST u $\mathrm{WICG}(n; C)$ takvim da su dve težine c_{d_1} i c_{d_2} pozitivne, a $c_{n/4} = c_{n/2} = 0$ ($d_1, d_2 \notin \{n/4, n/2\}$). Dokaz zahteva opširna razmatranja sa mnogo slučajeva, pa bi neka nova uopštavanja na ovu temu bila komplikovanija za dokazivanje. Međutim, pronalaženje klasa $\mathrm{WICG}(n; C)$ koji imaju PST takvih da je $c_{n/4} = c_{n/2} = 0$ bi moglo da poveća maksimalno PQCD na ovim mrežama.

Glava 3

Parametri integralnih cirkularnih grafova i primene

U ovoj glavi ćemo opisati pojedine parametre integralnih cirkularnih grafova. Da bi se projektovala cirkularna kvantna mreža koja dopušta kvantnu dinamiku (u prvom redu PST) poželjno je znati što više svojstava integralnih cirkularnih grafova. Tražeći maksimalan put koji informacija može potencijalno da pređe treba ispitati dijametar grafa, pa će ovaj parametar biti tema jedne od sekcija. Takodje, kako red grafa predstavlja broj kubitova u mreži, to znači da ce veliki red proizvesti i otežanu kontrolu mreže. U nastavku glave biće obrađeni parametri poput klike, hromatskog broja, grupe automorfizama integralnih cirkularnih grafova, kao što će biti data i karakterizacija bipartitnih integralnih cirkularnih grafova. Za sve parametara određena je ili eksplicitna formula izračunavanja ili oštra granica. Većina prikazanih rezultata su originalni i bazirani su na na našim radovima [**?**, **?**, **?**, **?**], a ostatak je preuzet iz literature [**?**, **?**].

3.1 Bipartitni integralni cirkularni grafovi

U ovom delu ćemo dati odgovor na pitanje koje osobine moraju zadovoljiti integralni cirkularni grafovi da bi bili bipartitni. Pretostavljamo da red grafa n ima sledeću kanonsku reprezentaciju $2^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$.

Teorema 3.1.1. *Integralni cirkularni graf* $\mathrm{ICG}_n(D)$ *je bipartitan ako i samo ako je* $n \in 2\mathbb{N}$ *i* $2j_0d/n \in 2\mathbb{N}+1$*, za neki prirodan broj* $0 \le j_0 \le n-1$ *i svaki* $d \in D$*.*

Dokaz. Kako je $\mathrm{ICG}_n(D)$ regularan graf sa stepenom regularnosti $k = \sum_{d\in D}\varphi(n/d)$ to je on i bipartitan ako i samo ako postoji sopstvena vrednost $\lambda_{j_0} = -k$.

Pretpostavimo da je $\mathrm{ICG}_n(D)$ bipartitan. Tada postoji $0 \le j_0 \le n-1$ takvo da je

$$\lambda_{j_0} = -k = \sum_{d\in D}\mu(t_{n/d,j_0})\frac{\varphi(n/d)}{\varphi(t_{n/d,j_0})},$$

gde je

$$t_{n/d,j_0} = \frac{n}{d\gcd(n/d,j_0)}.$$

Iz ove jednakosti može se izvesti sledeća nejednakost

$$|\lambda_{j_0}| = k \leq \sum_{d\in D} \varphi(n/d)\frac{|\mu(t_{n/d,j_0})|}{\varphi(t_{n/d,j_0})} = \sum_{d\in D}\varphi(n/d) = k.$$

Dalje zaključujemo da je jednakost zadovoljena ako i samo ako je

$$\frac{\mu(t_{n/d,j_0})}{\varphi(t_{n/d,j_0})} = -1,$$

a poslednje važi ako i samo ako je $\mu(t_{n/d,j_0}) = -1$ i $\varphi(t_{n/d,j_0}) = 1$. Ove dve jednačine po $t_{n/d,j_0}$ su zadovoljene samo za slučaj $t_{n/d,j_0} = 2$. Zapisivanjem poslednje jednakosti u obliku:

$$t_{n/d,j_0} = \frac{n}{d\gcd(n/d, j_0)} = 2.$$

dobijamo da ona važi ako je n parno i mora biti zadovoljeno $S_2(j_0) = S_2(n/d) - 1$ i $S_{p_i}(j_0) \geq S_{p_i}(n/d)$, za proizvoljan neparan broj p_i koji deli n/d. Poslednje činjenice impliciraju da je broj $2j_0$ deljiv brojem n/d za svako $d \in D$, kao i da je taj količnik neparan, čime je tvrđenje ovog dela teoreme dokazano.

Sa druge strane, ukoliko je n paran i $2j_0d/n$ neparan, tada je $S_2(j_0) = S_2(n/d) - 1$ i $S_{p_i}(j_0) \geq S_{p_i}(n/d)$, za proizvoljan $d \in D$ i proizvoljan neparan broj p_i koji deli n/d. Odavde direktno sledi da je $t_{n/d,j_0} = 2$.

Sopstvena vrednost na mestu j_0 je jednaka

$$\lambda_{j_0} = \sum_{d\in D}\varphi(n/d)\frac{\mu(t_{n/d,j_0})}{\varphi(t_{n/d,j_0})} = \sum_{d\in D}\varphi(n/d)\frac{\mu(2)}{\varphi(2)} = -\sum_{d\in D}\varphi(n/d) = -k.$$

Kako je $\lambda_0 = -\lambda_{j_0}$ to je graf $\mathrm{ICG}_n(D)$ bipartitan, čime je teorema dokazana. □

Primećujemo da je poslednjom teoremom data karakterizacija kako povezanih tako i nepovezanih grafova. U nastavku ćemo videti kakavog oblika mora biti indeks j_0 u slučaju povezanih bipartitnih grafova. Najpre ćemo sledećim dvema lemama dati karakterizaciju povezanih integralnih cirkularnih grafova.

Lema 3.1.2. *Integralni cirkularni graf* $\mathrm{ICG}_n(\{d_1, d_2, \ldots, d_t\})$ *je povezan ako i samo ako je* $\gcd(d_1, d_2, \ldots, d_t) = 1$.

Dokaz. Pretpostavimo da je $\gcd(d_1, d_2, \ldots, d_t) = 1$. Tada na osnovu Euklidovog algoritma postoje brojevi $a_1, a_2, \ldots, a_t \in \mathbb{Z}$ takvi da je

$$a_1d_1 + a_2d_2 + \ldots + a_td_t = 1. \tag{3.1}$$

Dokazaćemo da postoji šetnja izmedju proizvoljnih čvorova a i b grafa $\mathrm{ICG}_n(\{d_1, d_2, \ldots, d_t\})$, gde je $a > b$. Neka je $l = a-b$. Na osnovu relacije (**??**) imamo da je $la_1d_1+la_2d_2+\ldots+la_td_t = l$. Ako sa $r_n(a)$ za $a \in \mathbb{Z}$ označimo najmanji nenegativan broj, manji od n, takav da je $r_n(a) \equiv a \bmod n$, tada postoji sledeća šetnja između a i b:

$$\begin{aligned}
&a, r_n(a + d_1), \ldots, r_n(a + la_1d_1),\\
&r_n(a + la_1d_1 + d_2), r_n(a + la_1d_1 + 2d_2), \ldots, r_n(a + la_1d_1 + la_2d_2),\\
&\ldots\\
&r_n(a + la_1d_1 + la_2d_2 + \ldots a_{t-1}d_{t-1} + d_t), r_n(a + la_1d_1 + la_2d_2 + \ldots a_{t-1}d_{t-1} + 2d_t), \ldots, b
\end{aligned}$$

.

Jasno je da između svaka dva čvora u nizu postoji ivica pošto je razlika uzastopnih elemenata niza jednaka d_i za neko $1 \leq i \leq t$.

Pretpostavimo da je graf $\mathrm{ICG}_n(\{d_1, d_2, \ldots, d_t\})$ povezan i da je $\gcd(d_1, d_2, \ldots d_t) = d > 1$. Uočimo podgrafove grafa $\mathrm{ICG}_n(\{d_1, d_2, \ldots, d_t\})$ koji se sastoje od sledećih skupova čvorova

$$H_n(r) = \{h \mid 0 \leq h < n,\ h \equiv r \mod d\}\ \ 0 \leq r \leq d-1. \tag{3.2}$$

Za proizvoljne čvorove $a \in H(r_1)$ i $b \in H(r_2)$, gde je $0 \leq r_1, r_2 \leq d-1$, važi da je $a - b \equiv r_1 - r_2 \mod d$. Kako je $r_1 \neq r_2$ to $d \nmid a - b$, pa čvorovi a i b nisu susedni budući da $\gcd(a-b, n) \notin \{d_1, d_2, \ldots d_t\}$. To znači da ukoliko je $d > 1$, podgrafovi $H_n(r)$ nisu međusobno povezani pa je graf $\mathrm{ICG}_n(\{d_1, d_2, \ldots, d_t\})$ nepovezan. Ovim je dobijena kontradikcija. □

Lema 3.1.3. *Neka su $d_1, d_2, \ldots, d_t$ delioci brojan n, takvi da je $\gcd(d_1, d_2, \ldots, d_t) = d$, tada graf $\mathrm{ICG}_n(\{d_1, d_2, \ldots, d_t\})$ ima tačno d povezanih komponenti koje su izomorfne sa $\mathrm{ICG}_{n/d}(\{d_1/d, d_2/d, \ldots, d_t/d\})$.*

Dokaz. Neka je $D' = \{\frac{d_1}{d}, \frac{d_2}{d}, \ldots, \frac{d_k}{d}\}$. Iz dokaza prethodne teoreme smo videli da pografovi $H_n(0), H_n(1), \ldots, H_n(d-1)$ dati relacijom (**??**) nisu međusobno povezani u $\mathrm{ICG}_n(\{d_1, d_2, \ldots, d_t\})$, pa ostaje da se dokaže da su povezani. Ovo ćemo dokazati konstruisanjem izomorfizma između proizvoljnog podgrafa $H_n(r)$ za $0 \leq r \leq d-1$ i $\mathrm{ICG}_{n/d}(D')$. Na osnovu prethodne leme imamo da je $\mathrm{ICG}_{n/d}(D')$ povezan. Definišimo preslikavanje $f : H_n(r) \to \mathrm{ICG}_{n/d}(D')$ definisano sa $f(r + kd) = k = \lfloor \frac{r+kd}{d} \rfloor$. Preslikavanje f je očigledno bijekcija i na osnovu

$$gcd((r+kd)-(r+ld), n) \in D \text{ ako i samo ako } gcd\left(f(r+kd) - f(r+ld), \frac{n}{d}\right) = gcd\left(k-l, \frac{n}{d}\right) \in D',$$

zaključujemo da je f izomorfizam. □

Neka je graf $\mathrm{ICG}_n(d_1, d_2, \ldots d_t)$ povezan, to jest $\gcd(d_1, d_2, \ldots d_t) = 1$. Iz dokaza Teoreme **??** imamo da je $\mathrm{ICG}_n(d_1, d_2, \ldots d_t)$ bipartitan ako i samo ako postoji $0 \leq j_0 \leq n-1$ tako da je $S_2(j_0) = S_2(n/d_j) - 1$ i $S_{p_i}(j_0) \geq S_{p_i}(n/d_j)$ za svako $1 \leq i \leq k$ i $1 \leq j \leq t$. Kako je $\gcd(d_1, d_2, \ldots d_t) = 1$ to znači da postoji bar jedan neparan delilac d_j. Odavde imamo da je $S_2(n/d_j) = S_2(n)$, zbog čega je $S_2(j_0) = S_2(n) - 1$. Sa druge strane, za proizvoljan neparan prost delilac p_i od n, postoji delilac d_j takav da $p_i \nmid d_j$. U suprotnom bi svi delioci $d_1, d_2, \ldots d_t$ bili deljivi brojem p_i, što je suprotno pretpostavci o povezanosti grafa. Tada je $S_{p_i}(n/d_j) = S_{p_i}(n)$, odakle sledi da je $S_{p_i}(j_0) = S_{p_i}(n)$. Korišćenjem poslednja dva uslova za j_0 imamo da je $j_0 = n/2$. Prema Teoremi **??**, konačno zaključujemo da je povezan $\mathrm{ICG}_n(D)$ bipartitan ako i samo ako je $n \in 2\mathbb{N}$ i $D \subseteq 2\mathbb{N} + 1$.

3.2 Dijametar

U ovoj sekciji ćemo dati donju i gornju granicu za dijametar integralnih cirkularnih grafova, kao i podklase za koje su pomenute granice dostižne. U prethodoj sekciji je data eksplicitna formula za jednu klasu grafova, a ovde je pokazano da je asimptotska ocena dijametra jednaka $O(\ln \ln n)$. Ako je graf G reda n cirkularan jasno je da važi $1 \leq diam(G) \leq n/2$. U ovoj glavi pretostavljamo da red grafa n ima sledeću kanonsku reprezentaciju $2^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Najpre ćemo navesti Henselovu lemu za rešavanje polinomialnih kongruencija koja će biti kasnije korišćena:

Lema 3.2.1. *Neka je $P(x) \in \mathbb{Z}[x]$, p prost broj i $a \in \mathbb{Z}$ rešenje kongruencije $P(x) \equiv 0 \mod p^i$ za prirodan broj i. Ako je $P'(a) \not\equiv 0 \mod p$, tada postoji $b \equiv a \mod p^i$ tako da je $P(b) \equiv 0 \mod p^{i+1}$.*

Teorema 3.2.2. *Za dati integralni cirkularni graf* $\mathrm{ICG}_n(D)$ *važi*

$$t \leq diam(\mathrm{ICG}_n(D)) \leq 2t + 1,$$

gde je t broj elemenata najmanjeg aditivnog generatornog skupa sadržanog u D za $\mathbb{Z}_n$.

Dokaz. Kako t predstavlja veličinu najmanjeg aditivnog generatornog skupa za $\mathbb{Z}_n$ to će za neko $l \in \mathbb{Z}_n$ postojati $k \geq t$ elemenata $d_1, d_2, \ldots d_k \in D$ tako da je $l \equiv d_1 + d_2 + \ldots + d_k \mod n$. Poslednja činjenica direktno implicira da je $t \leq diam(\mathrm{ICG}_n(D))$.

Dokažimo i gornju granicu. Neka $d_1, d_2, \ldots d_t \in D$ predstavlja generatorni skup. Kako je graf povezan, imamo da je $\gcd(d_1, d_2, \ldots, d_t, n) = 1$, pa je i jedan od delilaca neparan. Neka je $d_1 \in 2\mathbb{N} + 1$. Za proizvoljno $l \in \mathbb{Z}_n$ dokazaćemo da postoje $x_0, x_1, \ldots, x_{2t} \in (\mathbb{Z}_n)^*$ za koje važi

$$d_1 x_0 + d_1(x_1 + x_{t+1}) + \ldots + d_t(x_t + x_{2t}) \equiv l \mod n \tag{3.3}$$

ili

$$d_1(x_1 + x_{t+1}) + \ldots + d_t(x_t + x_{2t}) \equiv l \mod n. \tag{3.4}$$

Ovo znači da će za svako $l \in \mathbb{Z}_n$ postojati $2t$ ili $2t + 1$ brojeva $a_1, a_2, \ldots, a_k$, za koje važi $\gcd(a_i, n) \in \{d_1, d_2, \ldots, d_t\}$ i $a_1 + a_2 + \ldots + a_k \equiv l \mod n$, gde je $t \leq k \leq t + 1$.

Ako je n paran tada ćemo uzeti da su svi brojevi $x_0, x_1, \ldots, x_{2t}$ neparni. Ako je l paran tada je zadovoljena relacija (**??**) po modulu 2. U suprotnom imamo da je zadovoljena relacija (**??**) po modulu 2. Koristeći Lemu **??** dobijamo da postoje brojevi $x_0, x_1, \ldots, x_{2t}$ koji zadovoljavaju relacije (**??**) ili (**??**) po modulu 2^{α_1}.

Neka je p_i neparan prost delilac broja n. Kako je $\gcd(d_1, d_2, \ldots, d_t, n) = 1$ pretpostavićemo da $p_i \nmid d_1$ za $2 \leq i \leq k$. Odaberimo $x_0, x_1, \ldots, x_{2t}$ tako da je

$$x_2 \equiv \ldots \equiv x_t \equiv 1 \equiv x_{t+2} \equiv \ldots \equiv -x_{2t} \mod p_i.$$

Tada se relacije **??** svodi na $d_1(x_1 + x_{t+1}) \equiv l \mod p_i$, tj.

$$x_1 + x_{t+1} \equiv l \cdot d_1^{-1} \mod p_i$$

odakle nalazimo $x_1, x_{t+1} \not\equiv 0 \mod p_i$. Dakle, imamo rešenje $x_1, x_2, \ldots, x_{2t}$ po modulu p_i. Koristeći Lemu **??** dobijamo da se može naći rešenje $x_1, x_2, \ldots, x_{2t}$ po modulu $p_i^{\alpha_i}$.

Konačno, na osnovu Kineske teoreme o ostacima dobijamo rešenje $x_0, x_2, \ldots, x_{2t}$ po modulu n. □

Direktna posledice prethodne teoreme je sledeća nejednakost

$$2 \leq diam(\mathrm{ICG}_n(D)) \leq 2|D| + 1. \tag{3.5}$$

Sledeći rezultat pokazuje da je navedena granica dostižna i da uopštem slučaju nije moguća bolja.

Teorema 3.2.3. *Za dijametar integralnog cirkularnog grafa važe sledeća tvrđenja:*

i) Za neparan broj $n = p_1 p_2 \dots p_k$ *gde je* $k \geq 3$ *i* $D = \{p_1, p_2, \dots, p_k\}$ *važi da je* $diam(\mathrm{ICG}_n(D)) = 2$.

ii) Neka je m *proizvod neparanih prostih brojeva,* $n = 2m^2$ *i* $D = \{(m/p_1)^2, (m/p_2)^2, \dots, (m/p_k)^2\}$. *Tada je* $diam(\mathrm{ICG}_n(D)) = 2k + 1$.

Dokaz. *i)* Neka je $n = p_1 p_2 \dots p_k$ i $D = \{p_1, p_2, \dots, p_k\}$. Pokazaćemo da za svako $l \in \mathbb{Z}_n$ postoje $s_1, s_2 \in \mathbb{Z}_n$ tako da je $s_1 + s_2 \equiv l \mod n$ i $\gcd(s_1, n), \gcd(s_2, n) \in D$.

Preptostavimo najpre da je $\gcd(l, n) = 1$ i pronađimo brojeve s_1 i s_2 tako da je $\gcd(s_1, n) = p_1$ i $\gcd(s_2, n) = p_2$. Iz poslednje relacije za s_1 dobijamo sistem kongruencijskih jednačina $s_1 \equiv 0 \mod p_1$ i $s_1 \not\equiv 0 \mod p_i$ za $2 \leq i \leq k$. Slično, za s_2 imamo da je $s_2 \equiv 0 \mod p_2$ i $s_2 \not\equiv 0 \mod p_i$ za $1 \leq i \leq k, i \neq 2$. Kako je $s_1 \equiv l - s_2 \mod n$, objedinjujući prethodne sisteme kongruencijskih jednačina dobijamo sistem po s_1:

$$\begin{aligned} s_1 &\equiv 0 \mod p_1 \\ s_1 &\equiv l \mod p_2 \\ s_1 &\not\equiv 0, l \mod p_i, \text{ za } 3 \leq i \leq k. \end{aligned}$$

Kako su brojevi $p_1, p_2, \dots, p_k$ neparni to za dato l postoji jedinstveno s_1 po modulu $p_1 p_2 \dots p_k$ koje je rešenje datog sistema, na osnovu Kineske teoreme o ostacima.

Neka je sada $\gcd(l, n) \neq 1$ i bez gubljenja opštosti pretpostavimo da $p_1 \mid l$. Slično prethodnom rasuđivanju možemo pronaći brojeve s_1 i s_2 takve da je $\gcd(s_1, n) = p_1$ i $\gcd(s_2, n) = p_1$. Naime gornji sistem kongruencijskih jednačina dobija sledeći oblik:

$$\begin{aligned} s_1 &\equiv 0 \mod p_1 \\ s_1 &\not\equiv 0, l \mod p_i, \text{ za } 2 \leq i \leq k. \end{aligned}$$

Na isti način, koristeći Kinesku teoremu o ostacima dobijamo da sistem ima rešenje po modulu $p_1 p_2 \dots p_k$.

ii) Neka je $m = p_1 p_2 \dots p_k$, $n = 2m^2$ i $D = \{(m/p_1)^2, (m/p_2)^2, \dots, (m/p_k)^2\}$. Pokazaćemo da ne postoje brojevi $s_1, s_2, \dots, s_{2k}$ takvi da je

$$s_1 + s_2 + \ldots + s_{2k} \equiv m \mod n \tag{3.6}$$

i $\gcd(s_i, n) = d_i \in D$ za $1 \leq i \leq 2k$.

Pretpostavimo suprotno, da ovako definisani $s_1, s_2, \dots, s_{2k}$ postoje. Takodje, pretpostavimo da za dato $1 \leq j \leq 2k$ važi da $(m/p_j)^2 \notin \{d_1, d_2, \dots, d_{2k}\}$. To bi značilo da $p_j^2 \mid d_1, d_2, \dots, d_{2k}$, a time i $p_j^2 \mid s_1, s_2, \dots, s_{2k}$ čime konačno dobijamo na osnovu (**??**) da $p_j^2 \mid m$, što je kontradikcija.

Na osnovu prethodnog razmatranja, bez gubljenja ooštosti možemo pretpostaviti da je $d_1 = (m/p_1)^2$, $d_2 = (m/p_2)^2, \dots, d_1 = (m/p_k)^2$. Drugim rečima, postoje $x_1, x_2, \dots, x_{2k} \in \mathbb{Z}_n^*$ gde je $s_i = d_i x_i$ za $1 \leq i \leq 2k$ tako da relacija (**??**) dobija sledeći oblik:

$$\frac{m^2}{p_1^2} x_1 + \ldots + \frac{m^2}{p_k^2} x_k + d_{k+1} x_{k+1} + \ldots + d_{2k} x_{2k} \equiv m \mod n.$$

Ako prethodnu kongruenciju posmatramo po modulu p_1 dobijamo

$$\frac{m^2}{p_1^2} x_1 + d_{k+1} x_{k+1} + \ldots + d_{2k} x_{2k} \equiv m \mod p_1. \tag{3.7}$$

Pretpostavimo da $(m/p_1)^2 \notin \{d_{k+1}, \ldots, d_{2k}\}$. Odavde sledi da $p_1^2 \mid d_{k+1}, \ldots, d_{2k}$, kao i $p_1^2 \mid \frac{m^2}{p_1^2}x_1$ na osnove relacije (**??**). Ovo je kontradikcija budući da je $\gcd(x_1, p_1) = 1$.

Posmatrajući kongruencije po modulima $p_2, \ldots, p_k$ dobijamo da je $(m/p_1)^2, \ldots, (m/p_k)^2 \in \{d_{k+1}, \ldots, d_{2k}\}$. Bez gubljenja opštosti, pretpostavimo da je

$$d_{k+1} = \frac{m^2}{p_1^2}, \ldots, d_{2k} = \frac{m^2}{p_k^2}.$$

Relacija (**??**) se svodi na

$$\frac{m^2}{p_1^2}(x_1 + x_{k+1}) + \ldots + \frac{m^2}{p_k^2}(x_k + x_{2k}) \equiv m \mod n.$$

Kako su brojevi $x_1, \ldots, x_{2k}$ uzajamno prosti sa n, oni su neparni, pa je leva strana prethodne relacije parna. Ovo je kontradikcija, pošto je m neparan broj.

Zaključujemo da ne postoje $s_1, \ldots, s_{2k}$ tako da je $s_1+s_2+\ldots+s_{2k} \equiv m \mod n$ i $\gcd(s_i, n) = d_i \in D$ za $1 \leq i \leq 2k$, odakle sledi da je $diam(\mathrm{ICG}_n(D)) > 2k$. Kako na osnovu (**??**) važi i $diam(\mathrm{ICG}_n(D)) \leq 2k + 1$, dobijamo da je $diam(\mathrm{ICG}_n(D)) = 2k + 1$. □

Neka je $\{d_1, d_2, \ldots, d_t\} \subseteq D$ najmanji generatorni skup sadržan u D. Kako je $1 \in \mathbb{Z}_n$ linearna kombinacija delioca generatornog skupa to važi da je

$$\gcd(n, d_1, d_2, \ldots, d_t) = 1.$$

Takođe, neka $\omega(n)$ predstavlja broj različitih prostih delioca broja n. Kako je skup $\{d_1, d_2, \ldots, d_t\}$ najmanji to za svako $1 \leq s \leq t$ važi i da je

$$\gcd(n, d_1, d_2, \ldots, d_{s-1}, d_{s+1}, \ldots, d_t) > 1.$$

Odavde proizilazi da za svaki s postoji prost delilac p_s od n takav da $p_s \nmid d_s$ i $p_s \mid d_i$ za svako $i \neq s$. Zato, možemo definisati preslikavanje $\alpha : \{d_1, d_2, \ldots, d_t\} \to \{p_1, p_2, \ldots, p_{\omega(n)}\}$ takvo da je $\alpha(d_s) = p_s$. Kako važi da je $p_{s_1} \neq p_{s_2}$, ako je $d_{s_1} \neq d_{s_2}$, to odavde zaključujemo da je preslikavanje α injekcija i $t \leq \omega(n)$. Ovim dokazujemo na osnovu Teoreme **??** sledeću posledicu:

Posledica 3.2.4. *Za proizvoljan integralni cirkularni graf* $\mathrm{ICG}_n(D)$ *važi da je* $diam(\mathrm{ICG}_n(D)) \leq 2\omega(n) + 1$.

Kako za $\omega(n)$ važi sledeća procena

$$\omega(n) \approx \ln\ln n + B_1 + \sum_{k=1}^{\infty}(-1 + \sum_{j=0}^{k-1}\frac{\gamma_j}{j!})\frac{(k-1)!}{(\ln n)^k}$$

gde je B_1 *Mertensova konstanta* i γ_j *Stiltjesova konstanta* ([**?**, **?**, **?**, **?**]) to dobijmao sledeću posledicu

Posledica 3.2.5. *Za proizvoljan integralni cirkularni graf* $\mathrm{ICG}_n(D)$ *važi da je* $diam(\mathrm{ICG}_n(D)) = O(\ln\ln n)$.

Takođe važi sledeće poboljšanje gornje granice nejednakosti (**??**).

Teorema 3.2.6. *Neka je* $\{d_1, d_2, \ldots, d_t\} \subseteq D$ *najmanji aditivni generatorni skup za* $\mathbb{Z}_n$. *Ako je* n/d_i *neparan broj za svako* $1 \leq i \leq t$, *tada je* $diam(\mathrm{ICG}_n(D)) \leq 2t$.

Dokaz. Neka je

$$H_n(d_i) = \{h \in \mathbb{Z}_n \mid h \equiv 0 \mod d_i\}.$$

za proizvoljno $1 \leq i \leq t$ i $0 \leq j \leq n-1$. Takođe, neka je $j + H_n(d_i)$ podgraf od $\mathrm{ICG}_n(D)$ takav da je skup čvorova $j + h$, gde je $h \in H_n(d_i)$ i dva čvora $j + h'$ i $j + h''$ su susedna ako je $h'' - h' \in G_n(d_i)$. Dokazaćemo da je dijametar podgrafa $j + H_n(d_i)$ najviše dva.

Neka su $j + h_1$ i $j + h_2$ dva nesusedna čvora u podgrafu $j + H_n(d_i)$. Kako je $h_1, h_2 \in H_n(d_i)$ to jest $h_1 = d_i g_1$ i $h_2 = d_i g_2$ to je dovoljno pronaći brojeve $f', f'' \in \mathbb{Z}^*_{n/d}$ takve da je

$$h_1 - h_2 \equiv d_i f' + d_i f'' \mod n.$$

Neka je $n/d_i = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ kanonska faktorizacija broja n/d_i. Kako su brojevi n/d_i neparni i time $p_j > 2$ za $1 \leq j \leq m$, to se uslovi $\gcd(f', n/d_i) = 1$ i $\gcd(f'', n/d_i) = 1$ mogu zapisati sistemom kongruencija:

$$f' \not\equiv 0, g_2 - g_1 \mod p_j$$

za $1 \leq j \leq m$. Pretpostavka $p_j > 2$ garantuje egzistenciju rešenja na osnovu Kineske teoreme o ostacima. Iz poslednjeg zaključujemo da je dijametar podgrafa $j + H_n(d_i)$ najviše dva.

Neka su u i v dva proizvpljna čvora u $\mathrm{ICG}_n(D)$. Kako je $\{d_1, d_2, \dots, d_t\}$ generatorni skup u $\mathbb{Z}_n$ to postoje koeficijenti $\alpha_1, \alpha_2, \dots, \alpha_t \in \mathbb{Z}_n$ takvi da je

$$v - u \equiv \alpha_1 d_1 + \alpha_2 d_2 + \dots \alpha_t d_t \mod n.$$

Tada se šetnja W od čvora u do v sastoji iz sledećih delova:

- put od u do $u + \alpha_1 d_1$ ivicama grafa $u + H_n(d_1)$.
- put od $u + \alpha_1 d_1$ do $u + \alpha_1 d_1 + \alpha_2 d_2$ ivicama grafa $(u + \alpha_1 d_1) + H_n(d_1)$.
- ...
- put od $u + \sum_{i=1}^{t-1} \alpha_i d_i$ do $u + \sum_{i=1}^{t} \alpha_i d_i = v$ ivicam čvora $(u + \sum_{i=1}^{t-1} \alpha_i d_i) + H_n(d_t)$.

Kako svako parče puta ima dužinu najviše dva, to će rastojanje između čvorova u i v biti najviše $2t$. □

3.3 Klika sa najvećim brojem čvorova

Klika datog grafa $G = (V, E)$ predstavlja podskup skupa čvorova $C \subseteq V$, takav da za svaka dva čvora u C, postoji ivica koja ih spaja [**?**]. Drugim rečima, podgraf indukovan skupom čvorova C je kompletan. Problem nalaženja veličine klike sa najvećom kardinalnošću skupa C je NP-kompletan problem [**?**]. Takođe, neki autori pod klikom upravo podrazumevaju maksimalan kompletan graf [**?**]. Za graf $G = (V, E)$ sa $\omega(G)$ označićemo kliku sa najvećim brojem čvorova.

Pojam koji je blizak pojmu klike je hromatski broj. Hromatski broj grafa G predstavlja najmanji broj boja $\chi(G)$ potrebnih za bojenje skupa čvorova grafa G tako da dva susedna čvora ne mogu biti obojena istom bojom [**?**]. Takođe se kaže da je to najmanji broj k, takav da je graf G k-obojiv. Iz definicija parametara $\omega(G)$ i $\chi(G)$ imamo da je $\omega(G) \leq \chi(G)$. Definišimo i pojam komplementarnog ili inverznog grafa garafu G. To je graf H koji ima isti skup čvorova kao i graf G takvih da su dva čora u H susedna ako i samo ako su u G nesusedna. Tada graf H označavamo sa $\overline{G}$. Takođe, svaku kliku grafa $\overline{G}$ nazivamo nezavisnim skupom u G.

U ovoj sekciji ćemo izračunati veličinu maksimalne klike $\omega(\mathrm{ICG}_n(D))$, gde se skup D sastoji od jednog ili dva delioca. Ovaj rezultat potvrđuje hipotezu iznetu u [**?**] da parametar $\omega(\mathrm{ICG}_n(D))$ deli red grafa n. Međutim, u nastavku ćemo konstruisati familiju grafova $\mathrm{ICG}_n(D)$ takvih da je $|D| \geq 3$ za koje ne važi pomenuta hipoteza. Na kraju ćemo dati gornju i donju granicu za veličinu najveće klike integralnih cirkularnih grafova.

Takođe pretpostavićemo da za dati graf $\mathrm{ICG}_n(D)$ važi da je $D = \{d_1, d_2, \ldots, d_t\}$, kao i da broj n ima kanonsku reprezentaciju $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, gde je $p_1 < p_2 < \ldots < p_k$ i $\alpha_i \geq 1$. Takođe sa $f(n)$ označimo najmanji prost delilac od n. Za unitarne Kejlijeve grafove važi sledeće tvrđenje

Teorema 3.3.1. *Ako je $D = \{1\}$ i $X_n = \mathrm{ICG}_n(D)$ tada je*

$$\chi(X_n) = \omega(X_n) = f(n), \quad \chi(\overline{X_n}) = \omega(\overline{X_n}) = \frac{n}{f(n)}. \tag{3.8}$$

Dokaz. Neka je $p = f(n)$. Kako čvorovi $\{0, 1, \ldots, p-1\}$ indukuju kliku u X_n imamo da je $\chi(X_n) \geq \omega(X_n) \geq p$. Sa druge strane, podgrafovi indukovani skupovima čvorova

$$G_n(r) = \{a \mid 0 \leq a < n,\ h \equiv r \mod p\} \quad 0 \leq r \leq p-1.$$

čine nezavisne skupove. Zaista, za proizvoljne čvorove $a, b \in G_n(r)$ važi $p \mid a - b$, pa je $\gcd(a - b, n) \geq p > 1$, odakle dobijamo da a i b nisu susedi. Ako se svi čvorovi u podgrafovu $G_n(r)$ oboje istom bojom, a svaki od podgrafova $G_n(0), G_n(1), \ldots, G_n(p-1)$ međusobno različitim bojama, dobijamo da je graf X_n p-obojiv. Odavde imamo da je $\chi(X_n) \leq p$, čime je dokazana prva jednakost za X_n.

Slično, uzimajući indukovane podgrafove $G_n(r) = \{a \mid 0 \leq a < n/p,\ h \equiv r \mod n/p\}$ $0 \leq r \leq n/p - 1$ po modulu n/p dobijamo da su nezavisni skupovi u X_n, to jest klike u $\overline{X_n}$, pa je $\chi(\overline{X_n}) \geq \omega(\overline{X_n}) \geq \frac{n}{p}$.

Takođe čvorovi $H_n(r) = \{a \mid kp \leq a < (k+1)p - 1\}$ $0 \leq k \leq n/p - 1$ čine nezavisan skup u $\overline{X_n}$. Zaista, za $a, b \in H_n(r)$ važi da je $|a - b| \leq p - 1$, odakle sledi da je $\gcd(a - b, n) = 1$. Dakle, proizvoljna dva čvora u $H_n(r)$ su susedni pa je ovaj podgraf klika u X_n, to jest nezavisni skup u $\overline{X_n}$. To znači da je graf $\overline{X_n}$ n/p-obojiv pa je i $\chi(\overline{X_n}) \leq n/p$, što dokazuje jednakost u (**??**) za $\overline{X_n}$. □

Razmotrimo slučaj kada se skup D sastoji od jednog delioca tj. $D = \{d\}$, gde je $d \geqslant 1$ proizvoljan delilac od n. Na osnovu Leme **??**, $\mathrm{ICG}_n(d)$ ima d povezanih komponenti - klase ostataka po modulu d in $Z_n = \{0, 1, 2, \ldots, n-1\}$.

Posledica 3.3.2. *Za integralni cirkularni graf $X_n(d) = \mathrm{ICG}_n(d)$ važi da je:*

$$\chi(X_n(d)) = \omega(X_n(d)) = f\left(\frac{n}{d}\right) \quad \chi(\overline{X_n(d)}) = \omega(\overline{X_n(d)}) = \frac{n}{df(n/d)}$$

Dokaz.

Podgrafovi $H_n(r)$ definisani relacijom (**??**) predstavljaju povezane komponente u $X_n(d)$ izomorfne sa $\mathrm{ICG}_{n/d}(1)$, na osnovu Leme **??**. To znači da su parametri ω i χ grafova $X_n(d)$ i $\overline{X_n(d)}$ jednaki istim parametrima grafova $\mathrm{ICG}_{n/d}(1)$ i $\overline{\mathrm{ICG}_{n/d}(1)}$, redom. Konačno, direktnom primenom Teoreme **??** važi tvrđenje. □

3.3.1 Veličina maksimalne klike za $t = 2$

Neka je D dvoelementni skup $D = \{d_1, d_2\}$, gde je $d_1 > d_2$. Neka je Q skup svih prostih delioca broja n koji ne dele d. Glavni rezultat ove sekcije je sledeća teorema.

Teorema 3.3.3. *Za graf* $\mathrm{ICG}_n(d_1, d_2)$ *važi:*

$$\omega\left(\mathrm{ICG}_n(d_1,d_2)\right) = \begin{cases} \min\left(\min_{p\in Q} p, f(n)\cdot f\left(\frac{n}{d_1}\right)\right), & \text{if } d_2 = 1, \\ \omega(X_{\frac{n}{d_2}}(1, \frac{d_1}{d_2})), & \text{if } d_2 \mid d_1 \text{ i } d_2 > 1, \\ \max\left(f\left(\frac{n}{d_1}\right), f\left(\frac{n}{d_2}\right)\right), & \text{u suprotnom.} \end{cases}$$

U cilju jasnijeg izlaganja, dokaz ove teoreme biće podeljen u dva slučaja i nekoliko teorema.

Na osnovu definicije integralnih cirkularnih grafova, skup ivica grafa $\mathrm{ICG}_n(d_1, d_2)$ predstavlja uniju skupova ivica grahova $\mathrm{ICG}_n(d_1)$ i $\mathrm{ICG}_n(d_2)$. Obojimo ivice grafa $\mathrm{ICG}_n(d_1, d_2)$ dvema bojama: ivica $\{a, b\}$ je plava ako $gcd(a-b, n) = d_1$ i crvena ako $gcd(a-b, n) = d_2$. Zato na osnovu Posledice **??** imamo

$$\omega\left(\mathrm{ICG}_n(d_1,d_2)\right) \geq \max\left(f\left(\frac{n}{d_1}\right), f\left(\frac{n}{d_2}\right)\right). \tag{3.9}$$

Slučaj 1: $1 \in D$

Pretpostavimo da je $D = \{1, d\}$, gde je $d = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$. Neka je i prvi najmanji indeks takav da je $\beta_i < \alpha_i$, to jest $f(\frac{n}{d}) = p_i$. Na osnovu (**??**), znamo da je $\omega(\mathrm{ICG}_n(1, d)) \geq p_i$.

Lema 3.3.4. *Za graf* $\mathrm{ICG}_n(1, d)$ *važi*

$$\omega(\mathrm{ICG}_n(1,d)) \leq f(n)\cdot f\left(\frac{n}{d}\right).$$

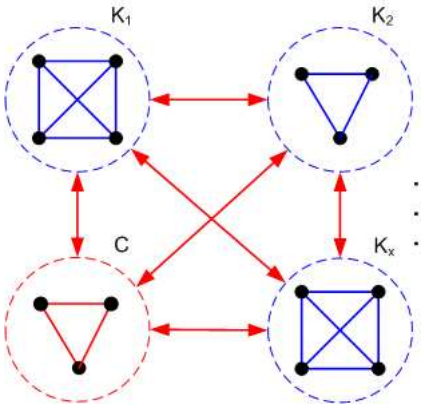
Dokaz. Obojimo ivice grafa $\mathrm{ICG}_n(1, d)$ dvema bojama. Neka su plave ivice one za koje važi da je $gcd(a-b, n) = d$, a neka za crvene važi da je $gcd(a-b, n) = 1$. Ako su dve incidentne ivice (a, b) i (a, c) plave, tada je ivica koja spaja čvorove b i c takođe plava, ukoliko takva ivica postoji. Poslednje zaključujemo iz činjenice da ako $d \mid a-b$ i $d \mid a-c$, tada d deli $gcd(b-c, n)$. To znači da za bilo koje dve klike čije su ivice plave nemaju zajedničkih čvorova. Neka su dalje $K_1, K_2, \ldots, K_x$ klike sa maksimalnim brojem čvorova sa plavim ivicama sadržane u maksimalnoj kliki C^* iz $\mathrm{ICG}_n(1, d)$. Jasno je da bilo koja dva susedna čvora u različitim klikama K_i i K_j čine ivicu crvene boje. Štaviše, proizvoljni čvor iz $V(C^*) \setminus (V(K_1) \cup V(K_2) \cup \ldots \cup V(K_x))$ ne pripada ni jednoj plavoj kliki, odakle sledi da čvorovi $V(C^*) \setminus (V(K_1) \cup V(K_2) \cup \ldots \cup V(K_x))$ indukuju kliku C sastavljenu samo od crvenih ivica. Po Posledici **??**, red klika K_i ($i \in \{1, 2, \ldots, x\}$) je najviše $p_i = f(\frac{n}{d})$ i red klike C je manji ili jednak p_1.

Neka y predstavlja red klike C. Ako izaberemo po jedan čvor iz svake klike K_i, tada ovih x čvorova zajedno sa y čvorova klike C formiraju kliku sa crvenim ivicama u grafu $\mathrm{ICG}_n(1, d)$. Zato važi $x + y \leqslant p_1$. Konačno je broj čvorova maksimalne klike C^* iz $\mathrm{ICG}_n(1, d)$

$$\sum_{j=1}^{x} |K_j| + |C| \leq x \cdot p_i + y = x \cdot (p_i - 1) + (x + y) \leq p_1 \cdot (p_i - 1) + p_1 = p_i \cdot p_1,$$

odakle imamo da je red od C^* manji ili jednak $f(n) \cdot f(\frac{n}{d})$. □

Neka je R skup svih prostih delioca koji dele d i $\frac{n}{d}$. Sa q označimo najmanji prost broj iz Q, ukoliko takav postoji. I neka je M proizvod svih brojeva iz $R \cup Q$.



Slika 3.1: *Maksimalna klika u grafu* $\mathrm{ICG}_n(1,d)$

Lema 3.3.5. *Za porizvoljan delilac d broja n, važi sledeća nejednakost:*

$$\omega(\mathrm{ICG}_n(1,d)) \leq \min_{p\in Q} p = q.$$

Dokaz. Neka je p proizvoljan broj iz Q. Ako pretpostavimo da maksimalna klika sadrži više od p čvorova, onda postoje dva čvora a i b sa istim ostatkom po modulu p. To znači da je $gcd(a-b,n)$ deljivo sa p, i zato ne može biti jednak ni 1 ni d. Poslednje dovodi do kontradikcije, pa je $\omega(X_n(1,d)) \leq p$. □

Teorema 3.3.6. *Ako je Q prazan skup ili $q > p_1 \cdot p_i$, onda*

$$\omega(\mathrm{ICG}_n(1,d)) = p_1 \cdot p_i.$$

Dokaz. Koristeći Lemu **??** dovoljno je konstruisati kliku veličine $p_1 \cdot p_i$ sa čvorovima oblika $x_{rs} = a_s \cdot d + r$, gde je $0 \leq s < p_i$ i $0 \leq r < p_1$. Izaberimo brojeve a_s kao rešenje sledećeg sistema kongruencija:

$$\begin{aligned} a_s &\equiv s && \mod p && \text{za svaki } p \in R \\ a_s \cdot d &\equiv s \cdot p_1 && \mod p && \text{za svaki } p \in Q. \end{aligned}$$

Ovaj sistem ima rešenje ako i samo ako je $gcd(d,p) \mid s \cdot p_1$ za svaki $p \in Q$. Poslednje je trivijalno zadovoljeno budući da su d i $p \in Q$ uzajamno prosti. Konačno, korišćenjem Kineske teoreme o ostacima možemo jedinstveno odrediti brojeve a_s po modulu M.

Posmatrajmo sada proizvoljnu razliku $\Delta = x_{rs} - x_{r's'} = d\cdot(a_s - a_{s'}) + (r - r')$. Pretpostavimo najpre da je $r \neq r'$. Za svaki prost delilac p od d (a time i za svaki prost delilac iz R), broj Δ ne može biti deljiv sa p jer je $0 < |r - r'| < p_1$. Ukoliko je $p \in Q$, imamo da je $x_{rs} - x_{r's'} \equiv (s - s')\cdot p_1 + (r - r') \mod p$. Ostatak $|(s - s')\cdot p_1 + (r - r')| \leq (p_i - 1)\cdot p_1 + (p_1 - 1) < p_i \cdot p_1 < q$ je manji od p i različit od nule - što znači da je najveći zajednički delilac brojeva Δ i n jednak 1.

Neka je sada $r = r'$. Tada za proizvoljni prost broj $p \in Q$, imamo da je $(s - s')\cdot p_1$ ostatak od Δ pri deljenju sa p, što je različito od 0. Zaista, važi da je $s \neq s'$ i $|(s - s')\cdot p_1| < p_i \cdot p_1 < q \leq p$. Kada je p element iz R, imamo da razlika $a_s - a_{s'} \equiv s - s' \mod p$ ne može biti deljiva sa p jer važi $0 < |s - s'| < p_i \leq p$. To dalje znači da je $gcd(\Delta/d, n/d) = 1$, to jest $gcd(\Delta, n) = d$.

Poslenjim smo dokazali da je najveći zajednički delilac brojeva Δ i n jednak 1 ili d, čime je dokaz završen.

Ako je Q prazan skup, možemo iskoristiti istu konstrukciju da bi dobili kliku veličine $p_1 \cdot p_i$. □

Teorema 3.3.7. *Ako je $q < p_1 \cdot p_i$, onda važi*

$$\omega(\mathrm{ICG}_n(1,d)) = q.$$

Dokaz. Na osnovu Leme **??** dovoljno je naći kliku sa q čvorova u grafu $\mathrm{ICG}_n(1,d)$. Definišimo niz brojeva $x_k = a_k \cdot d + b_k$ za $k = 0, 1, \ldots, q-1$, gde je b_k ostatak broja k pri deljenju sa p_1, a za a_k važe sledeći uslovi:

$$\begin{aligned} a_k \cdot d + b_k &\equiv k && \mod p && \text{za svako} p \in Q \\ a_k &\equiv \lfloor k/p_1 \rfloor && \mod p && \text{za svako} p \in R \end{aligned}$$

Brojevi a_k se mogu jedinstveno odrediti korišćenjem Kineske teoreme o ostacima po modulu M, jer su d i p uzajamno prosti, za svaki prost broj $p \in Q$. Dokazaćemo da je najveći zajednički delilac brojeva $x_k - x_{k'}$ i n jednak d ili 1, odakle bi sledilo da temena x_k čine kliku. Naime, za svaki prost $p \in Q$, imamo $x_k - x_{k'} \equiv k - k' \mod p$. Kako je $|k - k'| < q$, to $x_k - x_{k'}$ ne može biti deljivo sa p.

Dalje, razmotrimo slučaj kada k i k' imaju isti ostatak pri deljenju sa p_1 i $k \neq k'$. Drugim rečima je $b_k = b_{k'}$ i $k \neq k'$. Ako je $a_k - a_{k'}$ deljivo nekim prostim $p \in R$, to je takođe i $\lfloor k/p_1 \rfloor \equiv \lfloor k'/p_1 \rfloor \mod p$. Pošto je $k \leq q < p_1 \cdot p_i$, zaključujemo da je razlika celobrojnih delova brojeva $|\lfloor k/p_1 \rfloor - \lfloor k'/p_1 \rfloor| < p_i \leq p$, pa su $\lfloor k/p_1 \rfloor$ i $\lfloor k'/p_1 \rfloor$ jednaki. Kako imamo još i da je $b_k = b_{k'}$, dobijamo $k = k'$. Na ovaj način dobijamo kontradikciju i zato je $\gcd(x_k - x_{k'}, n) = d$. U slučaju $b_k \neq b_{k'}$, imamo da $x_k - x_{k'}$ nije deljivo ni sa jednim $p \in R$, jer je d deljivo sa p i $0 < |b_k - b_{k'}| < p_1$. Konačno je $gcd(x_k - x_{k'}, n) = 1$, čime je dokaz završen. □

Sledeću teorema predstavlja posledicu prethodnih rezultata.

Teorema 3.3.8. *Za proizvoljan delilac d broja n, važi:*

$$\omega(\mathrm{ICG}_n(1,d)) = \min\left(\min_{p \in Q} p, f(n) \cdot f\left(\frac{n}{d}\right)\right).$$

Slučaj 2: $1 \notin D$

Teorema 3.3.9. *Neka je $\mathrm{ICG}_n(d_1, d_2)$ integralan cirkularan graf tako da su oba delioca d_1 i d_2 veći od jedinice. Tada važi sledeća jednakost:*

$$\omega\left(\mathrm{ICG}_n(d_1,d_2)\right) = \begin{cases} \omega(\mathrm{ICG}_{\frac{n}{d_2}}(1, \frac{d_1}{d_2})), & \text{ako } d_2 \mid d_1, \\ \max\left(f\left(\frac{n}{d_1}\right), f\left(\frac{n}{d_2}\right)\right), & \text{u suprotnom.} \end{cases}$$

Dokaz. Pretpostavimo da $d_2 \mid d_1$. Korišćenjem Leme **??**, graf $\mathrm{ICG}_n(d_1,d_2)$ je nepovezan i izomorfan sa d_2 kopije grafa $\mathrm{ICG}_{n/d_2}(1, \frac{d_1}{d_2})$. Otuda je $\omega(\mathrm{ICG}_n(d_1,d_2)) = \omega(\mathrm{ICG}_{n/d_2}(1, \frac{d_1}{d_2}))$, a rešenje poslednjeg problema je dato Teoremom **??**.

Pretpostavimo da $d_2 \nmid d_1$. Takođe ćemo pretpostaviti da maksimalna klika sadrži ivice koje su obojene obema bojama. Tada među ivicama grafa postoji trougao čije su tačno dve ivice obojene istom bojom. Ako je ta boja crvena, onda možemo naći tri čvora a, b i c tako da je:

$$\gcd(a-b,n) = d_1, \quad \gcd(a-c,n) = d_2, \quad \gcd(b-c,n) = d_2.$$

Oduzimajući poslednje dve nejednakosti dobijamo da $d_2 \mid (a-c)-(b-c)$, odakle sledi da d_2 deli d_1, što je kontradikcija. Ako imamo trougao sa dve plave ivice, slično ćemo naći da d_1 deli d_2 – što je nemoguće budući da je $d_1 > d_2$. Stoga imamo da je maksimalna klika jednobojna, pa je prema Posledici **??** gornja jednaskost u ovom slučaju dokazana. □

3.3.2 Veličina maksimalne klike za $t \geq 2$

U ovom odeljku testiramo hipotezu da veličina maksimalne klike intergralnih cirkularnih grafova deli red grafa, koja je data u [**?**]. Najpre, na osnovu Teoreme **??** i Posledice **??** zaključujemo da je hipoteza tačna u slučaju kada je skup delioca integralnog cirkularnog grafa najviše dvočlan. Tada je veličina maksimalne klike grafa $\mathrm{ICG}_n(D)$ jednaka proizvodu dva prosta broja delioca od n. Hipotezu smo najpre testirali kompjuterskom metodom implementiranjem *Backtracking algoritma sa odsecanjem* [**?**] za pronalaženje maksimalne klike (videti prilog). Za $t = 3$ and $t = 4$, može se konstruisati beskonačna familija integralnih circularnih grafova, takvih da veličina maksimalne klike ne deli n. Na primer, korišćenjem navedenog algoritma sveobuhvatom proverom dobija se $\omega(\mathrm{ICG}_{20}(1,4,10)) = 6$ i $\omega(\mathrm{ICG}_{30}(1,2,6,15)) = 7$. Ovi primeri impliciraju da hipoteza nije uvek zadovoljena za $3 \leq t \leq 4$. Sledećim tvrđenjem odbacićemo hipoetezu dokazujući tvrđenje teoretski.

Propozicija 3.3.10. *Veličina najveće klike integralnog cirkularnog grafa* $\mathrm{ICG}_{20}(1,4,10)$ *je* 6 *ili* 7*.*

Dokaz. Lako se može uočiti da čvorovi $0, 1, 4, 8, 11, 12$ formiraju kliku u $\mathrm{ICG}_{20}(1,4,10)$. Obojimo ivice grafa trima bojama: *crvenom* ako je $gcd(a-b,20) = 1$, *plavom* ako je $gcd(a-b,20) = 4$, i *zelenom* ako je $gcd(a-b,20) = 10$.

Na osnovu Posledice **??**, maksimalna klika sa crvenim ivicama ima 2 čvora, maksimalna klika sa plavim ivicama ima 5 čvorova, i za zelenu boju ima 2 čvora. Ako u datom grafu trougao ima jednu plavu i jednu zelenu ivicu, to zbog parnosti, treća ivica ne sme biti crvena. Ako bi treća ivica bila plave boje, tada je apsolutna vrednost razlike čvorova na zelenoj ivici deljiva sa 4, što je nemoguće. Na isti način, ako bi treća ivica bila zelene boje, tada je apsolutna vrednost razlike čvorova na plavoj ivici deljiva sa 5. Zato ne postoji trougao koji se sastoji samo od plavih i zelenih ivica.

Zaključujemo, ako je maksimalna klika dvobojna, ona sadrži crvene i plave ivice ili crvene i zelene. U prvom slučaju problem se svodi na nalaženje maksimalne klike u $\mathrm{ICG}_{20}(1,4)$. Primenom Teoreme **??** zaključujemo da je $\omega(\mathrm{ICG}_{20}(1,4)) = 5$. Analogno, veličina maksimalne klike sa crvenim i zelenim ivicama je $\omega(\mathrm{ICG}_{20}(1,10)) = 4$ by Theorem **??**. U oba slučaja obe klike ne mogu biti maksimalne, jer smo već pronašli kliku veličine 6. Odavde imamo da maksimalna klika mora biti trobojna.

Sada pretpostavimo da se maksimalna trobojna klika sastoji od x klika plave boje i y klika zelene boje. Korišćenjem pomenutog zaključka da ne postoji trougao sa plavim i zelenim ivicama, lako se može uočiti da ne postoji trougao samo sa plavim i crvenim, kao ni zelenim

i crvenim ivicama. Odavde imamo da samo crvene ivice spajaju čvorove ovih $x + y$ klika. Ako izaberemo po jedan čvor iz svake klike, dobićemo crvenu kliku sa $x + y$ čvorova. Kako maksimalna klika sa crvenim čvorovima ima samo dva čora, to mora biti $x = y = 1$. Dakle, gornja granica za veličinu maksimalne klike je $2 + 5 = 7$, a donja granica je 6, što u oba slučaja nisu delioci broja 20. □

Propozicija 3.3.11. *Neka je $X_n(D)$ integralni cirkularni graf čiji je skup delioca $D = \{d_1, d_2, \ldots, d_k\}$. Ako je $N = n \cdot p$ gde je p proizvoljni prost broj veći od n, tada važi sledeća nejednakost*

$$\omega(\mathrm{ICG}_N(D)) = \omega(\mathrm{ICG}_n(D)).$$

Dokaz. Kako je $p > n$ i zbog toga $gcd(a-b, n) = gcd(a-b, p\cdot n)$ to za proizvoljne čvorove $a, b \in \mathrm{ICG}_n(D)$, dobijamo sledeću nejednakost $\omega(\mathrm{ICG}_N(D)) \geqslant \omega(\mathrm{ICG}_n(D))$. Dalje, pretpostavimo da čvorovi $\{a_1, a_2, \ldots, a_c\}$ čine maksimalnu kliku u $\mathrm{ICG}_N(D)$ i posmatrajmo čvorove $\{b_1, b_2, \ldots, b_c\}$ u grafu $\mathrm{ICG}_n(D)$, gde je b_i ostatak od a_i po modulu n. Prost broj p ne deli ni jedan od delilaca d_i, te zato ni $a_i - a_j$ nije deljivo sa p ni za koje $1 \leqslant i < j \leqslant c$. Konačno imamo

$$gcd(b_i - b_j, n) = gcd(a_i - a_j, n) = gcd(a_i - a_j, N) \in D.$$

Odavde sledi da je $\omega(\mathrm{ICG}_N(D)) \leqslant \omega(\mathrm{ICG}_n(D))$, to jest $\omega(\mathrm{ICG}_N(D)) = \omega(\mathrm{ICG}_n(D))$. □

Korišćenjem ovog tvrđenja možemo konstruisati klasu kontraprimera $\mathrm{ICG}_{20p}(1, 4, 10)$ izvedenu iz grafa $\mathrm{ICG}_{20}(1, 4, 10)$, gde je p prost broj veći od 20. Slično možemo izvesti klasu kontraprimera iz $\mathrm{ICG}_{30}(1, 2, 6, 15)$ za četvoročlane skupove.

U ovoj sekciji je data formula za veličinu maksimalne klike u slučaju $1 \leq t \leq 2$, a u slučaju $t \geq 3$ imamo da veličina maksimalne klike ne mora da deli red grafa. Takođe, u opštem slučaju važi sledeća nejednakost

$$\max_{d_i \in D} f\left(\frac{n}{d_i}\right) \leqslant \omega(X_n(D)) \leqslant \prod_{i=1}^{k} f\left(\frac{n}{d_i}\right).$$

Donja granica direktno sledi iz Posledice **??**, a gornja granica se može dokazati indukcijom po broju delilalaca. Zaista, nakon dodavanja ivica $\{a, b\}$ takvih da je $gcd(a - b, n) = d_i$ grafu $\mathrm{ICG}_n(d_1, d_2, \ldots, d_{i-1})$, možemo podeliti svaku klasu čorova obojenu jednom bojom na najviše $f(\frac{n}{d_i})$ nezavisnih delova (obojiti sa najviše $f(\frac{n}{d_i})$ novih boja). Dakle, broj klasa je manji ili jednak proizvodu brojeva $f(\frac{n}{d_i})$, za svako $d_i \in D$.

3.4 Hromatski broj

U ovoj sekciji razmatramo hromatski broj integralnih cirkularnih grafova i istražujemo hipotezu datu u [**?**] da hromatski broj deli red n grafa $\mathrm{ICG}_n(D)$. Za integralni cirkularni graf sa dva delioca daćemo oštru gornju i donju granicu hromatskog broja. Takođe ako je jedan od delioca jednak jedinici, hromatski broj je eksplicitno određen formulom zatvorene forme. Za $|D| \geq 3$ konstruisali smo familiju kontraprimera korišćenjem sveobuhvatnog algoritma za bojenje grafa i pobili hipotezu u ovom slučaju. Na kraju sekcije su dati neki rezultati, kao i otvoreni problemi vezani za ivični hromatski broj integralnih cirkularnih grafova. Razmatranja hromatskog broja u ovoj sekciji predstavljaju prirodni nastavak izučavanje klike iz prethodne glave, pa ćemo i

ovde pretpostaviti da je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gde su $p_1 < p_2 < \ldots < p_k$ različiti prosti brojevi i $\alpha_i \geq 1$. Takođe, $f(n)$ predstavlja najmanji prost delilac broja n. Neka je d proizvoljni delilac broja n. Definišimo skup Q_d kao skup svih prostih delilaca od n koji ne dele d i R_d skup delilaca od d koji takođe dele $\frac{n}{d}$.

Na osnovu rezultata datog u Lemi **??**, dovoljno je posmatrati hromatski broj povezanih integralnih cirkularnih grafova. Takođe kao nastavak rezultata datog u Posledici **??**, može se dokazati da postoji jedinstveno bojenje grafa $\mathrm{ICG}_n(\{1\})$ sa $p = f(n)$ boja. Čvorovi $0, 1, \ldots, p-1$ moraju pripadati različitim klasama bojenja (svaka dva čvora moraju biti povezana, jer je razlika manja od p). Iz istog razloga, sledeći čvor p ne može biti u istoj klasi bojenja zajedno sa čvorovima $p-1, p-2, \ldots, 1$, pa zato mora biti u istoj klasi bojenja kao i 0. Ponovo, čvor $p+1$ je u istoj klasi kao i čvor 1. Nastavkom ove procedure, jedinstveno određujemo boje čvorova $p, p+1, \ldots, 2p-1$ i konačno dobijamo da su klase bojenja grafa $\mathrm{ICG}_n(\{1\})$ ustvari klase po modulu p.

3.4.1 Kontraprimeri

Da bi testirali hipotezu datu u [**?**], implementiran je algoritam *Backtracking Sequential Coloring* [**?**] za određivanje hromatskog broja integralnih cirkularnih grafova $\mathrm{ICG}_n(D)$ za različite vrednosti broja n (videti prilog). Takođe je korišćen *Cliquer algorithm* [**?**] za određivanje svih maksimalnih klika u grafu. Za $t = 3$ i $t = 4$, nađena je beskonična familija grafova takva da hromatski broj ne deli red grafa n.

Jedan od kontraprimera predstavlja graf $\mathrm{ICG}_n(D)$, gde je $n = 30$ sa skupom delioca $D = \{1, 6, 10\}$. Takođe, jedno od bojenja sa minimalnim brojem boja, koje je generisano algoritmom je

$$[1, 2, 7, 3, 2, 1, 5, 3, 4, 1, 4, 5, 3, 4, 1, 5, 6, 8, 7, 6, 5, 6, 8, 7, 6, 8, 2, 7, 3, 2]\,,$$

te se može zaključiti da je $\chi(\mathrm{ICG}_{30}(1, 6, 10)) = 8$, što nije delitelj broja 30.

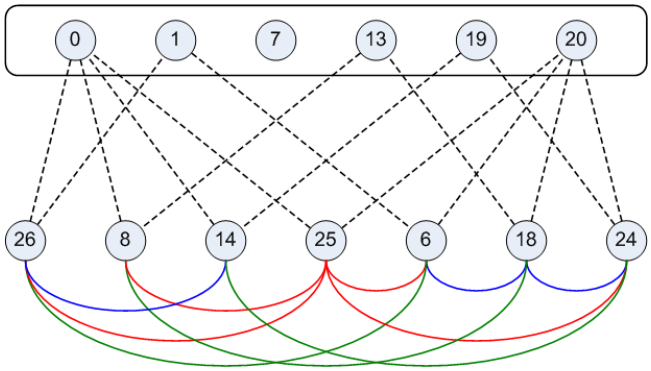
Čvorovi $C = \{0, 1, 7, 13, 19, 20\}$ generišu kliku u datom grafu, što znači da je $6 \leq \chi(\mathrm{ICG}_{30}(D)) \leq 8$. Za odbacivanje hipoteze teoretski, dovoljno je pokazati da je hromatski broj različit od 6.

Propozicija 3.4.1. *Hromatski broj integralnog cirkularnog grafa* $\mathrm{ICG}_{30}(1, 6, 10)$ *je strogo veći od* 6.

Dokaz. Pretpostavimo da su čvorovi klike C obojeni bojama $c_1, c_2, c_3, c_4, c_5, c_6$ i da je $\chi(\mathrm{ICG}_{30}(1, 6, 10)) = 6$. Čvor 6 se može obojiti samo bojama c_2 ili c_6, jer je povezan sa čvorovima $0, 7, 13, 19$. Slično, ispitujući susede čvorova $8, 14, 18, 24, 25, 26$ koji pripadaju skupu C zaključujemo da se čvor 8 može obojiti bojama $\{c_1, c_4\}$, čvor 14 bojama $\{c_1, c_5\}$, čvor 18 bojama $\{c_4, c_6\}$, čvor 24 bojama $\{c_5, c_6\}$, čvor 25 bojama $\{c_1, c_6\}$ i čvor 26 bojama $\{c_1, c_2\}$. Na slici 3.2 ispod, isprekidane linije predstavljaju ivice u komplementarnom grafu, a u drugom nivou čvorova su označene neke od ivica grafa $\mathrm{ICG}_{30}(1, 6, 10)$.

Pretpostavimo da je čvor 6 obojen bojom c_6. Čvorovi $18, 6, 25$ formiraju put, tako da čvor 18 mora biti obojen bojom c_4, a čvor 25 bojom c_1. Čvor 8 je sused čvorovima 18 i 25, što znači da ne može biti obojen bojama c_1 i c_4.

U drugom slučaju, neka je čvor 6 obojen sa c_2. Čvorovi $6, 26, 25, 24$ predstavljaju put, pa 26 mora biti obojen sa c_1, 25 sa c_6 i 24 sa c_5. Međutim, čvor 14 je sused čvorovima 24 i 26, odakle imamo da ne može biti obojen bojama c_1 i c_5. Ovim kompletiramo dokaz i zaključujemo da je $\chi(\mathrm{ICG}_{30}(1, 6, 10)) > 6$. □



Slika 3.2: *Veličina maksimalne klike u grafu* $\mathrm{ICG}_{30}(1, 6, 10)$

Pretpostavimo da već znamo hromatski broj datog grafa $\mathrm{ICG}_n(D)$ sa fiksnim skupom delioca $D = \{d_1, d_2, \ldots, d_t\}$. Sledeće pitanje se prirodno nameće: *Koji je odnos između hromatskog broja grafova* $\mathrm{ICG}_N(D)$ *i* $\mathrm{ICG}_n(D)$, *gde je* $N = n \cdot p$ *i* p *proizvoljan prost broj veći od* n*?*

Graf $\mathrm{ICG}_n(D)$ je indukovani podgraf od $\mathrm{ICG}_N(D)$, pošto za proizvoljne čvorove $0 \leq a, b < n$ imamo da je

$$\gcd(a - b, n) = d_i \quad \text{ako i samo ako} \quad \gcd(a - b, N) = d_i.$$

Odavde sledi da je $\chi(\mathrm{ICG}_N(D)) \geq \chi(\mathrm{ICG}_n(D))$. Optimalno bojenje grafa $\mathrm{ICG}_N(d_1, d_2, \ldots, d_t)$ može biti izvedeno iz bojenja grafa $\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)$ na sledeći način. Proizvoljni čvor $v \in \mathrm{ICG}_N(D)$ treba biti obojen istom bojom kao i čvor koji je ostatak od v po modulu n u $\mathrm{ICG}_n(D)$. Dokazaćemo da je ovo pravilno bojenje grafa $\mathrm{ICG}_N(D)$.

Ako su a i b čvorovi jednaki po modulu n, imamo da je

$$\gcd(a - b, N) = n \cdot \gcd(k, p) = n > d_i,$$

za neko $0 \leq k = \frac{a-b}{n} < p$ i $d_i \in D$. Odavde imamo da čvorovi iz iste klase po modulu n nisu susedni. Neka su $x_1 + y_1 \cdot n$ i $x_2 + y_2 \cdot n$ susedni čvorovi iz različitih klasa grafa $\mathrm{ICG}_N(D)$, gde su $0 \leq x_1, x_2 \leq n - 1$, $0 \leq y_1, y_2 \leq p - 1$ i $x_1 \neq x_2$. Neka je d najveći zajednički delilac brojeva $x_1 - x_2$ i n. Odavde sledi da je

$$\gcd((x_1 - x_2) + (y_1 - y_2) \cdot n, N) = d_i,$$

za neko $d_i \in D$ i da d_i deli $x_1 - x_2$ što nas dovodi do $d_i \mid d$. Sa druge strane, d je delilac od $x_1 - x_2$, n i N, te zato d deli d_i. Konačno je odavde $d = d_i$, odakle zaključujemo da su čvorovi $x_1 + y_1 \cdot n$ i $x_2 + y_2 \cdot n$ susedni u $\mathrm{ICG}_N(d_1, d_2, \ldots, d_t)$ ako i samo ako su čvorovi x_1 i x_2 susedi u $\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)$. Iz optimalnog bojenja grafa $\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)$ dobijamo da su čvorovi $x_1 + y_1 \cdot n$ i $x_2 + y_2 \cdot n$ u $\mathrm{ICG}_N(d_1, d_2, \ldots, d_t)$ u različitim klasama.

Gornja razmatranja nas dovode do sledećeg zaključka

Propozicija 3.4.2. *Neka je* $\mathrm{ICG}_n(D)$ *integralni cirkulantni graf sa skupom delioca* $D = \{d_1, d_2, \ldots, d_t\}$. *Tada važi*

$$\chi(\mathrm{ICG}_N(D)) = \chi(\mathrm{ICG}_n(D)),$$

gde je p *proizvoljan prost broj veći od* n *i* $N = n \cdot p$.

Na osnovu prethodnog rezultata možemo konstruisati klasu kontraprimera za $n = 30 \cdot p$ i $D = \{1, 6, 10\}$, gde je p prost broj veći od 30. Slično, za $n = 30$ i skup delioca $D = \{1, 6, 10, 15\}$ možemo naći novu klasu kontraprimera takvu da je $\chi(\mathrm{ICG}_n(D)) = 8$ i $|D| = 4$, takođe nađenu od strane algoritma.

3.4.2 Hromatski broj za $t = 2$

U ovoj podsekciji dajemo gornju i donju granicu za hromatski broj integralnih cirkularnih grafova sa proizvoljnim brojem delioca. Za povezani integralni cirkularni graf $\mathrm{ICG}_n(D)$, gde je $D = \{d_1, d_2\}$ granica se može poboljšati, dok se za $D = \{1, d\}$, može dobiti eksplicitna formula za hromatski broj.

Teorema 3.4.3. *Za graf* $\mathrm{ICG}_n(d_1, d_2)$ *važi sledeća nejednakost*

$$\max\left(f\left(\frac{n}{d_1}\right), f\left(\frac{n}{d_2}\right)\right) \leq \chi(\mathrm{ICG}_n(d_1, d_2)) \leq f\left(\frac{n}{d_1}\right) \cdot f\left(\frac{n}{d_2}\right).$$

Dokaz. Na osnovu Posledice **??**, lako se može utvrditi da je hromatski broj grafa $\mathrm{ICG}_n(d_1, d_2)$ veći ili jednak maksimumu brojeva $f(\frac{n}{d_1})$ i $f(\frac{n}{d_2})$.

Skup ivica grafa $\mathrm{ICG}_n(d_1, d_2)$ se sastoji od skupa ivica podgrafova $\mathrm{ICG}_n(d_1)$ i $\mathrm{ICG}_n(d_2)$. U prvom grafu $\mathrm{ICG}_n(d_1)$ imamo tačno $f(\frac{n}{d_1}) = p$ klasa bojenja. Da bi procenili hromatski broj $\mathrm{ICG}_n(d_1, d_2)$, možemo svaku klasu ivica obojenih istom bojom iz $\mathrm{ICG}_n(d_1)$ podeliti na klase bojenja podgrafa $\mathrm{ICG}_n(d_2)$. Svaka klasa bojenja od $\mathrm{ICG}_n(d_1)$ ima tačno $\frac{n}{p}$ čvorova. Iz Posledice **??**, postoji pravilno bojenje grafa $\mathrm{ICG}_n(d_2)$ sa $f(\frac{n}{d_2}) = q$ boja. Zato čvorovi u proizvoljnoj klasi bojenja grafa $\mathrm{ICG}_n(d_1)$ mogu takođe biti podeljeni u najviše q nezavisnih klasa. Na ovaj način dobijamo pravilno bojenje grafa $\mathrm{ICG}_n(d_1, d_2)$ sa najviše $p \cdot q$ boja. □

Prethodna teorema može biti uopštena za proizvoljni skup delioca D. Donja granica sledi iz Leme **??**, dok se gornja granica dobija primenom matematičke indukcije na broj delioca u D.

$$\max_{d_i \in D} f\left(\frac{n}{d_1}\right) \leq \omega(\mathrm{ICG}_n(D)) \leq \chi(\mathrm{ICG}_n(D)) \leq \prod_{i=1}^{t} f\left(\frac{n}{d_i}\right). \tag{3.10}$$

Gornja granica se dostiže za $n = p^\alpha$, gde je p prost broj i $\alpha \geq 2$. Svaki delilac broja n je oblika p^β, gde je $0 \leq \beta \leq \alpha$. Za povezani graf $\mathrm{ICG}_n(D)$, važi da je $d_1 = 1$. Pokazaćemo da je

$$\omega(X_n(d_1, d_2, \ldots, d_t)) = \chi(X_n(d_1, d_2, \ldots, d_t)) = p^t.$$

Neka je $d_i = p^{\beta_i}$, gde je $0 = \beta_1 < \beta_2 < \ldots < \beta_t < \alpha$ i $t \leq \alpha$. Dokazujemo da čvorovi

$$C = \left\{ \sum_{i=1}^{t} \alpha_i \cdot p^{\beta_i} \mid 0 \leq \alpha_i \leq p-1 \right\}$$

obrazuju kliku veličine p^t u grafu $\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)$. Primetimo najpre da su svi brojevi iz C različiti uzimajući ih u sistemu brojeva sa osnovom p:

$$v = \sum_{i=1}^{t} \alpha_i \cdot p^{\beta_i} = \overline{\alpha_1 \alpha_2 \ldots \alpha_k}\ .$$

Neka je $a = \sum_{i=1}^{t} \alpha_i \cdot p^{\beta_i}$ i $b = \sum_{i=1}^{t} \alpha'_i \cdot p^{\beta_i}$ proizvoljni čvorovi iz C. Kako je $a \neq b$, postoji najmanji indeks $1 \leq s \leq t$, takav da je $\alpha_s \neq \alpha'_s$. Odavde je

$$a - b = (\alpha_s - \alpha'_s) \cdot p^{\beta_s} + (\alpha_{s+1} - \alpha'_{s+1}) \cdot p^{\beta_{s+1}} + \ldots + (\alpha_t - \alpha'_t) \cdot p^{\beta_t}.$$

Najveći zajednički delilac brojeva $a - b$ i $n = p^\alpha$ jednak je p^{β_s}, jer je $0 < |\alpha_s - \alpha'_s| < p$. Zato zaključujemo da su svaka dva čvora iz C susedna, te je C klika veličine p^t u $\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)$.

Sledeća nejednakost je od suštinske važnosti u budućim razmatranjima.

Teorema 3.4.4. *Neka je* $\mathrm{ICG}_n(D)$ *integralni cirkularni graf sa skupom delioca* $D = \{d_1, d_2, \ldots, d_t\}$. *Neka je* p *prost delilac broja* n *takav da* $p \nmid d_i$ *za* $i = 1, 2, \ldots, t$. *Tada je*

$$\chi(\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)) \leq p.$$

Dokaz. Obojimo čvorove grafa $\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)$ sa p boja, tako da su klase bojenja ustvari klase po modulu p. Zaista je ovo pravilno bojenje, jer je za svaki par čvorova a i b iz iste klase bojenja imamo da je $\gcd(a - b, n) = \gcd(l \cdot p, n) = p \cdot s \notin \{d_1, d_2, \ldots, d_t\}$, za neko $0 \leq l < \frac{n}{p}$ i $s \in \mathbb{N}$. To znači da ne postoji ni jedna ivica među čvorovima iz iste klase po modulu p, odakle direktno dobijamo gornju jednakost. □

Slučaj $1 \in D$

Teorema 3.4.5. *Za integralni cirkularni graf* $\mathrm{ICG}_n(1, d)$, *gde je* d *delilac od* n, *važi*

$$\chi(\mathrm{ICG}_n(1, d)) = \min\left(\min_{p \in Q_d} p, f(n) \cdot f\left(\frac{n}{d}\right)\right).$$

Dokaz. Direktnom primenom Teorema **??** i **??** dobijamo da je

$$\chi(\mathrm{ICG}_n(1, d)) \leq \min\left(\min_{p \in Q_d} p, f(n) \cdot f\left(\frac{n}{d}\right)\right).$$

Sa druge strane, prema Teoremi **??** važi da je

$$\chi(\mathrm{ICG}_n(1, d)) \geq \omega(\mathrm{ICG}_n(1, d)) = \min\left(\min_{p \in Q_d} p, f(n) \cdot f\left(\frac{n}{d}\right)\right),$$

čime je dokaz teoreme kompletiran. □

Slučaj $1 \notin D$

Pretpostavimo da je $\mathrm{ICG}_n(d_1, d_2)$ povezan, što znači da je $\gcd(d_1, d_2) = 1$. Neka je Q_j skup svih prostih delioca broja n koji ne deli d_j, pri čemu sa q_j označimo najmanji prost delilac skupa Q_j (ukoliko postoji), za $j = \overline{1, 2}$.

Propozicija 3.4.6. *Neka su* d_1 *i* d_2 *delioci prirodnog broja* n *takvi da je* $\gcd(d_1, d_2) = 1$. *Tada je*

$$f\left(\frac{n}{d_1}\right) = q_1 = p_1 \qquad \textit{ili} \qquad f\left(\frac{n}{d_2}\right) = q_2 = p_1,$$

gde je p_1 *najmanji prost delilac od* n.

Dokaz. Kako su delioci d_1 i d_2 uzajamno prosti, oni ne mogu oba biti deljivi sa p_1. Bez gubljenja opštosti, pretpostavimo da $p_1 \nmid d_2$. Iz poslednjeg direktno imamo da je $p_1 \in Q_2$ i da $p_1 \mid \frac{n}{d_2}$, odakle sledi da je $q_2 = p_1 = f(\frac{n}{d_2})$. □

Zato možemo u nastavku pretpostaviti da $p_1 \nmid d_2$.

Teorema 3.4.7. *Za integralni cirkularni graf* $\mathrm{ICG}_n(d_1, d_2)$ *važi da je*

$$\chi(\mathrm{ICG}_n(d_1, d_2)) \leq \min_{p \in Q_1} p = q_1.$$

Dokaz. Pretpostavimo najpre da q_1 ne deli d_2. Iz Teoreme **??**, kako $q_1 \nmid d_1$ sledi da je $\chi(\mathrm{ICG}_n(d_1, d_2)) \leq q_1$. Pretpostavimo sada da $q_1 \mid d_2$. Kako p_1 ne deli d_2, imamo nejednakost $q_1 > p_1$. Štaviše, ako p_1 ne deli d_1, ponovnom primenom Teoreme **??**, zaključujemo da je $\chi(\mathrm{ICG}_n(d_1, d_2)) \leq p_1 < q_1$.

Zato pretpostavimo da $p_1 \mid d_1$. Posmatrajmo sledeću particiju skupa čvorova u klase $C_0, C_1, \ldots, C_{q_1-1}$, definisanu sa

$$C_l = \{i \mid 0 \leq i < n,\ 0 \leq r \leq p_1 - 1\ ,\ i \equiv p_1 \cdot l + r \mod p_1 \cdot q_1\}.$$

Svaka klasa ima $\frac{n}{q_1}$ čvorova. Za proizvoljne čvorove $a \equiv p_1 l + r' \mod p_1 \cdot q_1$ i $b \equiv p_1 l + r'' \mod p_1 \cdot q_1$ iz iste klase C_l, važi da je $a - b \equiv r' - r'' \mod p_1 \cdot q_1$. Iz $0 \leq |r' - r''| < p_1 < q_1$ sledi da ili $p_1, q_1 \nmid a - b$ ili $p_1 \cdot q_1 \mid a - b$.

Ako je $p_1 \nmid a - b$ i $q_1 \nmid a - b$, imamo da $p_1 \cdot q_1 \nmid \gcd(a - b, n)$. Prema prethodnoj pretpostavci važi da $p_1 \mid d_1$ i $q_1 \mid d_2$, te zato $\gcd(a - b, n)$ ne može biti jednako ni sa d_1 ni sa d_2. Slično, eliminišemo drugi slučaj kada $p_1 \cdot q_1 \mid \gcd(a - b, n)$, jer $p_1 \nmid d_2$ i $q_1 \nmid d_1$. Dakle, svaka od klasa C_l je nezavisni skup, pa ih možemo obojiti različitim bojama i dobiti pravilno bojenje.

□

Primenom Teorema **??** i **??** dobijamo sledeći rezultat

Teorema 3.4.8. *Za povezan integralni cirkularni graf* $\mathrm{ICG}_n(d_1, d_2)$*, važi da je*

$$\chi(\mathrm{ICG}_n(d_1, d_2)) \leq \min\ \left(\max(\min_{p \in Q_1} p, \min_{p \in Q_2} p), f\left(\frac{n}{d_1}\right) \cdot f\left(\frac{n}{d_2}\right)\right).$$

Iz Teorema **??** i **??** sledi da je $\chi(\mathrm{ICG}_n(d_1, d_2)) = 2$ ako i samo ako je $q_1 = 2$. Ovaj rezultat predstavlja uopštenje Teoreme **??** za unitarne Kejlijeve grafove, gde stoji da je $\mathrm{ICG}_n(1)$ bipartitan ako i samo ako je n parno.

Interesantno bi bilo ispitati ivični hromatski broj integralnih cirkularnih grafova, a mi ovde dajemo neke parcijalne rezultate. Najmanji mogući broj boja potreban za pravilno bojenje ivica grafa označavamo sa $\chi'(G)$. Na osnovu čuvene Vizingove teoreme imamo da je $\Delta \leq \chi'(G) \leq \Delta + 1$, gde je Δ maksimalni stepen u grafu G. Graf $\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)$ je regularan graf stepena $\varphi(\frac{n}{d_1}) + \varphi(\frac{n}{d_2}) + \ldots + \varphi(\frac{n}{d_t})$.

Ako je n neparan, $\mathrm{ICG}_n(D)$ se ne može razložiti u 1-faktorne skupove, te je zato $\chi'(\mathrm{ICG}_n(D)) = \Delta + 1$. Sada pretpostavimo da je n paran. Unitarni Kejlijev graf $\mathrm{ICG}_n(1)$ se može razložiti na $\varphi(n)/2$ Hamiltonovih ciklova [**?**] i svaki od ovih ciklova je parne dužine. Svaki cikl se može obojiti u dve boje, bojeći naizmenično ivice različitim bojama. Posle bojenja svih ciklova, dobijamo pravilno bojenje grafa $\mathrm{ICG}_n(\{1\})$ korišćenjem $\varphi(n)$ boja. Kako je $\varphi(n)$ maksimalan stepen grafa $\mathrm{ICG}_n(1)$ sledi da je $\chi(\mathrm{ICG}_n(1)) = \Delta$. Primenom Teoreme **??**, zaključujemo da je ivični hromatski broj grafa $\mathrm{ICG}_n(d)$ jednak Δ ako i samo ako je $\frac{n}{d}$ paran. U opštem slučaju, svaki delilac d_i indukuje $\varphi(\frac{n}{d_i})$ novih ivica iz svakog čvora. Ako je $\frac{n}{d_i}$ paran za svako $i = 1, 2, \ldots, k$, možemo nezavisno posmatrati ove delioce, pa nakon primene iste činjenice dobijamo da je $\chi'(\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)) = \Delta$.

Jasno je da nije lako izračunati eksplicitno formulu za hromatski broj integralnih cirkularnih grafova, čak i u slučaju kada je $t = 2$. Takođe, primeri ukazuju da je jednakost u Teoremi **??** uvek dostižna. Sa druge strane, nemamo kompletnu karakterizaciju integralnih cirkularnih grafova takvih da je $\chi'(\mathrm{ICG}_n(d_1, d_2, \ldots, d_t)) = \Delta$, što ostavljamo kao otvoren problem.

3.5 Grupa automorfizama

Automorfizam je permutacija skupa čvorova koja čuva njihovo susedstvo. Skup svih automorfizama, u oznaci

$$Aut(G) = \{f : V(G) \to V(G) \mid f \text{ je bijekcija i } (a,b) \in E(G) \text{ akko } (f(a), f(b)) \in E(G)\}$$

predstavlja grupu u odnosu na operaciju kompozicije preslikavanja (grupa automorfizama).

U ovoj sekciji je data karakterizacija grupe automorfizma unitarnih Kejlijevih grafova i nekih klasa integralnih cirkluarnih grafova. Treba napomenuti da je više autora proučavalo koncept izomorfizama i automorfizama na cirkularnim grafovim, kao i na srodnim klasama. Možemo izdvojiti studije o izomorfizmima na cirkularnim i Kejlijevim grafovima [**?**, **?**], grupi automorfizama Kejlijevih digrafova [**?**], integralnim Kejlijevim grafovima na Abelovim grupama [**?**], racionalnim cirkularnim grafovima [**?**], itd. Pregled rezultati o automorfizmima na cirkularnim grafovima dati su u članku [**?**]. Sledeći metodologiju radova Kovács [**?**] i Dobson i Morris [**?**, **?**], razmatraćemo dva slučaja: $n = p^k$ je stepen prostog broja i $n = p_1p_2 \dots p_k$ je proizvod različitih prostih brojeva. Ovi rezultati su od suštinske važnosti za buduća istraživanja u ovoj oblasti. Takodje, glavno sredstvo za opisivanje relevantnih osobina automorfizama na integralnim cirkularnim grafovima, biće formula za izračunavanje broja zajedničkih suseda proizvoljna dva čvora. Zato će se početni rezultati sledeće podsekcije odnositi upravo na ovu formulu.

Pri karakterizaciji grupe automorfizama, koristimo koncept proizvoda (engl. wreath producst) grupa (sliačan leksikografskom proizvodu u teoriji grafova) [**?**].

Definicija 3.5.1. *Neka su G i H date grupe permutacija na skupovima X i Y, redom. "Wreath" proizvod grupa H i G, u oznaci $G \wr H$, je permutaciona grupa elemenata iz $X \times Y$ koja sadrži sve permutacije oblika $(x, y) \to (g(x), h_x(y))$, gde su $g \in G$ i $h_x \in H$.*

3.5.1 Grupa automorfizama za unitarne Kejlijeve grafove

Za graf G, označimo sa $N(a, b)$ broj zajedničkih suseda čvorova a i b. Sledećom teorema određuje broj zajedničkih suseda para čvorova u unitarnom Kejlijevom grafu $\mathrm{ICG}_n(1)$:

Teorema 3.5.1. *Broj zajedničkih suseda različitih čvorova a i b u unitarnom Kejlijevom grafu $\mathrm{ICG}_n(1)$ jednak je $F_n(a-b)$, gde je $F_n(s)$ definisana sa*

$$F_n(s) = n \prod_{p|n,\ p\ prost} \left(1 - \frac{\varepsilon(p)}{p}\right), \qquad gde\ je \qquad \varepsilon(p) = \begin{cases} 1 & ako\ je \quad p \mid s \\ 2 & ako\ je \quad p \nmid s \end{cases}$$

Dokaz. Neka su $p_1, p_2, \dots, p_k$ različiti prosti brojevi broja n, pri čemu je $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}$ i $m = p_1p_2 \dots p_k$ najveći square free broj koji deli n.

Neka su a i b čvorovi grafa $\mathrm{ICG}_n(1)$ takvi da je $a > b$ i $s = a-b$. Tada postoji čvor c susedan čvorovima a i b, ako postoje $x = |a - c|$ i $y = |b - c|$ takvi da je $\gcd(x, n) = \gcd(y, n) = 1$ i

$$x + y \equiv s \mod n. \tag{3.11}$$

Primetimo da je $\gcd(x, n) = 1$ ako i samo ako je $\gcd(x, m) = 1$. Poslednje tvrđenje je ekvivalento činjenici da je $x \not\equiv 0 \mod p_i$, za svako $1 \le i \le k$. Isto važi i za y, to jest $y \not\equiv 0 \mod p_i$, za svako $1 \le i \le k$. Kako je sa druge strane i $y \equiv s - x \mod n$, to dobijamo da

postoji čvor c susedan čvorovima a i b ako i samo ako postoji x koji je rešenje sledećeg sistema kongruencija

$$x \not\equiv 0, s \mod p_i$$

za svako $1 \leq i \leq k$. Na osnovu Kineske teoreme o ostacima imamo da ukoliko postoji rešenje ovog sistema, ono je jedinstveno po modulo m. Broj mogućnosti za $x_i \notin \{0, s\}$, gde je $x \equiv x_i \mod p_i$ jednak je $p_i - 1$ ako $p_i \mid s$ ili $p_i - 2$ ako $p_i \nmid s$. To znači da je broj mogućih sistema jednak

$$(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2)) \dots (p_k - \varepsilon(p_k)),$$

pri čemu je rešenje sistema dato jedinstveno po modulo m. Dakle, traženi broj čvorova je

$$\frac{n}{m}(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2)) \dots (p_k - \varepsilon(p_k)),$$

što je upravo $F_n(s)$. □

Najpre ćemo odrediti kardinalnost grupe automorfizama $\mathrm{ICG}_n(1)$ kad je n stepen prostog broja.

Teorema 3.5.2. *Neka je $n = p^k$, gde je p prost broj i k prirodan. Tada je*

$$|Aut(\mathrm{ICG}_n(1))| = p! \left((p^{k-1})!\right)^p.$$

Dokaz. Neka su $C_0, C_1, \dots, C_{p-1}$ klase kongruencije brojeva od 0 do $n-1$, po modulu p

$$C_i = \{j \mid 0 \leq j < p^k,\ j \equiv i \mod p\}, \qquad 0 \leq i \leq p-1.$$

Dva čvora a i b grafa $\mathrm{ICG}_n(1)$ su susedna ako i samo ako je $\gcd(a-b, n) = \gcd(a-b, p^k) = 1$ ili ekvivalentno ukoliko $p \nmid (a-b)$. Ovo znači da su svi čvorovi iz klase C_i susedi sa čvorovima iz $X_n \setminus C_i$. Primetimo takođe da svaka klasa ima $|C_i| = \frac{n}{p} = p^{k-1}$ čvorova.

Neka je $f \in Aut(\mathrm{ICG}_n(1))$ proizvoljan automorfizam grafa $\mathrm{ICG}_n(1)$. Neka su a i b dva proizvoljna čvora iz iste klase C_i i neka je $f(a) \in C_j$, gde su $0 \leq i, j \leq p-1$. Odavde sledi da $p \mid a - b$, odakle imamo da su čvorovi a i b nesusedni, i zbog toga su takođe $f(a)$ i $f(b)$ nesusedni. Na osnovu pređašnjeg razmatranja, $f(a) - f(b)$ je deljivo sa p, te stoga zaključujemo da $f(b)$ pripada istoj klasi po modulu p kao i $f(a)$, tj. $f(b) \in C_j$. Odavde sledi da se čvorovi iz klase C_i preslikavanjem f slikaju u čvorove klase C_j. Kako smo odabrali proizvoljan indeks i, dobijamo da klase permutuju u odnosu na automorfizam f.

Pretpostavimo da se klasa C_i slika u klasu C_j. Kako je indukovani podgraf određen čvorovi klase C_i nezavisan skup i restrikcija automorfizma f na čvorovima klase C_i bijekcija iz C_i u C_j, to imamo $|C_i|! = (p^{k-1})!$ permutacija čvorova klase C_i. Kona'v cno, uzevši u obzir da klase permutuju nezavisno, koristeći pravilo proizvoda dobijamo da je broj automorfizama grafa $\mathrm{ICG}_n(1)$ jednak $p! \left((p^{k-1})!\right)^p$. □

Definišimo skupove

$$C_i^{(j)} = \{0 \leq a < n \mid a \equiv i \mod p_j\}, \qquad 1 \leq j \leq k, \qquad 0 \leq i < p_j.$$

Iz prethodnog poglavlja smo videli da je hromatski broj grafa $\mathrm{ICG}_n(1)$ jednak najmanjem prostom broju koji deli n i da je bojenje grafa $\mathrm{ICG}_n(1)$ jedinstveno, pri čemu su klase bojenja jednake klasama po modulu p_1. Ovo znači da su maksimalni nezavisni skupovi određeni klasama $C_0^{(1)}, C_1^{(1)}, \dots, C_{p_1-1}^{(1)}$ i da klase po modulu p_1 permutuju u odnosu na automorfizam f. Sledećom teoremom dokazujemo da za proizvoljan prost broj p koji deli n klase po modulu p permutuju u odnosu na automorfizam f.

Lema 3.5.3. *Za proizvoljan automorfizam f na* $\mathrm{ICG}_n(1)$ *i prost delilac p_i broja n važi:*

$$p_i \mid a-b \qquad \text{ako i samo ako} \qquad p_i \mid f(a)-f(b),$$

gde su $0 \leq a, b \leq n-1$ *i* $1 \leq i \leq k$.

Dokaz. Kako je f^{-1} automorfizam, dokazaćemo da za prost broj p_i koji deli n važi

$$p_i \mid a-b \qquad \Rightarrow \qquad p_i \mid f(a)-f(b),$$

a suprotan smer tvrđenja se svodi na ovaj smenom $a \mapsto f^{-1}(a)$ za $0 \leq a \leq n-1$.

Pretpostavimo da je tvrđenje leme nije zadovoljeno i neka je $2 \leq j \leq k$ najveći indeks takav da je $p_j \mid a-b$ i $p_j \nmid f(a)-f(b)$.

Najpre razmotrimo parove čvorova (a,b) oblika $(i, i+p_j)$ takve da $p_j \nmid f(i)-f(i+p_j)$, gde $0 \leq i \leq n-1-p_j$. Koristeći Teoremu **??** važi da je

$$N(i,i+p_j) = F_n(p_j) = (p_1-2)\cdot\ldots\cdot(p_{j-1}-2)(p_j-1)(p_{j+1}-2)\cdot\ldots\cdot(p_k-2)\cdot\frac{n}{p_1p_2\ldots p_k}.$$

Pošto $p_{j+1}, p_{j+2}, \ldots, p_k$ ne dele $f(i)-f(i+p_j)$ imamo takođe da je

$$N(f(i),f(i+p_j)) = (p_1-\varepsilon(p_1))\cdot\ldots\cdot(p_{j-1}-\varepsilon(p_{j-1}))(p_j-2)(p_{j+1}-2)\cdot\ldots\cdot(p_k-2)\cdot\frac{n}{p_1p_2\ldots p_k}.$$

Pošto f čuva broj zajedničkih suseda parova čvorova $(i, i+p_j)$ i $(f(i), f(i+p_j))$, to mora važiti jednakost $N(i,i+p_j) = N(f(i),f(i+p_j))$. Ako je $\varepsilon(p_1) = \varepsilon(p_2) = \ldots = \varepsilon(p_{j-1}) = 2$,

$$\frac{N(f(i),f(i+p_j))}{N(i,i+p_j)} = \frac{p_j-2}{p_j-1} < 1,$$

odakle dobijamo kontradikciju. To znači da postoji indeks $1 \leq s \leq j-1$, takav da je $\varepsilon(p_s) = 1$. Slično, imamo

$$\frac{N(f(i),f(i+p_j))}{N(i,i+p_j)} \geq \frac{(p_s-1)(p_j-2)}{(p_s-2)(p_j-1)} > 1,$$

pošto $p_s < p_j$. A odavde ponovo dobijamo kontradikciju, odakle sledi da $p_j \mid f(i)-f(i+p_j)$.

Za proizvoljne čvorove $a, b \in \mathrm{ICG}_n(1)$ takve da $p_j \mid a-b$ i $a < b$ je

$$p_j \mid (f(a)-f(a+p_j)) + (f(a+p_j)-f(a+2p_j)) + \ldots + (f(b-p_j)-f(b)) = f(a)-f(b),$$

i odakle konačno zaključujemo da klase po modulu p_j takođe permutuju u odnosu na automorfizam f. □

Teorema 3.5.4. *Neka je $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ kanonička reprezentacija broja n, gde je $p_1 < p_2 < \ldots < p_k$. Tada*

$$|Aut(\mathrm{ICG}_n(1))| = p_1!\cdot p_2!\cdot\ldots\cdot p_k!\cdot\left(\left(\frac{n}{p_1p_2\cdot\ldots\cdot p_k}\right)!\right)^{p_1p_2\cdot\ldots\cdot p_k}$$

Dokaz. Neka je $f \in Aut(\mathrm{ICG}_n(1))$ automorfizam grafa $\mathrm{ICG}_n(1)$ i $m = p_1p_2 \cdot \ldots \cdot p_k$ najveći delilac broja n koji ne sadrži kvadrate prostih brojeva. Dva čvora a i b iz $\mathrm{ICG}_n(1)$ su susedna ako i samo ako je $\gcd(a-b, m) = 1$.

Posmatrajmo klase $D_0, D_1, \ldots, D_{m-1}$, definisane sa

$$D_i = \{0 \leq a < n \mid a \equiv i \mod m\}.$$

Broj čvorova klase D_i jednak je $\frac{n}{m}$. Za proizvoljne čvorove $a, b \in D_i$ važi $m \mid a - b$, tako da je svaka klasa po modulu m nezavisan skup. Lemom **??**, imamo da je $f(a) - f(b)$ deljivo sa m odakle sledi da klase $D_0, D_1, \ldots, D_{m-1}$ permutuju u odnosu na automorfizam f. Neka su $a \in D_i$ i $b \in D_j$ dva proizvoljna čvora iz različitih klasa. Oni su susedi ako i samo ako je

$$\gcd(m(k-l) + (i-j), n) = 1$$

za neke $0 \leq k, l \leq \frac{n}{m} - 1$. Takođe, ako je $i - j$ relativno prost sa n, čvorovi iz klasa D_i i D_j formiraju kompletan bipartitan podgraf grafa $\mathrm{ICG}_n(1)$. U suprotnom, čvorovi iz klasa D_i i D_j formiraju nezavisan skup. Kako klase $\{D_0, D_1, \ldots, D_{m-1}\}$ permutuju u odnosu na automorfizam f tj. $f(D_i) = D_j$, to znači da postoji tačno $(\frac{n}{m})!$ mogućnosti za restrikciju preslikavanja f iz D_i na čvorove u D_j.

U nastavku ćemo prebrojati sve permutacije klasa D_i. Neka je i proizvoljan indeks takav da je $0 \leq i \leq m-1$, i neka $i_1, i_2, \ldots, i_k$ ostatak od i pri deljenju sa $p_1, p_2, \ldots, p_k$, redom. Za svaki $1 \leq s \leq k$, imamo $D_i \subseteq C_{i_s}^{(s)}$ odakle sledi

$$D_i \subseteq C_{i_1}^{(1)} \cap C_{i_2}^{(2)} \cap \ldots \cap C_{i_k}^{(k)}.$$

Sa druge strane, posmatrajmo sledeći sistem kongruencija u odnosu na ove indekse $i_1, i_2, \ldots, i_k$,

$$\begin{aligned} x &\equiv i_1 \mod p_1 \\ x &\equiv i_2 \mod p_2 \\ &\ldots \\ x &\equiv i_k \mod p_k. \end{aligned}$$

Prema Kineskoj teoremi o ostacima važi da postoji jedinstveno rešenje i sistema, takvo da je $0 \leq i < m = p_1p_2 \cdot \ldots \cdot p_k$ i

$$C_{i_1}^{(1)} \cap C_{i_2}^{(2)} \cap \ldots \cap C_{i_k}^{(k)} \subseteq D_i.$$

Konačno zaključujemo $D_i = C_{i_1}^{(1)} \cap C_{i_2}^{(2)} \cap \ldots \cap C_{i_k}^{(k)}$.

Koristeći Lemu **??**, za svaki prost broj p_s, $1 \leq s \leq k$, automorfizam f permutuje klase $C_0^{(s)}, C_1^{(s)}, \ldots, C_{p_s-1}^{(s)}$. Tada postoje indeksi $j_1, j_2, \ldots, j_k$ gde $0 \leq j_s < p_s$, $1 \leq s \leq k$, takvi da je $f(C_{i_s}^{(s)}) = C_{j_s}^{(s)}$. Kako je f bijekcija imamo

$$f(C_{i_1}^{(1)} \cap C_{i_2}^{(2)} \cap \ldots \cap C_{i_k}^{(k)}) = f(C_{i_1}^{(1)}) \cap f(C_{i_2}^{(2)}) \cap \ldots \cap f(C_{i_k}^{(k)}),$$

i $f(D_i) = C_{j_1}^{(1)} \cap C_{j_2}^{(2)} \cap \ldots \cap C_{j_k}^{(k)} = D_j$. Ako sa h_s označimo permutaciju indekasa po modulu p_s, možemo konstruisati preslikavanje $f(D_i) \mapsto D_j$ ako i samo ako $h_s(i_s) = j_s$, za $s = 1, 2, \ldots, k$. To znači da je klasa $f(D_i)$ određena permutacijom klasa $C_{j_s}^{(s)}$ za svako $1 \leq s \leq k$. Kako su ove permutacije nezavisne, broj permutacija klasa D_i je ograničen proizvodom broja permutacija klasa $C_{j_s}^{(s)}$, što je $p_1! \cdot p_2! \cdot \ldots \cdot p_k!$.

Sada ćemo pokazati da su ovako konstruisana preslikavanja zaista automorfizmi. Naime, za proizvoljne klase $D_{l'}$ i $D_{l''}$ postoje klase $D_{p(l')}$ i $D_{p(l'')}$ takve da je $f(D_{l'}) = D_{p(l')}$ i $f(D_{l''}) = D_{p(l'')}$, za neku permutaciju p indekasa $0, 1, \ldots, m-1$. Permutacija $p(l)$ odgovara rešenju sledećeg sistema kongruencija, gde h_i predstavljaju permutacije klasa $C_j^{(i)}$, $1 \leq i \leq k$ i $0 \leq j \leq p_i - 1$,

$$p(l) \equiv \sum_{i=1}^{k} c_{p_i} \cdot h_i(l_i) \mod m, \tag{3.12}$$

za svako $0 \leq l \leq m-1$ i $l_i \equiv l \mod p_i$ za $i = 1, 2, \ldots, k$. Konstante c_{p_i} su rešenja sistema sledećeg sistema od k kongruencija

$$\begin{aligned} c_{p_i} &\equiv 1 \mod p_i \\ c_{p_i} &\equiv 0 \mod p_j, \qquad 1 \leq j \leq k,\ j \neq i. \end{aligned}$$

Primetimo da forma rešenja (**??**) direktno sledi iz Kineske teoreme o ostacima, i na osnovu toga imamo

$$\begin{aligned} \gcd(p(l') - p(l''), n) = 1 \qquad &\Leftrightarrow \qquad \gcd\left(\sum_{i=1}^{k} c_{p_i} \cdot (h_i(l_i') - h_i(l_i'')), n\right) = 1 \\ &\Leftrightarrow \qquad p_i \nmid h_i(l_i') - h_i(l_i''), \quad i = 1, 2, \ldots, k \\ &\Leftrightarrow \qquad p_i \nmid l_i' - l_i'', \quad i = 1, 2, \ldots, k \\ &\Leftrightarrow \qquad \gcd\left(\sum_{i=1}^{k} c_{p_i} \cdot (l_i' - l_i''), n\right) = 1 \\ &\Leftrightarrow \qquad \gcd\left(l' - l'', n\right) = 1. \end{aligned}$$

Odavde zaključujemo da je tačno $p_1! \cdot p_2! \cdot \ldots \cdot p_k!$ mogućnosti za permutovanje klasa $\{D_0, D_1, \ldots, D_{m-1}\}$. Kako se čvorovi jedne klase slikaju bez ikakvih restrikcija u čvorove druge klase, korišćenjem pravila proizvoda, veličina grupe automorfizama grafa $\mathrm{ICG}_n(1)$ jednaka je

$$p_1! \cdot p_2! \cdot \ldots \cdot p_k! \cdot \left(\left(\frac{n}{m}\right)!\right)^m.$$

□

Neka je S_n grupa permutacija (simetrična grupa) stepena n. Više materijala o grupama permutacija može se naći u [**?**]. Primetimo da za prost broj p, graf $\mathrm{ICG}_p(1)$ je izomorfan kompletnom grafu K_p i zato je $Aut(\mathrm{ICG}_p(1)) = S_p$. Takođe, permutacije klasa po modulu m, čine grupu $S_{p_1} \times S_{p_2} \times \ldots \times S_{p_k}$.

Prema konstrukciji automorfizama za $\mathrm{ICG}_n(1)$ datoj u Teoremi **??**, zaključujemo da za svaku permutaciju klasa po modulu m, postoji m permutacija čvorova u svakoj klasi. To znači da je grupa automorfizama izomorfna "wreath" proizvodu permutacione klasa po modulu m i permutacione grupe čvorova u svakoj od tih klasa. Na osnovu ovoga dobijamo

$$Aut(X_n) = (S_{p_1} \times S_{p_2} \times \ldots \times S_{p_k}) \wr S_{n/m}.$$

Teorema 3.5.5. *Za proizvoljan delilac d broja n i $n' = \frac{n}{d} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$ važi*

$$|Aut(\mathrm{ICG}_n(d))| = d! \cdot \left(q_1! \cdot q_2! \cdot \ldots \cdot q_l! \cdot \left(\left(\frac{n'}{q_1 q_2 \cdot \ldots \cdot q_l} \right)! \right)^{q_1 q_2 \cdot \ldots \cdot q_l} \right)^d .$$

Dokaz. Na osnovu Leme **??** graf $\mathrm{ICG}_n(d)$ se sastoji iz d povezanih komponenti $C_0, C_1, \ldots, C_{d-1}$ koje su izomorfne sa $\mathrm{ICG}_{n/d}(1)$. Pretpostavimo da je f automorfizam na $\mathrm{ICG}_n(d)$, i neka su a i b dva proizvoljna čvora iz komponente C_i, za $0 \leq i \leq d-1$. Kako su a i b povezani nekim putem P u C_i, dobijamo da su čvorovi $f(a)$ i $f(b)$ takođe povezani slikom $f(P)$ puta P. To znači da $f(a)$ i $f(b)$ pripadaju istoj komponenti C_j, gde $0 \leq j \leq d-1$. Neka je $m' = q_1 q_2 \cdot \ldots \cdot q_l$ najveći delilac broja n', koji nije deljiv kvadratom prostog broja. Kako je veličina grupe automorfizma svake klase C_i data Teoremom **??** i kako one permutuju odnosu na automorfizam f dobijamo da je veličina grupe automorfizama grafa $\mathrm{ICG}_n(d)$ jednaka

$$d! \cdot \left(q_1! \cdot q_2! \cdot \ldots \cdot q_l! \cdot \left(\left(\frac{n'}{m'} \right)! \right)^{m'} \right)^d .$$

□

Sledeći konstrukcije automorfizama u Teoremama **??** i **??** važi

$$Aut(\mathrm{ICG}_n(d)) = S_d \wr Aut(\mathrm{ICG}_{\frac{n}{d}}(1)).$$

Za proizvoljne $a, b \in Z_n$, u radu [**?**] je definisan koncept afinih transformacija na čvorovima grafa

$$\psi_{a,b} : Z_n \to Z_n \qquad \text{gde je} \qquad \psi_{a,b}(x) = ax + b \mod n \qquad \text{for } x \in Z_n.$$

Lako se uočava da je $\psi_{a,b}$ automorfizam grafa $\mathrm{ICG}_n(1)$ ako i samo ako je $\gcd(a, n) = 1$. Takođe, $A(\mathrm{ICG}_n(1)) = \{\psi_{a,b} \mid a \in U_n, b \in Z_n\}$ je podgrupa grupe automorfizama $Aut(\mathrm{ICG}_n(1))$, gde je U_n skup svih invertibilnih elemenata u Z_n. Grupu $A(\mathrm{ICG}_n(1))$ nazivamo grupom afinih automorfizama grafa $\mathrm{ICG}_n(1)$ i očigledno je

$$|A(\mathrm{ICG}_n(1))| = n \cdot \varphi(n).$$

Kao motivacija za određivanje odnosa veličina grupe automorfizama i grupe afinih transformacija, poslužio nam je otvoreni problem postovljen u radu [**?**]. Naime, može se dokazati da je $|A(\mathrm{ICG}_n(1))| \leq |Aut(\mathrm{ICG}_n(1))|$, gde je jednakost zadovoljena ako i samo ako $n \in \{2, 3, 4, 6\}$.

Posmatrajmo količnik

$$\frac{|Aut(X_n)|}{|A(X_n)|} = \frac{p_1! p_2! \cdot \ldots \cdot p_k!}{p_1 p_2 \cdot \ldots \cdot p_k \cdot (p_1 - 1)(p_2 - 1) \cdot \ldots \cdot (p_k - 1)} \cdot \left(\frac{(p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1})!}{p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}} \right)^2 \cdot ((p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1})!)^{p_1 p_2 \cdot \ldots \cdot p_k - 2}.$$

Prvi faktor $(p_1 - 2)!(p_2 - 2)! \cdot \ldots \cdot (p_k - 2)!$ je veći ili jednak 1. Pri tome, dostiže jednakost ako i samo ako su 2 i 3 jedini prosti faktori broja n. Drugi faktor $(p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} - 1)!$ je takođe veći ili jednak 1, gde se jednakost dostiže ako i samo ako je n proizvod različitih prostih brojeva ili dvostruki proizvod različitih prostih brojeva. Treći faktor $((p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1})!)^{p_1 p_2 \cdot \ldots \cdot p_k - 2}$ je veći ili jednak 1, gde je jednakost zadovoljena ako i samo ako je n proizvod različitih prostih brojeva, ili $k = 1$ i $p_1 = 2$. Iz prethodnog razmatranja sledi da je $|A(\mathrm{ICG}_n(1))| < |Aut(\mathrm{ICG}_n(1))|$ za $n = 5$ i $n > 6$.

3.5.2 Broj zajedničkih suseda parova čvorova u $\mathrm{ICG}_n(d_1, d_2)$

Neka je $d_1 = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ i $d_2 = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}$. Ako $p^\alpha \mid n$ i $p^{\alpha+1} \nmid n$, pisaćemo $p^\alpha \| n$, tj. α je najveći eksponent takav da p^α deli n. Takođe, dodefinišimo funkciju F_n tako da je $F_n(s) = 0$ ako s nije ceo broj.

Teorema 3.5.6. *Neka su $d_2 > d_1 \geq 1$ delioci broja n. Broj zajedničkih suseda različitih čvorova a i b u povezanom integralnom cirkularnom grafu $\mathrm{ICG}_n(d_1, d_2)$ jednak je*

$$F_{n/d_1}\left(\frac{b-a}{d_1}\right) + 2 \cdot \frac{n}{M} \cdot \prod_{p_i \nmid (b-a) d_1 d_2} (p_i - 2) \cdot \prod_{p_i \mid (b-a),\ p_i \nmid d_1 d_2} (p_i - 1) \cdot \prod_{p_i \mid d_1 d_2,\ \alpha_i \neq \beta_i,\ \alpha_i \neq \gamma_i} (p_i - 1),$$

ako je $\gcd(b-a, d_1) = \gcd(b-a, d_2) = 1$, *i*

$$F_{n/d_1}\left(\frac{b-a}{d_1}\right) + F_{n/d_2}\left(\frac{b-a}{d_2}\right)$$

u suprotnom, gde je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ i

$$M = \prod_{i=1}^{k} p_i^{\min(\max(\beta_i+1, \gamma_i+1), \alpha_i)}.$$

Dokaz. Neka je c zajednički sused čvorova a i b grafa $\mathrm{ICG}_n(d_1, d_2)$, gde je $\gcd(d_1, d_2) = 1$. Razlikujemo četiri slučaja u zavisnosti od boje kojom su obojene ivice (a, c) i (a, b).

Slučaj 1. $\gcd(a - c, n) = d_1$ i $\gcd(b - c, n) = d_1$

Odavde zaključujemo da je $b - a$ deljivo sa d_1 i iz Teoreme **??** imamo da je broj rešenja sistema

$$\gcd\left(\frac{a-c}{d_1}, \frac{n}{d_1}\right) = 1 \qquad \text{i} \qquad \gcd\left(\frac{b-c}{d_1}, \frac{n}{d_1}\right) = 1$$

jednak $F_{n/d_1}((b-a)/d_1)$.

Slučaj 2. $\gcd(a - c, n) = d_2$ i $gcd(b - c, n) = d_2$

Analogno Slučaju 1, imamo da je broj zajedničkih suseda $F_{n/d_1}((b-a)/d_2)$.

Slučaj 3. $\gcd(a - c, n) = d_1$ i $gcd(b - c, n) = d_2$

Neka je p proizvoljan prost delilac broja n. Kako su delioci d_1 i d_2 uzajamno prosti, p može da deli najviše jedan od delioca d_1 ili d_2.

Pretpostavimo najpre da p ne deli ni d_1 ni d_2. Odavde sledi

$$c \not\equiv a \mod p \qquad \text{and} \qquad c \not\equiv b \mod p$$

Ako $a \equiv b \mod p$, tada c može da uzme $p - 1$ moguću vrednost po modulu p; u suprotnom, imamo $p - 2$ mogućnosti za c po modulu p.

Pretpostavimo da $p^\beta \| d_1$. Odavde imamo da $p \nmid d_2$ odakle sledi da $p \nmid b - c$ i $a \not\equiv b \mod p$. Dalje, u ovom slučaju imamo

$$c \equiv a \mod p^\beta.$$

Ako $p^\beta \| n$, ova kongruencija je dovoljna za određivanje čvora c po modulu p^β. U suprotnom, moramo uzeti u obzir uslov da $a - c$ nije deljivo sa $p^{\beta+1}$, tj.

$$c \not\equiv a \mod p^{\beta+1}.$$

U oba slučaja, kako je $a \not\equiv b \mod p$ i $c \equiv a \mod p$ važi da $c \not\equiv b \mod p$. Zato imamo $p-1$ mogućnost za odabir broja c po modulu $p^{\beta+1}$ kada $p^{\beta+1} \mid n$ i jednu mogućnost u suprotnom.

Pretpostavimo sada da $p^{\gamma} \| d_2$. Analogno, ako $p^{\gamma+1}$ ne deli n, imamo tačno jednu mogućnost za odabir broja c po modulu p^{γ}; u suprotnom ako $p^{\gamma+1}$ deli n, imamo $p-1$ mogućnost za c po modulu $p^{\gamma+1}$.

Na osnovu Kineske teoreme o ostacima, dobijamo rešenje gornjeg sistema kongruencija po modulu M. Za porste brojeve p_i takve da je $\beta_i = \gamma_i = 0$ imamo $p_i \| M$. U suprotnom, ako je $\beta_i > 0$ ili $\gamma_i > 0$, imamo $p_i^{\min(\beta_i+1,\alpha)} \| M$ ili $p_i^{\min(\gamma_i+1,\alpha)} \| M$. Ako p_i ne deli d_1 i d_2, imamo $p_i - 2$ mogućnosti kada $p_i \nmid (b-a)$ i $p_i - 1$ mogućnost kada $p_i \mid (b-a)$. Za $\alpha_i = \beta_i$, imamo samo jednu mogućnost po modulu p^{β_i}, dok za $\alpha_i \neq \beta_i$ postoji $p-1$ mogućnost po modulu p^{β_i+1}. Analogno, dobijamo simetričan izraz za d_2.

Iz poslednjih razmatranja sledi da imamo

$$S = \prod_{p_i \nmid (b-a)d_1d_2} (p_i - 2) \cdot \prod_{p_i \mid (b-a),\ p_i \nmid d_1d_2} (p_i - 1) \cdot \prod_{p_i \mid d_1,\ \alpha_i \neq \beta_i} (p_i - 1) \cdot \prod_{p_i \mid d_2,\ \alpha_i \neq \gamma_i} (p_i - 1)$$

rešenja za c po modulu M, što znači da je $\frac{n}{M} \cdot S$ rešenja takvih da je $0 \leq c < n$.

Slučaj 4. $\gcd(a-c, n) = d_2$ i $\gcd(b-c, n) = d_1$

Analogno slučaju 3, imamo

$$S = \prod_{p_i \nmid (b-a)d_1d_2} (p_i - 2) \cdot \prod_{p_i \mid (b-a),\ p_i \nmid d_1d_2} (p_i - 1) \cdot \prod_{p_i \mid d_1d_2,\ \alpha_i \neq \beta_i,\ \alpha_i \neq \gamma_i} (p_i - 1)$$

rešenja za c.

Konačno nakon sabiranja svih izraza po slučajevima dobijamo fomulu za broj zajedničkih suseda za a i b. □

Ovaj rezultat se može uopštiti za proizvoljan integralni cirkularni graf $\mathrm{ICG}_n(d_1, d_2, \ldots, d_k)$.

3.5.3 Grupa automorfizama nekih klasa integralnih cirkularnih grafova

n je stepen prostog broja

Lema 3.5.7. *Neka je $n = p^k$ i $d = p^l$, gde je p neparan prost broj takav da je $2 \leq l < k$ i $D = \{1, d\}$. Za automorfizam f grafa $\mathrm{ICG}_n(1, d)$ važi*

$$p^s \mid a - b \qquad \text{ako i samo ako} \qquad p^s \mid f(a) - f(b),$$

gde $0 \leq a, b \leq n-1$ i $l \leq s \leq l+1$.

Dokaz. Neka su $0 \leq a, b \leq n-1$ dva čvora grafa $\mathrm{ICG}_n(1, d)$ takva da je $a = b + p^s$. Pretpostavimo da p^s ne deli $f(a) - f(b)$. Kako automorfizam f čuva broj zajedničkih suseda parova (a, b) i $(f(a), f(b))$, ove vrednosti moraju biti jednake. Prema Teoremi **??** broj zajedničkih suseda čvorova a i b dat je formulom:

$$N(a,b) = F_{p^k}(p^s) + F_{p^{k-l}}(p^{s-l}) = \begin{cases} p^{k-1}(p-1) + p^{k-l-1}(p-2), & s = l \\ p^{k-1}(p-1) + p^{k-l-1}(p-1), & s > l. \end{cases}$$

Slučaj 1. $s = l$.

Ako $p \mid f(a) - f(b)$, važi

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) = p^{k-1}(p-1) < N(a,b).$$

Ako $p \nmid f(a) - f(b)$, imamo

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) + 2 \cdot \frac{p^k}{p^{l+1}} \cdot (p-1) = p^{k-1}(p-2) + 2p^{k-l-1}(p-1),$$

odakle sledi $N(a,b) - N(f(a), f(b)) = p^{k-1} - p^{k-l} \geq 0$. Međutim, kako je $l > 1$, u oba slučaja imamo da je $N(f(a), f(b)) \neq N(a,b)$, što dovodi do kontradikcije i konačnog zaključka da $p^l \mid f(a) - f(b)$.

Slučaj 2. $s = l + 1$.

Pretpostavimo da $p^l \mid f(a) - f(b)$. Kako $p^{l+1} \nmid f(a) - f(b)$, imamo

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) + F_{p^{k-l}}\left(\frac{f(a) - f(b)}{p^l}\right) = p^{k-1}(p-1) + p^{k-l-1}(p-2)$$

i zato je $N(f(a), f(b)) < N(a,b)$.

Pretpostavimo da $p^l \nmid f(a) - f(b)$.

Ako $p \mid f(a) - f(b)$ onda je $N(f(a), f(b)) = F_n(f(a) - f(b)) = p^{k-1}(p-1) < N(a,b)$. Ako $p \nmid f(a) - f(b)$ onda

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) + 2\frac{p^k}{p^{l+1}} \cdot (p-1) = p^{k-1}(p-2) + 2p^{k-l-1}(p-1),$$

i $N(a,b) - N(f(a), f(b)) = p^{k-l-1}(p^l - p + 1) > 0$.

U oba slučaja važi da je $N(f(a), f(b)) \neq N(a,b)$, što je kontradikcija, odakle konačno dobijamo da $p^{l+1} \mid f(a) - f(b)$.

□

Teorema 3.5.8. *Neka je $n = p^k$ i $d = p^l$, gde je p neparan prost broj, $1 \leq l \leq k-1$ i $D = \{1, d\}$. Tada je*

$$|Aut(\mathrm{ICG}_n(D))| = \begin{cases} (p^2)! \cdot \left(p^{k-2}!\right)^{p^2} & ako\ l = 1; \\ (p^{l-1}!)^p \cdot (p!)^{p^l+1} \cdot (p^{k-l-1}!)^{p^{l+1}} & ako\ l > 1. \end{cases}$$

Dokaz. Neka je f automorfizam grafa $\mathrm{ICG}_n(1, d)$. Dva čvora a i b iz $\mathrm{ICG}_n(1, d)$ su susedna ako i samo ako $p \nmid (a - b)$ or $p^l \| a - b$. Razlikujemo tri slučaja u zavisnosti od odnosa između l i k.

Slučaj 1. $l = 1$.

Neka je $C_0, C_1, \ldots, C_{p^2-1}$ particija skupa $\{0, 1, \ldots, p^k - 1\}$ po modulu p^2. Lako se može proveriti da su dva proizvoljna čvora a i b iz različitih klasa susedna, jer p^2 ne deli $a - b$, pa je $\gcd(a - b, p^k) \in \{1, p\}$. Svaka klasa C_i, gde $0 \leq i \leq p^2 - 1$ predstavlja nezavisan skup, i zato klase C_i permutuju u odnosu na automorfizam f. Na osnovu pravila proizvoda, sledi

$$|Aut(\mathrm{ICG}_{p^k}(1, p))| = (p^2)! \cdot \left(p^{k-2}!\right)^{p^2}.$$

Slučaj 2. $3 \leq l+1 = k$.
Neka $\{C_i\}$ predstavlja particiju skupa čvorova $\mathrm{ICG}_n(D)$ datu sa

$$C_i = \{\ 0 \leq a < p^{l+1} \mid a \equiv i \mod p^l\}, \qquad 0 \leq i \leq p^l - 1.$$

Na osnovu Leme **??** ove klase permutuju u odnosu na automorfizam f. Za proizvoljne čvorove a i b iz iste klase C_i važi da $p^l \mid (a-b)$ gde $0 \leq (a-b)/p^l \leq p-1$, što znači da $p^{l+1} \nmid a-b$ tj. klasa C_i je klika. Ako su $a \in C_i$, $b \in C_j$ i $i \neq j$ onda $p^l \nmid a-b$. Dalje možemo zaključiti da u slučaju kada $p \mid i-j$, tada ne postoji ivica grafa koja spaja čvorove iz različitih klasa C_i i C_j; dok su u slučaju kada $p \nmid i-j$ klase C_i i C_j klike.

Na osnovu Teoreme **??**, broj permutacija klasa C_i jednak je

$$|Aut(\mathrm{ICG}_{p^l})| = p! \cdot (p^{l-1}!)^p,$$

a broj permutacija čvorova u klasi C_i je $|C_i|!$. Kako je veličina svake klase jednaka p, na osnovu pravila proizvoda, dobijamo

$$|Aut(\mathrm{ICG}_{p^{l+1}}(1,p^l))| = p!(p^{l-1}!)^p \cdot (p!)^{p^l} = (p^{l-1}!)^p \cdot (p!)^{p^l+1}.$$

Slučaj 3. $3 \leq l+1 < k$.
Neka $\{D_i\}$ predstavlja particiju skupa čvorova $\mathrm{ICG}_n(D)$ data sa,

$$D_i = \{\ 0 \leq a < p^k \mid a \equiv i \mod p^{l+1}\}, \qquad 0 \leq i \leq p^{l+1} - 1.$$

Kako je razlika dva čvora iz iste klase deljiva sa p^{l+1}, zaključujemo da ti čvorovi nisu susedi. Dakle, klase D_i su nezavisni skupovi.

Čvorovi $a \in D_i$ i $b \in D_j$, $i \neq j$, su susedi ako i samo ako

$$gcd(i-j, p^k) \in \{1, p^l\} \qquad \Leftrightarrow \qquad gcd(i-j, p^{l+1}) \in \{1, p^l\}.$$

Koristeći Lemu **??**, klase D_i permutuju u odnosu na automorfizam f. Tada, koristeći Slučaj 2 broj permutacija klasa D_i jednak je kardinalnosti grupe automorfizama $|Aut(\mathrm{ICG}_{p^{l+1}}(1,p^l))|$. Konačno, kako je broj permutacija čvorova svake klase jednak $|D_i|!$, to na osnovu pravila proizvoda dobijamo

$$|Aut(\mathrm{ICG}_{p^k}(1,p^l))| = |Aut(\mathrm{ICG}_{p^{l+1}}(1,p^l))| \cdot (p^{k-l-1}!)^{p^{l+1}} = (p^{l-1}!)^p \cdot (p!)^{p^l+1} \cdot (p^{k-l-1}!)^{p^{l+1}}.$$

□

Prema konstrukciji automorfizama grafa $\mathrm{ICG}_n(D)$ u Teoremi **??**, zaključujemo da za svaku permutaciju klasa D_i po modulu p^{l+1}, postoji p^{l+1} permutacija čvorova u svakoj klasi (Slučaj 3). Ovo znači da je grupa automorfizama izomorfna "wreath" proizvodu permutacione grupe klasa po modulu p^{l+1} i permutacione grupe čvorova u svakoj od tih klasa

$$Aut(\mathrm{ICG}_{p^k}(1,p^l)) = Aut(\mathrm{ICG}_{p^{l+1}}(1,p^l)) \wr S_{p^{k-l-1}}.$$

Daljim razmatranjem, na osnovu Slučaja 2, grupa automorfizama klasa po modulu p^{l+1} je izomorfna "wreath" proizvodu grupe permutacija klasa C_i i grupe permutacija čvorova u svakoj toj klasi

$$Aut(\mathrm{ICG}_{p^{l+1}}(1,p^l)) = Aut(\mathrm{ICG}_{p^l}) \wr S_p.$$

Korišćenjem Teoreme **??** imamo

$$Aut(\mathrm{ICG}_{p^l}) = S_p \wr S_{p^{l-1}},$$

i konačno

$$Aut(\mathrm{ICG}_{p^k}(1, p^l)) = ((S_p \wr S_{p^{l-1}}) \wr S_p) \wr S_{p^{k-l-1}}.$$

Poslednjim smo dali kompletnu karakterizaciju grupe automorfizama grafa $\mathrm{ICG}_n(D)$, gde je $n = p^k$ i $|D| \in \{1, 2\}$. Primetimo da je u ovim slučajevima grupa automorfizama "wreath" proizvod dve ili četiri simetričnih grupa. Ovaj rezultata poboljšava, na primer, Teoremu 6.2 datu u [**?**].

n je proizvod različitih prostih faktora

Lema 3.5.9. *Neka je n prirodan broj čija je kanonička reprezentacija proizvod različitih prostih brojeva, $p > 1$ proizvoljan prost delilac broja n i $2^m \| \frac{n}{p}$. Za proizvoljan automorfizam f grafa $\mathrm{ICG}_n(1, p)$ i prost broj $p_i \neq 2$ koji deli $\frac{n}{p}$ važi*

$$2^m p_i \mid a - b \qquad \textit{ako i samo ako} \qquad 2^m p_i \mid f(a) - f(b),$$

gde $0 \leq a, b \leq n - 1$ i $1 \leq i \leq k$.

Dokaz. Primetimo da je $m \in \{0, 1\}$, pošto je n proizvod različitih prostih delilaca.

Pretpostavimo najpre da je $\frac{n}{p}$ neparan.

Pokazaćemo da ako $p_i \mid a - b$ onda $p_i \mid f(a) - f(b)$. Neka je p_i najveći prsot delilac broja $\frac{n}{p}$ i neka je $a = b + p_i$. Pretpostavimo da p_i ne deli $f(a) - f(b)$. Kako automorfizam f čuva broj zajedničkih suseda parova (a, b) i $(f(a), f(b))$, ovi brojevi moraju biti jednaki. Po Teoremi **??** broj zajedničkih suseda čvorova a i b dat je formulom

$$N(a, b) = F_n(p_i) + 2(p_i - 1) \prod_{q \mid \frac{n}{p},\ q \neq p_i} (q - 2) = (p_i - 1) \cdot p \cdot \prod_{q \mid \frac{n}{p},\ q \neq p_i} (q - 2).$$

Razlikujemo dva slučaja u zavisnosti od najvećeg zajedničkog delioca brojeva $f(a) - f(b)$ i p.

Slučaj 1. $p \mid f(a) - f(b)$.
Prema Teoremi **??** broj zajedničkih suseda čvorova $f(a)$ i $f(b)$ je

$$N(f(a), f(b)) = F_n(f(a) - f(b)) + F_{\frac{n}{p}}\left(\frac{f(a) - f(b)}{p}\right) = (p_i - 2) \cdot p \cdot \prod_{q \mid \frac{n}{p},\ q \neq p_i} (q - \varepsilon(q)).$$

Ako je $\gcd(f(a) - f(b), \frac{n}{p}) > 1$, onda postoji prost broj r delitelj $f(a) - f(b)$ i $\frac{n}{p}$. Tada je količnik vrednosti $N(f(a), f(b))$ i $N(a, b)$ jednak

$$\frac{N(f(a), f(b))}{N(a, b)} = \frac{(p_i - 2)(r - 1)}{(p_i - 1)(r - 2)} \cdot \frac{\prod_{q \mid \frac{n}{p},\ q \neq p_i, r} (q - \varepsilon(q))}{\prod_{q \mid \frac{n}{p},\ q \neq p_i, r} (q - 2)} \cdot \frac{p}{p} > 1. \tag{3.13}$$

Očigledno je drugi faktor proizvoda veći ili jednak 1. Takođe, prvi faktor je veći od 1, jer je p_i najveći prost broj koji deli $\frac{n}{p}$ i $p_i > r$. Iz poslednje činjenice sledi da je $N(f(a), f(b)) > N(a, b)$, što je kontradikcija.

Pretpostavimo sada da je $\gcd(f(a)-f(b),\frac{n}{p})=1$. Količnik brojeva $N(f(a),f(b))$ i $N(a,b)$ je u ovom slučaju

$$\frac{N(f(a),f(b))}{N(a,b)}=\frac{(p_i-2)\cdot p}{(p_i-1)\cdot p}<1. \tag{3.14}$$

Primetimo da je količnik $N(f(a),f(b))$ i $N(a,b)$ definisan jer je u oba slučaja $\prod_{q|\frac{n}{p}}(q-2)\neq 0$, pošto je $\frac{n}{p}$ neaparno. Zato dobijamo kontradikciju, tj. $f(a)-f(b)$ je deljivo sa p_i.

Slučaj 2. $\gcd(f(a)-f(b),p)=1$.

Koristeći Teoremu **??** broj zajedničkih suseda čvorova $f(a)$ i $f(b)$ je

$$N(f(a),f(b))=F_n(f(b)-f(a))+2(p_i-2)\prod_{q|\frac{n}{p},\ q\neq p_i}(q-\varepsilon(q))=(p_i-2)\cdot p\cdot\prod_{q|\frac{n}{p},\ q\neq p_i}(q-\varepsilon(q)).$$

Slično kao u prethodnom slučaju, zaključujemo da je $N(f(a),f(b))\neq N(a,b)$, što je kontradikcija, to jest $p_i\mid f(a)-f(b)$.

Za proizvoljne čvorove $a,b\in \mathrm{ICG}_n$ takve da $p_i\mid a-b$ i $a<b$ imamo

$$p_i\mid (f(a)-f(a+p_i))+(f(a+p_i)-f(a+2p_i))+\ldots+(f(b-p_i)-f(b))=f(a)-f(b).$$

Zato zaključujemo da klase p_i permutuju u odnosu na automorfizam f.

Pretpostavimo sada da je $\frac{n}{p}$ paran.

Neka je p_i najveći prost faktor delitelj $\frac{n}{p}$ i izaberimo čvorove a i b takve da je $a=b+2p_i$. Pretpostavimo da $2p_i$ ne deli $f(a)-f(b)$. Kako $p\nmid 2p_i$, na osnovu Teoreme **??** broj zajedničkih suseda čvorova a i b dat je sledećim izrazom:

$$N(a,b)=F_n(2p_i)+2(p_i-1)\prod_{q|\frac{n}{p},\ q\neq 2,p_i}(q-2)=(p_i-1)\cdot p\cdot\prod_{q|\frac{n}{p},\ q\neq 2,p_i}(q-2)>0.$$

Takođe možemo razlikovati dva slučaja u zavisnosti od najvećeg zajedničkog delioca brojeva $f(a)-f(b)$ i p.

Slučaj 1. $p\mid f(a)-f(b)$.

Korišćenjem Teoreme **??** broj zajedničkih suseda čvorova $f(a)$ i $f(b)$ dat je formulom

$$N(f(a),f(b))=F_n(f(a)-f(b))+F_{\frac{n}{p}}\left(\frac{f(a)-f(b)}{p}\right)=(p_i-2)\cdot p\cdot\prod_{q|\frac{n}{p},\ q\neq p_i}(q-\varepsilon(q))$$

Ako je $f(a)-f(b)$ neparan, tada za svako $q=2$ imamo da je $q-\varepsilon(q)=0$ i $N(f(a),f(b))=0<N(a,b)$, odakle sledi kontradikcija. U suprotnom, ponovo zaključujemo da je $N(f(a),f(b))\neq N(a,b)$, pošto dobijamo iste formule za $N(f(a),f(b))$ kao u (**??**) i (**??**).

Slučaj 2. $\gcd(f(a)-f(b),p)=1$.

Po Teoremi **??** broj zajedničkih suseda čvorova $f(a)$ i $f(b)$ dat je sa

$$N(f(a),f(b))=F_n(f(b)-f(a))+2(p_i-2)\prod_{q|\frac{n}{p},\ q\neq p_i}(q-\varepsilon(q))=(p_i-2)\cdot p\cdot\prod_{q|\frac{n}{p},\ q\neq p_i}(q-\varepsilon(q)).$$

Ako je $f(a)-f(b)$ neparan, onda je $N(f(a),f(b))=0$, odakle sledi kontradikcija. U suprotnom, zaključujemo da je $N(f(a),f(b))\neq N(a,b)$, što je kontradikcija u oba slučaja i $2p_i$ deli $f(a)-f(b)$.

Za proizvoljne čvorove $a, b \in \mathrm{ICG}_n(1,p)$ takve da $2p_i \mid a-b$ i $a<b$ dobijamo

$$p_i \mid (f(a)-f(a+2p_i))+(f(a+2p_i)-f(a+4p_i))+\ldots+(f(b-2p_i)-f(b))=f(a)-f(b).$$

Poslednje implicira da klase po modulu $2p_i$ takođe permutuju u odnosu na automorfizam f.

Sada se može primeniti matematička indukcija po prostim deliocima broja $n = p_1p_2 \cdot \ldots \cdot p_k$, uzimajući ih u opadajućem poretku. Koristeći isti metod kao u prethodnom delu dokaza možemo dokazati da za proizvoljno p_i važi, da ukoliko $2^m p_i \mid a-b$ onda $2^m p_i \mid f(a)-f(b)$ (u svim formulama za broj zajedničkih suseda od $f(a)$ i $f(b)$ imaćemo da je $\varepsilon(q)=1$ za svako $q > p_i$).

Kako je f^{-1} takođe automorfizam, suprotan smer tvrđenja sledi direktno, čime je dokaz okončan. □

Teorema 3.5.10. *Neka je n prirodan broj koji nije deljiv kvadratom prostog broja i p proizvoljan delilac od n. Kardinalnst grupe automorfizama grafa* $\mathrm{ICG}_n(1,p)$ *jednaka je*

$$|Aut(\mathrm{ICG}_n(1,p))| = \prod_{q|\frac{n}{p},\ q\ prime} q! \cdot (p!)^{\frac{n}{p}}.$$

Dokaz. Neka je $f \in Aut(\mathrm{ICG}_n(1,p))$. Definišimo skupove C_i na sledeći način:

$$C_i = \{0 \le a \le n-1 \mid a \equiv i \mod \frac{n}{p}\}$$

za $0 \le i \le \frac{n}{p}-1$. Na osnovu Leme **??**, klase C_i permutuju u odnosu na automorfizam f, jer važi

$$\frac{n}{p} \mid a-b \quad \Leftrightarrow \quad \frac{n}{p} \mid f(a)-f(b)$$

za svaka dva čvora $0 \le a, b \le n-1$. U specijalnom slučaju $n = 2p$, graf je bipartitan pa klase C_0 i C_1 permutuju u odnosu na automorfizam f. Zato za svaku klasu C_i postoji klasa $C_{h(i)}$ takva da je $f(C_i) = C_{h(i)}$, za neku permutaciju h indekasa $0, 1, \ldots, \frac{n}{p}-1$. Čvorovi $a \in C_i$ i $b \in C_j$ su susedni ako i samo ako

$$\gcd\left(\frac{n}{p}(k-l)+(i-j), n\right) \in \{1, p\}$$

za neko $0 \le k, l \le p-1$. Odavde sledi da ivica $\{a, b\}$ postoji samo ako su $i-j$ i $\frac{n}{p}$ uzajamno prosti. Na isti način, možemo uočiti da čvorovi iz iste klase predstavljaju nezavisan skup, jer za čvorove $a, b \in C_i$ važi $\frac{n}{p} \mid \gcd(a-b, n)$ i zato $\gcd(a-b, n) \notin \{1, p\}$.

Dakle, za C_i i C_j takve da je $\gcd(i-j, \frac{n}{p}) = 1$, i $a \in C_i$ i $b \in C_j$ imamo da $\frac{n}{p} \nmid \gcd(a-b, n)$ tako da $\gcd(a-b, n)$ može uzeti vrednosti 1 ili p. U oba slučaja a i b su susedni, tj. podgraf indukovan čvorovima iz klasa C_i i C_j je kompletan bipartitan podgraf.

Kako dalje imamo da struktura podgrafa indukovanog čvorovima iz C_i i C_j zavisi samo od razlike $i-j$, dobijamo da su svi takvi podgrafovi izomorfni jedni drugima za sve parove (i, j) takve da je $\gcd(i-j, \frac{n}{p}) = 1$. Isti zaključak stoji i za parove (i, j) takve da je $\gcd(i-j, \frac{n}{p}) \neq 1$, jer je u tom slučaju C_i i C_j čine nezavisan skup. Dalje, možemo konstruisati novi graf G' čiji je skup čvorova $Z_{n/p}$, a dva čvora i i j su susedna ako i samo ako klase C_i i C_j formiraju kompletan bipartitan graf. Odavde se jasno vidi da je G' izomorfan sa $\mathrm{ICG}_{n/p}(1)$ i pri tome

svaki čvor i odgovara klasi C_i. Konačno, prema Teoremi **??** broj permutacija ovih klasa jednak je $\prod_{q|n,\ q\neq p} q!$, što predstavlja kardinalnost grupe automorfizama unitarnog Kejlijevog grafa $Aut(\mathrm{ICG}_{n/p})$.

Pretpostavimo da se klasa C_i slika u klasu C_j. Kako čvorovi klase C_i formiraju nezavisan skup i restrikcija automorfizma f na čvorovima C_i je bijekcija iz C_i u C_j, to znači da je broj permutacija čvorova u klasi C_i upravo $|C_i|! = p!$. Kako klase i čvorovi permutuju nezavisno, korišćenjem pravila proizvoda veličina grupe automorfizama jednaka je

$$\prod_{q|\frac{n}{p}} q! \cdot (p!)^{\frac{n}{p}}.$$

□

Za ovu klasu grafova, grupa automorfizama predstavlja "wreath" proizvod grupe klasa permutacija C_i i simetrične grupe čvorova svake klase

$$Aut(\mathrm{ICG}_n(1,p)) = \Big(\prod_{q|\frac{n}{p}} S_q\Big) \wr S_p.$$

Iz dokaza prethodnih teorema vidi se da su oni zasnovani na tvrđenju da klase po modulu p permutuju u odnosu na automrfizam $f \in Aut(\mathrm{ICG}_n(D))$, za neki prost faktor p koji deli n. Takođe, permutacija klasa po prostom modulu je dokazana određivanjem broja zajedničkih suseda za proizvoljne čvorove u klasama. Ispostavilo se da je ideja prebrojavanja zajedničkih suseda suštinska, ali dokazi zahtevaju mnogo slučajeva. Sa druge strane primeri pokazuju da za proizvoljni integralni cirkularni graf $\mathrm{ICG}_n(D)$ i neki prost delilac p od n, klase permutuju u odnosu na automorfizam $f \in Aut(\mathrm{ICG}_n(D))$. Takođe se može zaključiti da grupe automorfizama predstavljaju dekartove ili wreath proizvode simetričnih grupa čiji je red, stepen prostog broja.

Glava 4

Bisimulacije na nedeterminističkim automatima

Centralno mesto ove glave predstavlja koncept simulacija i bisimulacija. Metode zasnovane na ovom konceptu pokazale su se kao veoma korisne u mnogim oblastima matematike i informatike, u modalnoj logici, teoriji konkurencije, teoriji skupova, u formalnoj teoriji verifikacija i proveri modela. Upotreba bisimulacija se uglavnom sastojala u modeliranju ekvivalencija na istom sistemu i redukovanju broja stanja tog sistema. Posebno su izučavani algoritmi koji nalaze najveću bisimilucionu ekvivalenciju na označenom grafu ili označenom tranzicionom sistemu. Takvi algoritmi su zasnovani na pronalaženju najveće bisimulacione ekvivalencije, što je ekvivalentno pronalaženju najgrublje particije (eng. relational coarsest partition problem) [**?**].

Najpre razmatramo koncept uniformnih relacija uveden kao način modeliranja ekvivalencija između stanja dva automata. Takođe definišemo koncept faktor automata u odnosu na proizvoljnu ekvivalenciju i dokazujemo dve teoreme koje predstavljaju verzije čuvenih teorema univerzalne algebre (za nedeterminističke automate): Druge teoreme o izomorfizmu i Teoreme o korespondenciji. Dalje proučavamo opšta svojstva direktnih i povratnih-direktnih bisimulacija. U slučaju kada postoji bar jedna direktna ili povratna-direktna bisimulacija, dokazujemo postojanje najveće, pri čemu je najveća direktna bisimulacija zapravo parcijalna uniformna relacija. Neka su data dva automata $\mathcal{A}$ i $\mathcal{B}$ i uniformna relacija φ između njihovih skupova stanja, tada pokazujemo da je $\varphi \subseteq A \times B$ direktna bisimulacija ako i samo ako su jezgro E_A^φ i kojezgro E_B^φ direktne bisimulacione ekvivalencije na $\mathcal{A}$ i $\mathcal{B}$, a funkcija $\widetilde{\varphi}$ indukovana sa φ izomorfizam između faktor automata $\mathcal{A}/E_A^\varphi$ i $\mathcal{B}/E_B^\varphi$. Na kraju glave, proučavamo slabe dirktne bisimulacije i dajemo analogne rezultate prethodnim rezultatima za bisimulacije. Napomenimo da su rezultati ove glave originalni i preuzeti su iz naših radova radova [**?**, **?**, **?**].

4.1 Uvodni pojmovi i notacija

Neka su A i B neprazni skupovi. Svaki podskup $R \subseteq A \times B$ se naziva *relacija iz A u B*. Jednakost, inkluzija, unija i presek relacija iz A u B se definišu kao iste operacije na podskupovima od $A \times B$. *Inverz* relacije $R \subseteq A \times B$ je relacija $R^{-1} \subseteq B \times A$ definisana kao $(b, a) \in R^{-1}$ ako i samo ako je $(a, b) \in R$, za svako $a \in A$ i $b \in B$. Ako je $A = B$, tj. ako je $R \subseteq A \times A$, tada je R *relacija na A*. Za relaciju $\varphi \subseteq A \times B$ definišemo podskup $\operatorname{Dom}\varphi$ od A i $\operatorname{Im}\varphi$ od B sa $\operatorname{Dom}\varphi = \{a \in A \mid (\exists b \in B)\,(a, b) \in \varphi\}$ i $\operatorname{Im}\varphi = \{b \in B \mid (\exists a \in A)\,(a, b) \in \varphi\}$. Podskup $\operatorname{Dom}\varphi$ nazivamo *domen* od φ, dok $\operatorname{Im}\varphi$ zovemo *slikom* od φ.

Za neprazne skupove A, B i C, i relacije $R \subseteq A \times B$ i $S \subseteq B \times C$, *kompozicija* relacija R i S je relacija $R \circ S \subseteq A \times C$ definisana sa

$$(a,c) \in (R \circ S) \iff (\exists b \in B)\big((a,b) \in R \wedge (b,c) \in S\big), \tag{4.1}$$

za svako $a \in A$ i $c \in C$. Za neprazne skupove A i B, relaciju $R \subseteq A \times B$ i podskupove $\alpha \subseteq A$ i $\beta \subseteq B$, definišimo skupove $\alpha \circ R \subseteq B$ i $R \circ \beta \subseteq A$ sa

$$b \in \alpha \circ R \iff (\exists a \in A)\big(a \in \alpha \wedge (a,b) \in R\big), \quad a \in R \circ \beta \iff (\exists b \in B)\big((a,b) \in R \wedge b \in \beta\big), \tag{4.2}$$

za svako $a \in A$ i $b \in B$. Da bi uprostili notaciju u nastavku, za neprazni skup A i podskupove $\alpha, \beta \subseteq A$ pisaćemo

$$\alpha \circ \beta = \begin{cases} 1 & \text{if } \alpha \cap \beta \neq \emptyset, \\ 0 & \text{if } \alpha \cap \beta = \emptyset, \end{cases} \tag{4.3}$$

tj., $\alpha \circ \beta$ je istinosna vrednost tvrđenja "$\alpha \cap \beta \neq \emptyset$".

Za neprazne skupove A, B, C i D, proizvoljne relacije $R \subseteq A \times B$, $S, S_1, S_2, S_i \subseteq B \times C$, gde je $i \in I$, i $T \subseteq C \times D$, kao i proizvoljne podskupove $\alpha \subseteq A$, $\beta \subseteq B$ i $\gamma \subseteq C$, važe sledeća tvrđenja:

$$(R \circ S) \circ T = R \circ (S \circ T), \tag{4.4}$$

$$\text{iz } S_1 \subseteq S_2 \text{ sledi } R \circ S_1 \subseteq R \circ S_2 \text{ and } S_1 \circ T \subseteq S_2 \circ T, \tag{4.5}$$

$$R \circ \big(\bigcup_{i \in I} S_i\big) = \bigcup_{i \in I} (R \circ S_i), \qquad \big(\bigcup_{i \in I} S_i\big) \circ T = \bigcup_{i \in I} (S_i \circ T) \tag{4.6}$$

$$(\alpha \circ R) \circ S = \alpha \circ (R \circ S), \qquad (\alpha \circ R) \circ \beta = \alpha \circ (R \circ \beta), \qquad (R \circ S) \circ \gamma = R \circ (S \circ \gamma), \tag{4.7}$$

$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}, \tag{4.8}$$

$$\text{iz } S_1 \subseteq S_2 \text{ sledi } S_1^{-1} \subseteq S_2^{-1}, \tag{4.9}$$

$$\alpha \circ R = R^{-1} \circ \alpha, \qquad R \circ \beta = \beta \circ R^{-1}. \tag{4.10}$$

Zaključujemo da se zagrade u (**??**) i (**??**) mogu izostaviti.

Primetimo da ako A, B i C predstavljaju konačne skupove kardinalnosti $|A| = k$, $|B| = m$ i $|C| = n$, onda R i S možemo smatrati $k \times m$ i $m \times n$ Bulovim matricama, a $R \circ S$ njihovim matričnim proizvodom. Štaviše, ako bi posmatrali α i β kao $1 \times k$ i $1 \times m$ Bulove matrice tj., smatrali ih Bulovim vektorima dužine k i m, onda bi $\alpha \circ R$ bio matrični proizvod α i R, a $R \circ \beta$ matrični proizvod R i β^t (transponovani vektor od β). Tada bi $\alpha \circ \beta$ bio skalarni proizvod vektora α i β.

Specijalne relacije na skupu A koje su vredne pažnje su *prazna relacija*, sa uobičajenom oznakom $\varnothing$, *relacija jednakosti* $\Delta_A = \{(x,x) \mid x \in A\}$, koja se takođe naziva i *dijagonala*, *identička relacija ili jednakost*, i *univerzalna* ili *puna relacija* $\nabla_A = A \times A$.

Posebno značajnu ulogu u daljem radu imaće *relacije ekvivalencije*. Neka je A neprazan skup. Relacija ξ na skupu A je:

- *refleksivna*, ako je $(a,a) \in \xi$, za svaki $a \in A$, tj. ako je $\Delta_A \subseteq \xi$;
- *simetrična*, ako za $a, b \in A$, iz $(a,b) \in \xi$ sledi $(b,a) \in \xi$, tj. ako je $\xi \subseteq \xi^{-1}$;
- *anti-simetrična*, ako za $a, b \in A$, iz $(a,b) \in \xi$ i $(b,a) \in \xi$ sledi da je $a = b$, tj. ako je $\xi \cap \xi^{-1} \subseteq \Delta_A$;

– *tranzitivna*, ako za $a, b, c \in A$, iz $(a, b) \in \xi$ i $(b, a) \in \xi$ sledi $(a, c) \in \xi$, tj. ako je $\xi \circ \xi \subseteq \xi$.

Refleksivnu, simetričnu i tranzitivnu relaciju nazivamo *relacija ekvivalencije*, ili jednostavno *ekvivalencija*. Sada ćemo se malo pozabaviti relacijama ekvivalencije. Neka je θ ekvivalencija na skupu A. Ako su elementi $a, b \in A$ u relaciji θ, tj. $(a, b) \in \theta$, tada kažemo i da su oni *ekvivalentni*. Skup θ_a nazivamo *klasa ekvivalencije* elementa $a \in A$ u odnosu na θ, ili kraće *θ-klasa* elementa a. Jasno je da je u tom slučaju $a \in \theta_a$. Skup svih θ-klasa označavaćemo sa A/θ ili A_θ i nazivaćemo ga *faktor skup* skupa A, ili prosto *faktor* skupa A, u odnosu na θ. Kadinalnost skupa A/θ, u oznaci $\mathrm{ind}(\theta)$, nazivamo *indeks* od θ. Preslikavanje

$$\theta^\natural : a \mapsto \theta_a$$

koje slika skup A na faktor skup A/θ nazivamo *prirodnim preslikavanjem* skupa A određenim ekvivalencijom θ. Sa druge strane, neka su A i B neprazni skupovi i $\phi : A \to B$. Relaciju

$$\ker \phi = \{(x, y) \in A \times A \mid \phi(x) = \phi(y)\}$$

na skupu A nazivamo *jezgrom preslikavanja ϕ*. Vezu između ekvivalencija i preslikavanja daje nam naredna teorema.

Teorema 4.1.1. *Neka je A neprazan skup. Ako je ϕ preslikavanje na skupu A u skup B, tada je $\ker \phi$ ekvivalencija na A. Osim toga, za proizvoljnu ekvivalenciju θ na A je $\ker(\theta^\natural) = \theta$.*

U narednim pasusima pozabavićemo se uređenim skupovima i mrežama.

Refleksivnu, antisimetričnu i tranzitivnu relaciju na skupu A nazivamo *parcijalnim uređenjem* na A, ili kraće samo *uređenjem* na A. Uređenja najčešće označavamo simbolom $\leq$. Par $(A, \leq)$ koji se sastoji od skupa A i parcijalnog uređenja $\leq$ na njemu nazivamo *parcijalno uređenim skupom*, ili kraće samo *uređenim skupom*. Jednostavnosti radi, umesto "$(A, \leq)$ je uređen skup" govorićemo "A je uređen skup", pri čemu ćemo podrazumevati da je uređenje na njemu označeno sa $\leq$. Ako je $\leq$ uređenje na skupu A, tada sa $<$ označavamo relaciju na A definisanu sa

$$a < b \text{ ako i samo ako je } a \leq b \text{ i } a \neq b,$$

a sa $\geq$ i $>$ označavamo inverzne relacije relacija $\leq$ i $<$, tim redom. Uređenje $\leq$ na A nazivamo *linearnim* ako za sve $a, b \in A$ važi $a \leq b$ ili $b \leq a$, i u tom slučaju kažemo da je A *linearno uređen skup* ili *lanac*.

Za preslikavanje ϕ koje slika uređen skup A u uređen skup B kažemo da je *izotono* ili *rastuće* ili da *očuvava uređenje* ako za sve $a, b \in A$, iz $a \leq b$ sledi $\phi(a) \leq \phi(b)$. Slično, za preslikavanje ϕ iz A u B kažemo da je *antitono* ili da je *opadajuće* ako za proizvoljne $a, b \in A$, iz $a \leq b$ sledi $\phi(b) \leq \phi(a)$. Za ϕ kažemo da je *izomorfizam uređenih skupova* A i B, ili *uređajni izomorfizam* iz A na B, ako je ϕ bijekcija iz A na B i ϕ i ϕ^{-1} su izotona preslikavanja.

Neka je A uređen skup. Za element $a \in A$ kažemo da je

– *minimalan element* skupa A, ako u A ne postoji element strogo manji od njega, tj. ako za svaki $x \in A$, iz $x \leq a$ sledi $x = a$;
– *maksimalan element* skupa A, ako u A ne postoji element strogo veći od njega, tj. ako za $x \in A$, iz $a \leq x$ sledi $a = x$;
– *najmanji element* skupa A, ako je manji od svakog drugog elementa iz A, tj. ako je $a \leq x$, za svaki $x \in A$;

– *najveći element* skupa A, ako je veći od svakog drugog elementa iz A, tj. ako je $x \leq a$, za svaki $x \in A$.

Neka je H neprazan podskup uređenog skupa A. Za element $a \in A$ kažemo da je

– *gornja granica* skupa H, ako je $x \leq a$, za svaki $x \in H$;
– *donja granica* skupa H, ako je $a \leq x$, za svaki $x \in H$;
– *najmanja gornja granica*, ili *supremum*, skupa H, ako je a najmanji element skupa svih gornjih granica skupa H, tj. ako je a gornja granica skupa H i za svaku gornju granicu b skupa H važi $a \leq b$;
– *najveća donja granica*, ili *infimum*, skupa H, ako je a najveći element skupa svih donjih granica skupa H, tj. ako je a donja granica skupa H i za svaku donju granicu b skupa H važi $b \leq a$.

Supremum skupa H, ako postoji, označavamo sa $\bigvee H$, a infimum, takođe ako postoji, sa $\bigwedge H$. Ukoliko je $H = \{x_i \mid i \in I\}$, tada umesto $\bigvee H$ i $\bigwedge H$ pišemo redom

$$\bigvee_{i \in I} x_i \qquad \text{i} \qquad \bigwedge_{i \in I} x_i.$$

Uređen skup čiji svaki dvoelementni podskup ima supremum i infimum nazivamo *mrežom*. Indukcijom se lako dokazuje da i svaki konačan podskup mreže ima supremum i infimum. Za beskonačne podskupove mreže to ne mora da važi. Ako je L mreža, tada se na L mogu definisati dve binarne operacije $\wedge$ i $\vee$ sa

$$\wedge : (a, b) \mapsto a \wedge b \qquad \text{i} \qquad \vee : (a, b) \mapsto a \vee b.$$

Po analogiji sa odgovarajućim operacijama na skupovima, operacije $\vee$ i $\wedge$ nazivaćemo, redom, *unijom* i *presekom*. Drugim rečima, govorićemo da je $\bigvee H$ *unija skupa* H a $a \vee b$ je *unija elemenata* a i b, i slično, da je $\bigwedge H$ *presek skupa* H, a $a \wedge b$ je *presek elemenata* a i b. Koristeći operacije unije i preseka, mrežu možemo definisati i kao univerzalnu algebru sa dve binarne operacije koje zadovoljavaju nekoliko specijalnih uslova. Naime, neposredno se dokazuje sledeća teorema.

Teorema 4.1.2. *Ako je L mreža, tada je $(L, \wedge, \vee)$ univerzalna algebra takva da za sve $x, y, z \in L$ važe sledeći uslovi:*

(L1) $x \wedge x = x$, $x \vee x = x$ (*idempotentnost*);
(L2) $x \wedge y = y \wedge x$, $x \vee y = y \vee x$ (*komutativnost*);
(L3) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$ (*asocijativnost*);
(L4) $x \wedge (x \vee y) = x$, $x \vee (x \wedge y) = x$ (*apsorpcija*).

Obratno, ako je L algebra sa dve binarne operacije $\wedge$ i $\vee$ koje zadovoljavaju uslove (L1)–(L4)*, tada je L mreža, u odnosu na parcijalno uređenje $\leq$ definisano sa*

$$a \leq b \iff a \wedge b = a \qquad (\textit{ili, ekvivalentno, } a \leq b \iff a \vee b = b).$$

Uslove (L1)–(L4) u Teoremi **??** nazivamo *aksiomama mreže*. Tretiranje mreže kao univerzalne algebre omogućava nam da kao i kod svake druge univerzalne algebre govorimo o *podmrežama*, kongruencijama, homomorfizmima, izomorfizmima, direktnim proizvodima mreža itd.

Neprazan podskup X mreže L naziva se *podmreža* mreže L ako za svaka dva elementa $a, b \in X$ važi $a \wedge b \in X$ i $a \vee b \in X$.

Za mrežu L i $a \in L$, podmreže

$$[a) = \{x \in L \mid a \leq x\} \qquad \text{i} \qquad (a] = \{x \in L \mid x \leq a\}$$

su *poluotvoreni intervali* mreže L, a za $a, b \in L$ takve da je $a \leq b$, podmreže

$$(a, b) = \{x \in L \mid a < x < b\} \qquad \text{i} \qquad [a, b] = \{x \in L \mid a \leq x \leq b\}$$

su *otvoreni interval* i *zatvoreni interval*, (ili *segment*) mreže L, tim redom.

Sistemi sa jednom binarnom idempotentnom, komutativnom i asocijativnom operacijom nazivaju se polumrežama. Ako neprazan skup L zajedno sa proizvoljnim elementima $a, b \in L$ sadrži i $a \wedge b$, odnosno $a \vee b$ onda se L naziva, redom $\wedge$-*polumreža* ili *donja polumreža*, tj. $\vee$-*polumreža* ili *gornja polumreža*.

4.2 Uniformne relacije

Neka je E ekvivalencija na skupu A. Sa E_a označimo klasu ekvivalencije elemenata $a \in A$ u odnosu na E, sa A/E odgovarajući faktor skup i sa $E^\natural$ prirodno preslikavanje iz A na A/E tj., preslikavanje dato sa $E^\natural(a) = E_a$, za svako $a \in A$.

Neka su A i B neprazni skupovi. Relacija $\varphi \subseteq A \times B$ se naziva *kompletna* ako za svako $a \in A$ postoji $b \in B$ tako da je $(a, b) \in \varphi$ i *sirjektivna* ako za svako $b \in B$ postoji $a \in A$ tako da je $(a, b) \in \varphi$. Primetimo da je φ kompletna ako i samo ako postoji funkcija $f : A \to B$ takva da je $(a, f(a)) \in \varphi$, za svako $a \in A$. Funkciju f sa ovim svojstvom nazvaćemo *funkcionalnim deskriptorom* relacije φ, a sa $FD(\varphi)$ označimo skup svih ovakvih funkcija. Za ekvivalenciju F skupa B, funkciju $f : A \to B$ nazivamo F-*sirjektivnom* ako za svako $b \in B$ postoji $a \in A$ tako da je $(f(a), b) \in F$. Drugim rečima, imamo da je f F-sirjektivna ako i samo ako je $f \circ F^\natural : A \to B/F$ sirjektivna funkcija.

Za relaciju $\varphi \subseteq A \times B$, gde su A i B neprazni skupovi, definišimo skupove φ_a i φ^b, na sledeći način:

$$\varphi_a = \{b \in B \mid (a, b) \in \varphi\}; \tag{4.11}$$
$$\varphi^b = \{a \in A \mid (a, b) \in \varphi\}, \tag{4.12}$$

za svako $a \in A$ i $b \in B$. Skup φ_a nazivamo φ-*afterset* od a, a skup φ^b, φ-*foreset* od b [**?**, **?**, **?**].

Takođe, relacije E^φ_A na A i E^φ_B na B definisane sa

$$(a_1, a_2) \in E^\varphi_A \iff (\forall b \in B)(\,(a_1, b) \in \varphi \iff (a_2, b) \in \varphi\,); \tag{4.13}$$
$$(b_1, b_2) \in E^\varphi_B \iff (\forall a \in A)(\,(a, b_1) \in \varphi \iff (a, b_2) \in \varphi\,), \tag{4.14}$$

za svako $a_1, a_2 \in A$ i $b_1, b_2 \in B$, nazivamo *jezgro*, i *kojezgro* relacije φ, redom. Koristeći gornju notaciju možemo pogodnije zapisati definicije jezgra i kojezgra na sledeći način

$$(a_1, a_2) \in E^\varphi_A \iff \varphi_{a_1} = \varphi_{a_2}; \tag{4.15}$$
$$(b_1, b_2) \in E^\varphi_B \iff \varphi^{b_1} = \varphi^{b_2}, \tag{4.16}$$

za svako $a_1, a_2 \in A$ i $b_1, b_2 \in B$

Neka su A i B neprazni skupovi. *Parcijalna uniformna relacija* iz A u B je relacija $\varphi \subseteq A \times B$ koja zadovoljava uslov

$$\varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset \Rightarrow \varphi_{a_1} = \varphi_{a_2}, \tag{4.17}$$

za svako $a_1, a_2 \in A$. Kompletna i sirjektivna parcijalna uniformna relacija se naziva *uniformnom relacijom*. Primetimo da je parcijalna uniformna relacija $\varphi \subseteq A \times B$ uniformna relacija definisana iz A' u B', gde je $A' = \{a \in A \mid (\exists b \in B)\,(a,b) \in \varphi\}$ (*domen* od φ) i $B' = \{b \in B \mid (\exists a \in A)\,(a,b) \in \varphi\}$ (*slika* od φ). Kako je uniformna relacija kompletna vidimo da se u ovom slučaju uslov (**??**) može zapisati kao

$$\varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset \Leftrightarrow (a_1, a_2) \in E_A^{\varphi}. \tag{4.18}$$

Parcijalne uniformne relacije i uniformne relacije predstavljaju krisp analogiju parcijalnih fazi funkcija i uniformnih fazi relacija [**?**]. Sledeće dve teoreme mogu biti izvedene i u fazi teoriji (Teoreme 3.1 i 3.3 [**?**]). Najpre ćemo dokazati pomoćno tvrđenje.

Lema 4.2.1. *Neka su A i B neprazni skupovi i relacija $\varphi \subseteq A \times B$. Tada za svako $a_1, a_2 \in A$ važi da je*

$$(a_1, a_2) \in \varphi \circ \varphi^{-1} \Leftrightarrow \varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset$$

Dokaz. Za $a_1, a_2 \in A$ imamo

$$\begin{aligned} (a_1, a_2) \in \varphi \circ \varphi^{-1} &\Leftrightarrow (\exists b \in B)\left((a_1, b) \in \varphi \wedge (b, a_1) \in \varphi^{-1}\right) \\ &\Leftrightarrow (\exists b \in B)\, b \in \varphi(a_1) \cap \varphi_{a_2} \\ &\Leftrightarrow \varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset. \end{aligned}$$

□

Teorema 4.2.2. *Neka su A i B neprazni skupovi i relacija $\varphi \subseteq A \times B$. Tada su sledeći uslovi ekvivalentni:*

(i) *φ je parcijalna uniformna relacija;*

(ii) *φ^{-1} je parcijalna uniformna relacija;*

(iii) *$\varphi \circ \varphi^{-1} \circ \varphi \subseteq \varphi$;*

(iv) *$\varphi^{-1} \circ \varphi \circ \varphi^{-1} \subseteq \varphi^{-1}$;*

(v) *$\varphi \circ \varphi^{-1} \subseteq E_A^{\varphi}$;*

(vi) *$\varphi^{-1} \circ \varphi \subseteq E_B^{\varphi}$.*

Dokaz. (iii) $\Longleftrightarrow$ (iv). Ova ekvivalencija je očigledna.

(i) $\Longrightarrow$ (iii). Neka je $(a,b) \in \varphi \circ \varphi^{-1} \circ \varphi$. Tada postoji $a_1 \in A$ tako da je $(a, a_1) \in \varphi \circ \varphi^{-1}$ i $(a_1, b) \in \varphi$. Na osnovu Leme **??** imamo da je poslednje ekvivalentno relacijama $\varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset$ i $b \in \varphi_{a_1}$. Kako je φ parcijalna uniformna relacija, koristeći (**??**), dobijamo da je $b \in \varphi_{a_1} = \varphi_a$, tj. $(a,b) \in \varphi$.

(iii) $\Longrightarrow$ (i). Neka je $\varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset$ i $b \in \varphi_{a_2}$. Iz Leme **??** dobijamo da je $(a_1, a_2) \in \varphi \circ \varphi^{-1}$ i $(a_2, b) \in \varphi$. Po definiciji kompozicije relacija imamo $(a_1, b) \in \varphi \circ \varphi^{-1} \circ \varphi = \varphi$, tj. $b \in \varphi_{a_1}$. Konačno zaključujemo da je $\varphi_{a_2} \subseteq \varphi_{a_1}$, pri čemu se obrat inkluzije slično dokazuje. Naime, za $b \in \varphi_{a_1}$ ili ekvivalentno $(b, a_1) \in \varphi^{-1}$, imamo da je $(a_2, b) \in \varphi^{-1} \circ \varphi \circ \varphi^{-1} = \varphi^{-1}$. Iz poslednje jednakosti sledi da je $b \in \varphi_{a_2}$, što je i trebalo dokazati.

(i)$\Longleftrightarrow$(v). Neka su a_1 i a_2 proizvoljni elementi skupa A. Tada iz Leme **??** imamo da je $(a_1, a_2) \in \varphi \circ \varphi^{-1} \Leftrightarrow \varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset$. Ukoliko je zadovoljen uslov (i) ((v)), dobijamo da je $(a_1, a_2) \in E_A^\varphi$, odakle sledi uslov (v) ((i)).

Slično možemo dokazati da je (ii) $\Longleftrightarrow$ (iv) $\Longleftrightarrow$ (vi), koristeći dokazanu činjenicu da je (i) $\Longleftrightarrow$ (iii) $\Longleftrightarrow$ (v), zamenom $\varphi \to \varphi^{-1}$. $\square$

Iz (iii) primećujemo da je φ parcijalna uniformna relacija ako i samo ako je $\varphi \circ \varphi^{-1} \circ \varphi = \varphi$, pošto obrnut smer uvek važi.

Ako je $\varphi \subseteq A \times B$ parcijalna uniformna relacija, onda se može lako pokazati da su $\varphi \circ \varphi^{-1}$ i $\varphi^{-1} \circ \varphi$ simetrične i tranzitivne relacije, ali u opštem slučaju ne moraju biti refleksivne. Naime, $\varphi \circ \varphi^{-1}$ je refleksivna ako i samo ako je φ kompletna, dok je $\varphi^{-1} \circ \varphi$ refleksivna ako i samo ako je φ sirjektivna. Zato, ako je φ uniformna relacija onda su obe relacije $\varphi \circ \varphi^{-1}$ i $\varphi^{-1} \circ \varphi$ ekvivalencije. Štaviše, važi sledeća teorema.

Teorema 4.2.3. *Neka su A i B neprazni skupovi i neka je $\varphi \subseteq A \times B$ data relacija. Tada su sledeći uslovi ekvivalentni:*

(i) *φ je uniformna relacija;*

(ii) *φ^{-1} je uniformna relacija;*

(iii) *φ je kompletna, sirjetivna i $\varphi \circ \varphi^{-1} \circ \varphi = \varphi$;*

(iv) *φ je kompletna, sirjetivna i $\varphi^{-1} \circ \varphi \circ \varphi^{-1} = \varphi^{-1}$;*

(v) *φ je sirjektivna i $\varphi \circ \varphi^{-1} = E_A^\varphi$;*

(vi) *φ je kompletna i $\varphi^{-1} \circ \varphi = E_B^\varphi$;*

(vii) *φ je kompletna i za sve $f \in FD(\varphi)$, $a \in A$ i $b \in B$, f je E_B^φ-sirjektivna i važi*

$$(a, b) \in \varphi \iff (f(a), b) \in E_B^\varphi; \tag{4.19}$$

(viii) *φ je kompletna i za sve $f \in FD(\varphi)$ i $a_1, a_2 \in A$, f je E_B^φ-sirjektivna i važi*

$$(a_1, f(a_2)) \in \varphi \iff (a_1, a_2) \in E_A^\varphi. \tag{4.20}$$

Dokaz.

(iii) $\Longleftrightarrow$ (iv). Ova ekvivalencija je očigledna.

(i) $\Longleftrightarrow$ (iii). Direkto sledi iz (i) $\Longleftrightarrow$ (iii) Teoreme **??**.

(i) $\Longrightarrow$ (v). Na osnovu smera (i) $\Longrightarrow$ (v) Teoreme **??** dovoljno je dokazati inkluziju $E_A^\varphi \subseteq \varphi \circ \varphi^{-1}$. Neka su $a_1, a_2 \in A$ proizvoljni elementi, takvi da je $(a_1, a_2) \in E_A^\varphi$. Kako je φ uniformma relacija, na osnovu (**??**) imamo da je $\varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset$. A poslednja nejednakost je ekvivalentna sa $(a_1, a_2) \in \varphi \circ \varphi^{-1}$ po Lemi **??**, što je trebalo dokazati.

(v) $\Longrightarrow$ (i). Iz Teoreme **??**, φ je parcijalna uniformna relacija, a prema pretpostavci je ona sirjektivna i $\varphi \circ \varphi^{-1} = E_A^\varphi$ refleksivna, odakle sledi da je φ kompletna.

(ii) $\Longleftrightarrow$ (iv) $\Longleftrightarrow$ (vi). Ovaj lanac ekvivalencija se dokazuje na isti način kao i lanac (i) $\Longleftrightarrow$ (iii) $\Longleftrightarrow$ (v).

(vi) $\Longrightarrow$ (vii). Neka je $f \in FD(\varphi)$, $a \in A$ i $b \in B$. Ako je $(a, b) \in \varphi$ i pošto je $(a, f(a)) \in \varphi$ dobijamo da je $(f(a), b) \in \varphi^{-1} \circ \varphi = E_B^\varphi$. Sa druge strane, ako je $(f(a), b) \in E_B^\varphi = \varphi^{-1} \circ \varphi$, onda na osnovu $(a, f(a)) \in \varphi$ sledi $(a, b) \in \varphi \circ \varphi^{-1} \circ \varphi = \varphi$. Prema prethodnom važi (**??**). Korišćenjem (**??**) i činjenice da je φ sirjektivna imamo da je f E_B^φ-sirjektivna.

(vii) $\Longrightarrow$ (vi). Iz E_B^φ-sirjektivnosti funkcije f i ekvivalencije (**??**) dobijamo da je φ sirjektivna. Neka je $(b_1, b_2) \in E_B^\varphi$. Tada postoji $a \in A$ tako da je $(f(a), b_1) \in E_B^\varphi$, pa je i $(f(a), b_2) \in E_B^\varphi$. Sada na osnovu (**??**) važi da je $(a, b_1) \in \varphi$ i $(a, b_2) \in \varphi$, odakle proizilazi $(b_1, b_2) \in \varphi^{-1} \circ \varphi$.

Obrnuto, neka je $(b_1, b_2) \in \varphi^{-1} \circ \varphi$. Tada postoji $a \in A$ takav da je $(a, b_1) \in \varphi$ i $(a, b_2) \in \varphi$, pa iz (**??**) sledi da je $(f(a), b_1) \in E_B^\varphi$ i $(f(a), b_2) \in E_B^\varphi$, odakle je konačno $(b_1, b_2) \in E_B^\varphi$.

(v) $\Longleftrightarrow$ (viii). Ova ekvivalencija se može dokazati slično ekvivalenciji (vi) $\Longleftrightarrow$ (vii).

□

Napomena 4.2.1. Naka su A i B neprazni skupovi i neka je φ parcijalna uniformna relacija iz A u B. Tada je φ uniformna relacija iz $\operatorname{Dom}\varphi$ u $\operatorname{Im}\varphi$, pa je iz tog razloga opravdan naziv parcijalna uniformna relacija.

Uniformne relacije možemo shvatiti kao usmereni bipartitan graf čiji je skup čvorova $A \cup B$ i skup ivica φ. Particije grafa su skupovi A i B, pri čemu su ivice usmerene iz čvorova u A ka čvorovima u B. Izlazni stepen čvorova u A, kao i ulazni stepen čvorova iz B mora biti veći ili jednak jedinici (φ je kompletna i sirjektivna). Takođe, svaka dva čvora $a_1, a_2 \in A$ imaju isti skup suseda u B, tj. $N(a_1) = N(a_2)$.

Lako je proveriti da je svaka ekvivalencija i svaka sirjektivna funkcija uniformna relacija, a da je svaka funkcija parcijalna uniformna relacija. Ovo potvrđuje komentar dat u uvodu da uniformne relacije predstavljaju zajedničko uopštenje (sirjektivnih) funkcija i relacija ekvivalencije.

Teorema 4.2.4. *Neka su A i B neprazni skupovi i neka je E ekvivalencija na A i F ekvivalencija na B. Tada postoji uniformna relacija $\varphi \subseteq A \times B$ takva da je $E = E_A^\varphi$ i $F = E_B^\varphi$ ako i samo ako postoji bijektivno preslikavanje $\phi : A/E \to B/F$.*

Ovo bijektivno preslikavanje se može pretstaviti kao $\phi = \widetilde{\varphi}$, gde je $\widetilde{\varphi} : A/E \to B/F$ funkcija definisana sa

$$\widetilde{\varphi}(E_a) = F_{f(a)}, \quad \text{za svako } a \in A \text{ i } f \in FD(\varphi). \tag{4.21}$$

Takođe važi da je $(\widetilde{\varphi})^{-1} = \widetilde{\varphi^{-1}}$.

Dokaz. Neka je $\varphi \subseteq A \times B$ uniformna relacija takva da je $E = E_A^\varphi$ i $F = E_B^\varphi$.

Prvo ćemo pokazati da je funkcija $\widetilde{\varphi} : A/E \to B/F$ data relacijom (**??**) dobro definisana, tj. da ne zavisi od izbora $f \in FD(\varphi)$ i $a \in A$. Zaista, na osnovu (**??**) i (**??**), za ma koje $a_1, a_2 \in A$ i $f_1, f_2 \in FD(\varphi)$ imamo

$$\begin{aligned} E_{a_1} = E_{a_2} \quad &\Longleftrightarrow \quad (a_1, a_2) \in E \quad \Longleftrightarrow \quad (a_1, f_2(a_2)) \in \varphi \quad \Longleftrightarrow \quad (f_1(a_1), f_2(a_2)) \in F \\ &\Longleftrightarrow \quad F_{f_1(a_1)} = F_{f_2(a_2)}. \end{aligned}$$

Ovim smo dokazali da je $\widetilde{\varphi}$ dobro definisana i ujedno injektivna. Dalje, prema Teoremi **??** (v) i (vi), svako $f \in FD(\varphi)$ je F-sirjektivno preslikavanje, pa je $\widetilde{\varphi}$ sirjektivno. Konačno zaključujemo da je $\widetilde{\varphi}$ bijekcija.

Obrnuto, neka je $\phi : A/E \to B/F$ bijekcija. Definišimo $\varphi \subseteq A \times B$ sa

$$(a, b) \in \varphi \quad \Longleftrightarrow \quad \phi(E_a) = F_b, \quad \text{za svako } a \in A \text{ i } b \in B. \tag{4.22}$$

Očigledno je φ kompletna i sirjektivna. Takođe je jasno da se za proizvoljne $a_1, a_2 \in A$ i $b \in B$, definicija (**??**) može zapisati kao $b \in \varphi_{a_1} \iff \phi(E_{a_1}) = F_b$ i $b \in \varphi_{a_2} \iff \phi(E_{a_2}) = F_b$. Odavde direktno zaključujemo da je

$$\begin{aligned} \varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset &\iff \phi(E_{a_1}) = \phi(E_{a_2}) \\ \varphi_{a_1} = \varphi_{a_2} &\iff \phi(E_{a_1}) = \phi(E_{a_2}). \end{aligned}$$

Na osnovu (**??**) dobijamo da je φ uniformna relacija, jer važi $\varphi_{a_1} \cap \varphi_{a_2} \neq \emptyset \Leftrightarrow \varphi_{a_1} = \varphi_{a_2}$.

Dalje, na osnovu (**??**), za proizvoljne $a_1, a_2 \in A$ imamo da je

$$(a_1, a_2) \in E_A^{\varphi} \iff \varphi_{a_1} = \varphi_{a_2} \iff \phi(E_{a_1}) = \phi(E_{a_2}) \iff E_{a_1} = E_{a_2} \iff (a_1, a_2) \in E,$$

te je zato $E_A^{\varphi} = E$. Takođe je i $E_B^{\varphi} = F$.

Konačno, za svako $a \in A$ i $f \in FD(\varphi)$, iz $(a, f(a)) \in \varphi$ i (**??**) sledi da je $\phi(E_a) = F_{f(a)} = \widetilde{\varphi}(E_a)$, pa je $\phi = \widetilde{\varphi}$. Takođe se lako može pokazati da je $(\widetilde{\varphi})^{-1} = \widetilde{\varphi^{-1}}$. □

Primetimo da bijektivna funkcija $\widetilde{\varphi}$ iz Teoreme **??** određuje neku vrstu "uniformnosti" među participajama koje odgovaraju ekvivalencijama E i F. Ovo je još jedan razlog zbog kojeg koristimo naziv uniformna relacija. Takođe, u grafovskom smislu ovaj rezultat možemo interpretirati na sledeći način: graf uniformne relacije predstavlja uniju kompletnih komponeneti u participajama A i B (klase ekvivalencije E_a i F_b), pri čemu postoji savršeno sparivanje (perfect matching, 1-faktor), definisano preslikavanjem $\widetilde{\varphi}$.

4.3 Nedeterministički automati i faktor automati

U daljem razmatranju, ukoliko nije drugačije rečeno, sa X ćemo označiti konačan neprazan skup, koji zovemo *alfabet* (ili *ulazni alfabet*). *Nedeterministički automat* nad alfabetom X se definiše kao uređena četvorka $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$, gde je A neprazan skup, koji zovemo *skupom stanja*, zatim $\delta^A \subseteq A \times X \times A$ ternarna relacija, koju zovemo *tranziciona relacija (funkcija prelaza)* i σ^A i τ^A podskupovi od A, koje zovemo respektivno skupovima *inicijalnih stanja* i *završnih stanja*. Za svako $x \in X$, definišimo binarnu relaciju $\delta_x^A \subseteq A \times A$ sa

$$(a, b) \in \delta_x^A \iff (a, x, b) \in \delta^A, \quad \text{za svako } a, b \in A,$$

koju takođe nazivamo *tranzicionom relacijom*. Za datu reč $u \in X^*$, gde je X^* slobodan monoid nad skupom X, možemo dodefinisati tranzicionu relaciju $\delta_u^A \subseteq A \times A$ induktivno, na sledeći način: za praznu reč $\varepsilon \in X^*$ definišimo δ_ε^A kao relaciju jednakosti, a za svako $u, v \in X^*$ stavimo da je $\delta_{uv}^A = \delta_u^A \circ \delta_v^A$. Ako zanemarimo inicijalna i završna stanja, onda uređeni par $\mathcal{A} = (A, \delta^A)$ nazivamo *označenim tranzicionim sistemom* nad X ([**?**, **?**]). Najčešće se pretpostavlja da su skup stanja i ulazni alfabet nedeterminističkih automata konačni. Ovakva pretpostavka ovde nije neophodna, mada ćemo pretpostaviti da je ulazni alfabet konačan, a iz metodoloških razloga, u nekim slučajevima dopustićemo da je skup stanaja beskonačan. Nedeterministički automat čiji je skup stanja konačan nazivamo *konačan nedeterministički automat*. Ako je $\sigma^A = \{a_0\}$, za neko $a_0 \in A$, i δ^A funkcija iz $A \times X$ u A, tj. za svako $(a, x) \in A \times X$ postoji jedinstveno $a' \in A$ takvo da je $(a, x, a') \in \delta^A$, onda $\mathcal{A}$ nazivamo *determinističkim automatom* i zapisujemo $\mathcal{A} = (A, \delta^A, a_0, \tau^A)$. U ovom slučaju će izrazi $(a, x, a') \in \delta^A$ i $\delta^A(a, x) = a'$ imati isto značenje. Takođe ćemo δ_u^A smatrati funkcijom iz A u A, za svako $u \in X^*$ i kad je to zgodnije

pisati $\delta_u^A(a) = a'$ umesto $(a, a') \in \delta_u^A$. Zbog jednostavnosti u nastavku ćemo umesto naziva nedeterministički automat koristiti termin *automat*.

Reverzibilni automat automata $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ je automat $\bar{\mathcal{A}} = (A, \bar{\delta}^A, \bar{\sigma}^A, \bar{\tau}^A)$ za koji su tranziciona relacija i skupovi inicijalnih i završnih stanja, za svako $a, b \in A$ i $x \in X$, definisani sledećim jednakostima: $\bar{\delta}^A(a, x, b) = \delta^A(b, x, a)$, $\bar{\sigma}^A = \tau^A$ i $\bar{\tau}^A = \sigma^A$. Drugim rečima je $\bar{\delta}_x^A = (\delta_x^A)^{-1}$, za svako $x \in X$.

Automat $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ je *podautomat* automata $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ ako je $B \subseteq A$, δ_x^B restrikcija od δ_x^A na $B \times B$, za svako $x \in X$, a σ^B i τ^B su restrikcije skupova σ^A i τ^A na B, tj. $\delta_x^B = \delta_x^A \cap B \times B$, $\sigma^B = \sigma^A \cap B$ i $\tau^B = \tau^A \cap B$.

Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati. Preslikavanje $\phi : A \to B$ je *izomorfizam* ako je bijektivno i ako za svako $a, a_1, a_2 \in A$ i $x \in X$ važi sledeće:

$$(a_1, a_2) \in \delta_x^A \iff (\phi(a_1), \phi(a_2)) \in \delta_x^B, \tag{4.23}$$

$$a \in \sigma^A \iff \phi(a) \in \sigma^B, \tag{4.24}$$

$$a \in \tau^A \iff \phi(a) \in \tau^B. \tag{4.25}$$

Ako postoji izomorfizam između $\mathcal{A}$ i $\mathcal{B}$, onda kažemo da su $\mathcal{A}$ i $\mathcal{B}$ *izomorfni* automati i zapisujemo $\mathcal{A} \cong \mathcal{B}$. Primetimo da uređeni par $\mathcal{A}^x = (A, \delta_x^A)$ predstavlja usmereni graf čiji je skup čvorova određen skupom stanja A, a skup ivica tranzicionom relacijom δ_x^A, za dato $x \in X$. Odavde zaključujemo da automat $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ predstavlja multigraf čiji je skup ivica $\delta^A = \cup_{x \in X} \delta_x^A$. Dakle, ako su dva automata $\mathcal{A}$ i $\mathcal{B}$ izomorfna, onda iz (**??**) imamo da su grafovi $\mathcal{A}^x$ i $\mathcal{B}^x$ takođe izomorfni, za svako $x \in X$. Drugim rečima, izomorfni automati se, u suštini razlikuju, samo u zapisu njihovih stanja. Specijalno, ako su $\mathcal{A} = (A, \delta^A, a_0, \tau^A)$ i $\mathcal{B} = (B, \delta^B, b_0, \tau^B)$ deterministički automati, onda je bijekcija $\phi : A \to B$ izomorfizam ako i samo ako zadovoljava uslove $\phi(a_0) = b_0$, (**??**) i

$$\phi(\delta^A(a, x)) = \delta^B(\phi(a), x), \tag{4.26}$$

za svako $x \in x$ i $a \in A$.

Lako je proveriti da je kompozicija dva izomorfizma automata takođe izomorfizam, pa zato za proizvoljne automate $\mathcal{A}$, $\mathcal{B}$ i $\mathcal{C}$, iz $\mathcal{A} \cong \mathcal{B}$ i $\mathcal{B} \cong \mathcal{C}$ sledi $\mathcal{A} \cong \mathcal{C}$. Injektivna funkcija $\phi : A \to B$ koja zadovoljava uslove (**??**)–(**??**) se naziva *monomorfizam* iz $\mathcal{A}$ u $\mathcal{B}$. Lako je proveriti da je $\phi : A \to B$ monomorfizam iz $\mathcal{A}$ u $\mathcal{B}$ ako i samo ako je izomorfizam iz $\mathcal{A}$ u podautomat $\mathcal{C} = (C, \delta^C, \sigma^C, \tau^C)$ od $\mathcal{B}$, gde je $C = \operatorname{Im} \phi$.

Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat. *Jezik raspoznat* automatom $\mathcal{A}$, u oznaci $L(\mathcal{A})$, je jezik iz X^* definisan na sledeći način: za svako $u \in X^*$

$$u \in L(\mathcal{A}) \iff (\exists a_1, a_2 \in A) \left(a_1 \in \sigma^A \wedge (a_1, a_2) \in \delta_u^A \wedge a_2 \in \tau^A\right). \tag{4.27}$$

Na osnovu notacije uvedene relacijama (**??**)–(**??**), imamo da se (**??**) može zapisati kao

$$u \in L(\mathcal{A}) \iff (\sigma^A \circ \delta_u^A) \cap \tau^A \neq \emptyset \iff \sigma^A \cap (\delta_u^A \circ \tau^A) \neq \emptyset \iff \sigma^A \circ \delta_u^A \circ \tau^A = 1. \tag{4.28}$$

Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat i neka je E proizvoljna ekvivalencija na A. Definišimo tranzicionu relaciju $\delta^{A/E} \subseteq A/E \times X \times A/E$ tako da je

$$\begin{aligned} (E_{a_1}, x, E_{a_2}) \in \delta^{A/E} &\iff (\exists a_1', a_2' \in A) \left((a_1, a_1') \in E \wedge (a_1', x, a_2') \in \delta^A \wedge (a_2', a_2) \in E\right) \\ &\iff (a_1, a_2) \in E \circ \delta_x \circ E, \end{aligned} \tag{4.29}$$

za svako $a_1, a_2 \in A$ i $x \in X$. Takođe, možemo definisati skupove $\sigma^{A/E}, \tau^{A/E} \subseteq A/E$ sa

$$E_a \in \sigma^{A/E} \iff (\exists a' \in A)\left(a' \in \sigma^A \wedge (a', a) \in E\right) \iff a \in \sigma^A \circ E, \tag{4.30}$$

$$E_a \in \tau^{A/E} \iff (\exists a' \in A)\left((a, a') \in E \wedge a' \in \tau^A\right) \iff a \in E \circ \tau^A, \tag{4.31}$$

za svako $a \in A$. Očigledno su $\delta^{A/E}$, $\sigma^{A/E}$ i $\tau^{A/E}$ dobro definisane, te je $\mathcal{A}/E = (A/E, \delta^{A/E}, \sigma^{A/E}, \tau^{A/E})$ nedeterministički automat, koji nazivamo *faktor automatom* od $\mathcal{A}$ u odnosu na E.

Sledeće teoreme se mogu shvatiti kao verzije čuvenih teorema iz univerzalne algebre: Druge teoreme o izomorfizmu i Teoreme o korespondenciji, za nedetermenističke automate ([**?**, II.§6]).

Teorema 4.3.1. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat i neka su E i F ekvivalencije na A takve da je $E \subseteq F$.*

Tada je relacija F/E na A/E definisana sa

$$(E_{a_1}, E_{a_2}) \in F/E \iff (a_1, a_2) \in F, \quad \text{za svako } a_1, a_2 \in A, \tag{4.32}$$

ekvivalencija na A/E, a faktor automati $(\mathcal{A}/E)/(F/E)$ i $\mathcal{A}/F$ izomorfni.

Dokaz. Neka su $a_1, a_1', a_2, a_2' \in A$ takvi da je $E_{a_1} = E_{a_1'}$ i $E_{a_2} = E_{a_2'}$, tj. $(a_1, a_1'), (a_2, a_2') \in E$. Tada je $(a_1, a_1'), (a_2, a_2') \in F$, odakle je $(a_1, a_2) \in F$ ako i samo ako je $(a_1', a_2') \in F$. Dakle, F/E je dobro definisana relacija. Takođe je lako dokazati da je F/E ekvivalencija.

Radi jednostavnijeg zapisa, neka je $F/E = P$. Definišimo funkciju $\phi : A/F \to (A/E)/P$ sa

$$\phi(F_a) = P_{E_a}, \qquad \text{za svako } a \in A.$$

Za proizvoljne $a_1, a_2 \in A$ imamo da je

$$F_{a_1} = F_{a_2} \iff (a_1, a_2) \in F \iff (E_{a_1}, E_{a_2}) \in P \iff P_{E_{a_1}} = P_{E_{a_2}} \iff \phi(F_{a_1}) = \phi(F_{a_2}),$$

te je otuda ϕ dobro definisana i injektivna funkcija. Takođe je jasno da je ϕ i sirjektivna, pa zaključujemo da je ϕ bijekcija iz A/F u $(A/E)/P$.

Kako je $E \subseteq F$ ekvivalentno sa $E \circ F = F \circ E = F$, za proizvoljne $a_1, a_2 \in A$ i $x \in X$ imamo

$$\begin{aligned}
(\phi(F_{a_1}), \phi(F_{a_2})) \in \delta_x^{(A/E)/P} &\iff (P_{E_{a_1}}, P_{E_{a_2}}) \in \delta_x^{(A/E)/P} \iff (E_{a_1}, E_{a_2}) \in (P \circ \delta_x^{A/E} \circ P) \\
&\iff (\exists a_3, a_4 \in A)\left((E_{a_1}, E_{a_3}) \in P \wedge (E_{a_3}, E_{a_4}) \in \delta_x^{A/E} \wedge (E_{a_4}, E_{a_2}) \in P\right) \\
&\iff (\exists a_3, a_4 \in A)\left((a_1, a_3) \in F \wedge (a_3, a_4) \in (E \circ \delta_x^A \circ E) \wedge (a_4, a_2) \in F\right) \\
&\iff (a_1, a_2) \in F \circ E \circ \delta_x^A \circ E \circ F = F \circ \delta_x^A \circ F \\
&\iff (F_{a_1}, F_{a_2}) \in \delta_x^{A/F}.
\end{aligned}$$

Štaviše, za svako $a \in A$ dobijamo

$$\begin{aligned}
\phi(F_a) \in \sigma^{(A/E)/P} &\iff P_{E_a} \in \sigma^{(A/E)/P} \iff E_a \in \sigma^{A/E} \circ P \\
&\iff (\exists a' \in A)\left(E_{a'} \in \sigma^{A/E} \wedge (E_{a'}, E_a) \in P\right) \iff (\exists a' \in A)\left(a' \in \sigma^A \circ E \wedge (a', a) \in F\right) \\
&\iff a \in \sigma^A \circ E \circ F \iff a \in \sigma^A \circ F \iff F_a \in \sigma^{A/F}.
\end{aligned}$$

Slično pokazujemo ekvivalenciju $\phi(F_a) \in \tau^{(A/E)/P} \iff F_a \in \tau^{A/F}$.

Stoga, ϕ predstavlja izomorfizam automata $\mathcal{A}/F$ i $(\mathcal{A}/E)/(F/E)$. □

Teorema 4.3.2. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat i E ekvivalencija na A.*

Funkcija $\Phi : \mathcal{E}_E(A) \to \mathcal{E}(A/E)$, gde je $\mathcal{E}_E(A) = \{F \in \mathcal{E}(A) \mid E \subseteq F\}$, definisana sa

$$\Phi(F) = F/E, \quad \text{za svako } F \in \mathcal{E}_E(A), \tag{4.33}$$

je mrežni izomorfizam, tj. sirjektivna je i važi

$$F \subseteq G \iff \Phi(F) \subseteq \Phi(G), \quad \text{za svako } F, G \in \mathcal{E}_E(A). \tag{4.34}$$

Dokaz. Uzmimo proizvoljnu ekvivalenciju $P \in \mathcal{E}(A/E)$. Definisaćemo relaciju $F \subseteq A \times A$ tako da je

$$(a_1, a_2) \in F \iff (E_{a_1}, E_{a_2}) \in P, \quad \text{za svako } a_1, a_2 \in A. \tag{4.35}$$

Lako je pokazati da je F ekvivalencija na A i da je $P = F/E$. Za proizvoljne $a_1, a_2 \in A$, ako je $(a_1, a_2) \in E$, onda je $E_{a_1} = E_{a_2}$ i $(E_{a_1}, E_{a_2}) \in P$, odakle sledi da je $(a_1, a_2) \in F$. Konačno je $E \subseteq F$, tj. $F \in \mathcal{E}_E(A)$, odakle zaključujemo da je Φ sirjekcija.

Dalje, za proizvoljne $F, G \in \mathcal{E}_E(A)$ imamo da je

$$\begin{aligned} F \subseteq G &\iff (\forall (a_1, a_2) \in A \times A)\ \big((a_1, a_2) \in F \implies (a_1, a_2) \in G\big) \\ &\iff (\forall (a_1, a_2) \in A \times A)\ \big((E_{a_1}, E_{a_2}) \in \Phi(F) \implies (E_{a_1}, E_{a_2}) \in \Phi(G)\big) \\ &\iff \Phi(F) \subseteq \Phi(G). \end{aligned}$$

Dakle, Φ je mrežni izomorfizam. □

Važno je napomenuti da u terminima teorije mreža, $\mathcal{E}_E(A)$ predstavlja *glavni filter* mreže $\mathcal{E}(A)$ (određen ili generisan ekvivalencijom E).

4.4 Simulacije i bisimulacije

Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i neka je $\varphi \subseteq A \times B$ neprazna relacija. Za φ kazemo da je *direktna simulacija* ako

$$\sigma^A \subseteq \sigma^B \circ \varphi^{-1}, \tag{4.36}$$
$$\varphi^{-1} \circ \delta_x^A \subseteq \delta_x^B \circ \varphi^{-1}, \quad \text{za svako } x \in X, \tag{4.37}$$
$$\varphi^{-1} \circ \tau^A \subseteq \tau^B, \tag{4.38}$$

i da je *povratna simulacija* ako

$$\sigma^A \circ \varphi \subseteq \sigma^B, \tag{4.39}$$
$$\delta_x^A \circ \varphi \subseteq \varphi \circ \delta_x^B, \quad \text{za svako } x \in X, \tag{4.40}$$
$$\tau^A \subseteq \varphi \circ \tau^B. \tag{4.41}$$

Relaciju φ zovemeno *direktna bisimulacija* ako su obe φ i φ^{-1} direktne simulacije, tj. ako zadovoljava (**??**)–(**??**) i

$$\sigma^B \subseteq \sigma^A \circ \varphi, \tag{4.42}$$
$$\varphi \circ \delta_x^B \subseteq \delta_x^A \circ \varphi, \quad \text{za svako } x \in X, \tag{4.43}$$
$$\varphi \circ \tau^B \subseteq \tau^A, \tag{4.44}$$

i *povratna bisimulacija* ako su obe φ i φ^{-1} povratne simulacije, tj. ako zadovoljava (**??**)–(**??**) i

$$\sigma^B \circ \varphi^{-1} \subseteq \sigma^A, \tag{4.45}$$
$$\delta_x^B \circ \varphi^{-1} \subseteq \varphi^{-1} \circ \delta_x^A, \quad \text{za svako } x \in X, \tag{4.46}$$
$$\tau^B \subseteq \varphi^{-1} \circ \tau^A. \tag{4.47}$$

Neka su A i B neprazni skpovi i $E \subseteq A \times B$. Tada se prema notaciji iz formule (**??**) može lako zaključiti da je $A \circ E = \overline{E}(A)$ i $E \circ B = \overline{E}(A)^{-1}$, gde je preslikavanje $\overline{E} : \wp(A) \to \wp(B)$ definisano sa

$$\overline{E}(A') = \{b \in B \mid (\exists a \in A')\ (a,b) \in E\}, \tag{4.48}$$
$$\overline{E}^{-1}(B') = \{a \in A \mid (\exists b \in B')\ (a,b) \in E\}, \tag{4.49}$$

za proizvoljne $A' \subseteq A$ i $B' \subseteq B$. Drugim rečima, skupovi $\overline{E}(A')$ i $\overline{E}^{-1}(B')$ predstavljaju slike skupova A' i B' u odnosu na relacije E i E^{-1}, redom. Na osnovu ovakvog razmatranja, primetimo da se uslov (**??**) može interpretirati tako da za svako $a \in \sigma^A$ postoji $b \in \sigma^B$ tako da je $(a,b) \in \varphi$. Slično, (**??**) znači da za svako $b \in \sigma^B$ postoji $a \in \sigma^A$ tako da je $(a,b) \in \varphi$. Sa druge strane, uslov (**??**) označava da je $\{b \in B \mid (\exists a \in \tau^A)\,(a,b) \in \varphi\} \subseteq \tau^B$, dok uslov (**??**) znači da $\{a \in A \mid (\exists b \in \tau^B)\,(a,b) \in \varphi\} \subseteq \tau^A$. Slična interpretacija se može formulisati za uslove (**??**), (**??**), (**??**) i (**??**).

Dalje, φ nazivamo *direktna-povratna simulacija* ako je φ direktna i φ^{-1} povratna simulacija, tj. ako je

$$\sigma^A = \sigma^B \circ \varphi^{-1}, \tag{4.50}$$
$$\varphi^{-1} \circ \delta_x^A = \delta_x^B \circ \varphi^{-1}, \quad \text{za svako } x \in X, \tag{4.51}$$
$$\varphi^{-1} \circ \tau^A = \tau^B, \tag{4.52}$$

i *povratna-direktna simulacija* ako je φ povratna i φ^{-1} direktna simulacija, tj. ako je

$$\sigma^A \circ \varphi = \sigma^B, \tag{4.53}$$
$$\delta_x^A \circ \varphi = \varphi \circ \delta_x^B, \quad \text{za svako } x \in X, \tag{4.54}$$
$$\tau^A = \varphi \circ \tau^B. \tag{4.55}$$

Radi jednostavnosti, φ ćemo zvati samo *simulacija* ako je ona ili direktna ili povratna simulacija, a sa druge strane nazvaćemo je *bisimulacija* ukoliko pripada jednom od gore navedena četiri tipa bisimulacija. Štaviše, direktne i povratne bisimulacije zvaćemo *istorodnim*, a povratne-direktne i direktne-povratne bisimulacije ćemo zvati *raznorodnim*.

U brojnim radovima koji se bave simulacijama i bisimulacijama, uglavnom su bile proučavane direktne simulacije i direktne bisimulacije. Najčešće su za pojmove simulacija i bisimulacija bili korišćeni termini *jaka simulacija* i *jaka bisimulacija* ([**?**, **?**, **?**]), a najveća ekvivalencija koja je i bisimulacija nazivana je *"bisimilarity"*. Razlika između direktne i povratne simulacije sa jedne, i direktne i povratne bisimulacije sa druge, data je, na primer, u [**?**, **?**, **?**] (za različite vrste automata), ali se ovi koncepti manje ili više razlikuju od koncepata datih u ovoj tezi, iako imaju ista imena. Slični koncepti direktnih i povratnih simulacija i bisimulacija su proučavani u [**?**], i [**?**, **?**] (za stabla automate).

Sledeća lema se veoma lako može dokazati indukcijom.

Lema 4.4.1. *Ako uslov* (**??**) *ili uslov* (**??**) *važe za za svako* $x \in X$*, onda takođe važe i za svako* $u \in X^*$*, ako svako pojavljivanje slova* x *zamenimo rečju* u*.*

Lema 4.4.2. *Neka su* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *automati, i neka je* $\varphi \subseteq A \times B$ *relacija. Tada važe sledeća tvrđenja.*

(a) *Ako je* φ *simulacija, onda je* $L(\mathcal{A}) \subseteq L(\mathcal{B})$*.*

(b) *Ako je* φ *bisimulacija, onda je* $L(\mathcal{A}) = L(\mathcal{B})$*.*

Dokaz. (a) Neka je φ direktna simulacija. Tada za svako $u \in X^*$ imamo

$$\sigma^A \circ \delta_u^A \circ \tau^A \subseteq \sigma^B \circ \varphi^{-1} \circ \delta_u^A \circ \tau^A \subseteq \sigma^B \circ \delta_u^B \circ \varphi^{-1} \circ \tau^A \subseteq \sigma^B \circ \delta_u^B \circ \tau^B,$$

te na osnovu (**??**) dobijamo da je $L(\mathcal{A}) \subseteq L(\mathcal{B})$. Slično, ako je φ povratna simulacija, onda je takođe $L(\mathcal{A}) \subseteq L(\mathcal{B})$:

$$\sigma^A \circ \delta_u^A \circ \tau^A \subseteq \sigma^A \circ \delta_u^A \circ \varphi \circ \tau^B \subseteq \sigma^A \circ \varphi \circ \delta_u^B \circ \tau^B \subseteq \sigma^B \circ \delta_u^B \circ \tau^B.$$

(b) Ovaj deo tvrđenja direktno sledi iz dela (a). □

Na osnovu ove leme možemo reći da je i u slučaju povratne i direktne simulacije automat $\mathcal{A}$ simulira "rad" automata $\mathcal{B}$, jer važi da je $L(\mathcal{A}) \subseteq L(\mathcal{B})$. Iz dokaza leme se vidi zašto je opravdana upotreba termina povratna i direktna simulacija. Naime, neka je φ direktna simulacija i neka je $a_0, a_1, \ldots, a_k$ niz stanja automata $\mathcal{A}$ kojim se određuje reč $u = x_1 x_2 \ldots x_k \in L(\mathcal{A})$, gde je $x_k \in X$, za svako $1 \leq i \leq n$. Tada na osnovu relacije (**??**) sledi da postoji $b_0 \in \sigma^B$ tako da je $(a_0, b_0) \in \varphi$. Dalje, kako je sada $(b_0, a_1) \in \varphi^{-1} \circ \delta_{x_1}^A$ to je i $(b_0, a_1) \in \delta_{x_1}^B \circ \varphi^{-1}$, odakle sledi da postoji neko $b_1 \in B$ takvo da je $(b_0, b_1) \in \delta_{x_1}^B$ i $(a_1, b_1) \in \varphi$. Induktivno, za svako stanje $a_k \in A$ dobijamo stanje $b_k \in B$, za svako $1 \leq k \leq n$, pri čemu stanje a_n mora biti u τ^A i kako je $(a, b) \in \varphi$ imamo da je $b_n \in \tau^B$, zbog (**??**). Dakle, kretanjem kroz niz stanja $a_0, a_1, \ldots, a_n$, generišemo niz stanja $b_0, b_1, \ldots, b_n$ koji određuju istu reč $u \in X^*$ i pri tome je $(a_k, b_k) \in \varphi$. Slično možemo zaključiti, da ako je φ povratna, tada kretanjem kroz niz stanja $a_n, a_{n-1}, \ldots, a_0$, generišemo niz stanja $b_n, b_{n-1}, \ldots, b_0$ koji određuju istu reč $u \in X^*$ i pri tome je $(a_k, b_k) \in \varphi$. Slika 4.1 daje vizuelizaciju prethodnog razmatranja vezanog za definiciju direktne simulacije.

Lema 4.4.3. *Neka su* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *automati i neka je* $\varphi \subseteq A \times B$ *relacija. Tada je*

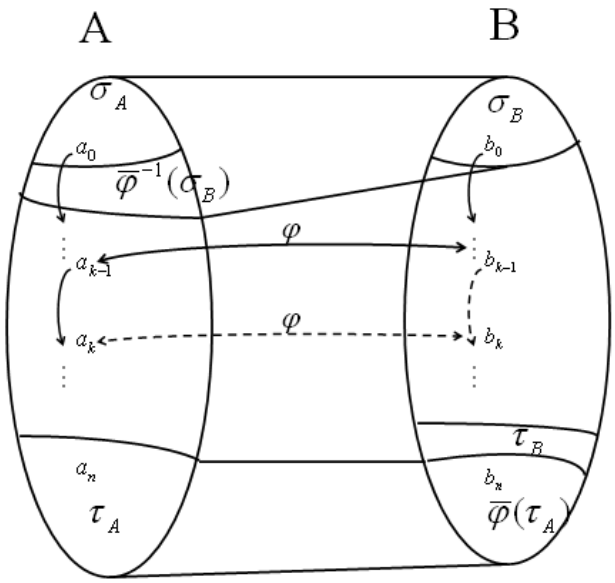
(a) φ *povratna bisimulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$ *ako i samo ako je direktna bisimulacija iz* $\bar{\mathcal{A}}$ *u* $\bar{\mathcal{B}}$*.*

(b) φ *je direktna-povratna bisimulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$ *ako i samo ako je povratna-direktna bisimulacija iz* $\bar{\mathcal{A}}$ *u* $\bar{\mathcal{B}}$*.*

Dokaz. Direktnom primenom (**??**) dobijamo da je

$$\begin{aligned} &\delta_x^A \circ \phi \subseteq \varphi \circ \delta_x^B \iff \\ &(\delta_x^A \circ \phi)^{-1} \subseteq (\varphi \circ \delta_x^B)^{-1} \iff \\ &\varphi^{-1} \overline{\delta}_x^A \subseteq \overline{\delta}_x^B \circ \varphi^{-1}. \end{aligned}$$

Takođe, iz $\sigma^A \circ \varphi = \varphi^{-1} \circ \sigma^A = \overline{\varphi}(\sigma^A) \subseteq \sigma^B$ i $\tau^A \subseteq \varphi \circ \tau^B = \tau^B \circ \varphi^{-1} = \overline{\varphi}^{-1}(\tau^B)$, zaključujemo da je φ povratna simulacija iz A u B ako i samo ako je φ direktna simulacija iz $\overline{A}$ u $\overline{B}$. Kako



Slika 4.1: *Direktna simulacija* φ

isti dokaz možemo sprovesti i za φ^{-1} imamo da direktno važi prvi deo tvrđenja. Jasno je da se i drugi deo tvrđenja dokazuje na isti način. □

Na osnovu prethodne leme, za bilo koje univerzalno tačno tvrđenje koje važi za direktne (povratne-direktne) bisimulacije (vezano za nedeterminističke automate), postoji odgovarajuće univerzalno tvrđenje za povratne (direktne-povratne) bisimulacije. Iz tog razloga, radićemo samo sa direktnim i povratnim-direktnim bisimulacijama.

Možemo uočiti neke razlike između istorodnih i raznorodnih bisimulacija. Trivijalno se zaključuje da je inverz direktne (povratne) bisimulacije takođe direktna (povratna) bisimulacija. Međutim, inverz povratne-direktne (direktne-povratne) bisimulacije nije obavezno povratna-direktna (direktna-povratna) bisimulacija. Inverz povratne-direktne bisimulacije je direktna-povratna bisimulacija, i obrnuto. Kasnije ćemo istaći i druge razlike među ovim tipovima bisimulacija.

Lako je proveriti da je sledeće tvrđenje tačno.

Lema 4.4.4. *Kompozicija dve direktne* (*povratne-direktne*) *bisimulacije, kao i unija proizvoljne familije direktnih* (*povratnih-direktnih*) *bisimulacija je takođe direktna* (*povratna-direktna*) *bisimulacije.*

Sada možemo pokazati sledeći rezulatat koji je od suštinske važnosti za dalje izlaganje.

Teorema 4.4.5. *Neka su* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *automati tako da postoji najmanje jedna direktna bisimulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$*.*

Tada postoji najveća direktna bisimulacija iz $\mathcal{A}$ *u* $\mathcal{B}$*, koja je i paracijalna uniformna relacija.*

Dokaz. Po pretpostavci teoreme, familija $\{\varphi_i\}_{i\in I}$ svih direktnih bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$ je neprazna. Neka je φ unija ove familije relacija. Na osnovu Leme **??**, dobijamo da je φ direktna bisimulacija, te je evidentno i najveća.

Prema Lemi **??** takođe imamo da je $\varphi \circ \varphi^{-1} \circ \varphi$ direktna bisimulacija, a kako je φ najveća, zaključujemo da je $\varphi \circ \varphi^{-1} \circ \varphi \subseteq \varphi$. Konačno, na osnovu Teoreme **??** imamo da je φ parcijalna uniformna relacija. □

Slična teorema može biti dokazana i za povratne-direktne bisimulacije, ali u ovom slučaju ne možemo dokazati da je najveća povratna-direktna bisimulacija parcijalna uniformna relacija. Drugim rečima, važi sledeće tvrđenje.

Teorema 4.4.6. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati takvi da postoji bar jedna povratna-direktna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$. Tada postoji najveća povratna-direktna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$.*

Lema 4.4.7. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i $\varphi \subseteq A \times B$ relacija. Takođe, neka su $\mathcal{C} = (C, \delta^C, \sigma^C, \tau^C)$ i $\mathcal{D} = (D, \delta^D, \sigma^D, \tau^D)$ podautomati od $\mathcal{A}$ i $\mathcal{B}$, gde je $C = \operatorname{Dom}\varphi$ i $D = \operatorname{Im}\varphi$. Tada je $\varphi \subseteq C \times D$ i*

(a) *ako je φ direktna (povratna) simulacija iz $\mathcal{A}$ u $\mathcal{B}$, onda je ona direktna (povratna) simulacija iz $\mathcal{C}$ u $\mathcal{D}$;*

(b) *ako je φ^{-1} direktna (povratna) simulacija iz $\mathcal{B}$ u $\mathcal{A}$, onda je ona direktna (povratna) simulacija iz $\mathcal{D}$ u $\mathcal{C}$.*

Takođe, ako je $A = C$, onda važi suprotan smer implikacije u (a)*, a ako je $B = D$, onda važi suprotan smer implikacije u* (b)*.*

Dokaz. Dokazaćemo prvi deo tvrđenja (a) u slučaju direktnih simulacija. Ostatak tvrđenja se na isti način može dokazati. Dakle, neka je φ direktna simulacija iz $\mathcal{A}$ u $\mathcal{B}$.

Najpre, neka je $a \in \sigma^C \subseteq \sigma^A \subseteq \sigma^B \circ \varphi^{-1}$. Tada postoji $b \in B$ takav da je $b \in \sigma^B$ i $(b, a) \in \varphi^{-1}$, tj. $(a, b) \in \varphi$, odakle sledi da je $b \in D$. Ovo znači da je $b \in \sigma^B \cap D = \sigma^D$, te je $a \in \sigma^D \circ \varphi^{-1}$. Ovim smo dokazali da je $\sigma^C \subseteq \sigma^D \circ \varphi^{-1}$.

Dalje, neka je $(b, a) \in \varphi^{-1} \circ \delta_x^C \subseteq \varphi^{-1} \circ \delta_x^A \subseteq \delta_x^B \circ \varphi^{-1}$. Iz $(b, a) \in \varphi^{-1} \circ \delta_x^C$ sledi da je $(b, a') \in \varphi^{-1}$ i $(a', a) \in \delta_x^C$, za neko $a' \in C$, odakle sledi da je $b \in D$. Štaviše, iz $(b, a) \in \delta_x^B \circ \varphi^{-1}$ dobijamo da postoji $b' \in B$ takvo da je $(b, b') \in \delta_x^B$ i $(b', a) \in \varphi^{-1}$, odakle je $b' \in D$. Dalje imamo da je $b, b' \in D$ i $(b, b') \in \delta_x^B$, te je $(b, b') \in \delta_x^D$, a kako je i $(b', a) \in \varphi^{-1}$, zaključujemo da je $(b, a) \in \delta_x^D \circ \varphi^{-1}$. Konačno je $\varphi^{-1} \circ \delta_x^C \subseteq \delta_x^D \circ \varphi^{-1}$.

Neka je $b \in \varphi^{-1} \circ \tau^C \subseteq \varphi^{-1} \circ \tau^A \subseteq \tau^B$. Iz $b \in \varphi^{-1} \circ \tau^C$ sledi da postoji $a \in C$ takav da je $(b, a) \in \varphi^{-1}$ i $a \in \tau^C$, odakle je $b \in D$. To znači da je $b \in \tau^B \cap D = \tau^D$, pa je konačno pokazano da je $\varphi^{-1} \circ \tau^C \subseteq \tau^D$.

Ako je $A = C$ ili $B = D$, onda je suprotan smer implikacije u (a) i (b) direktna posledica relacije (**??**). □

Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ proizvoljan automat. Ako je $\varphi \subseteq A \times A$ direktna bisimulacija iz skupa $\mathcal{A}$ na samog sebe, zvaćemo je *direktna bisimulacija na $\mathcal{A}$* (analogno definišemo *povratne bisimulacije na $\mathcal{A}$*). Familija svih direktnih bisimulacija na $\mathcal{A}$ je neprazna (sadrži relaciju jednakosti), pa kao i u dokazu Teoreme **??** može se dokazati da postoji najveća direktna bisimulacija na $\mathcal{A}$, koja je ekvivalencija ([**?**], [**?**]). Direktne bisimulacije na $\mathcal{A}$ koje su ekvivalencije nazvaćemo *direktnim bisimulacionim ekvivalencijama* (analogno se definiše pojam *povratnih bisimulacionih ekvivalencija*). Skup svih direktnih bisimulacionih ekvivalencija na $\mathcal{A}$ označićemo sa $\mathcal{E}^{\mathrm{fb}}(\mathcal{A})$.

Zbog svojstva simetričnosti, ekvivalencija E na A je direktna bisimulacija na $\mathcal{A}$ ako i samo ako je

$$E \circ \delta_x^A \subseteq \delta_x^A \circ E, \quad \text{za svako } x \in X, \tag{4.56}$$
$$E \circ \tau^A = \tau^A. \tag{4.57}$$

Važno je napomenuti da su uslovi (**??**) i (**??**) zadovoljeni kad god je $A = B$ i φ refleksivna na A, a E je ekvivalencija na A. Na osnovu Teoreme 4.1 [**?**] (takođe Teorema 1 [**?**]), uslov (**??**) je ekvivalentan sa

$$E \circ \delta_x^A \circ E = \delta_x^A \circ E, \quad \text{za svako } x \in X. \tag{4.58}$$

Slično, ekvivalencija E na A je povratna bisimulacija na $\mathcal{A}$ ako i samo ako je

$$\delta_x^A \circ E \subseteq E \circ \delta_x^A, \quad \text{za svako } x \in X, \tag{4.59}$$
$$\sigma^A \circ E = \sigma^A, \tag{4.60}$$

pri čemu takođe imamo da je uslov (**??**) ekvivalentan sa

$$E \circ \delta_x^A \circ E = E \circ \delta_x^A, \quad \text{za svako } x \in X. \tag{4.61}$$

Direktne bisimulacione ekvivalencije su proučavane u mnogim radovima u kontekstu označenih tranzicionih sistema, gde su uspešno korišćene za redukciju broja stanja sistema. Posebno je predložen i veliki broj algoritama za izračunavanje najveće direktne bisimulacione ekvivalencije datog označenog tranzicionog sistema, a najbrži je zasnovan na ekvivalenciji problema traženja najveće direktne bisimulacione ekvivalencije i pronalaženju najgrublje particije ([**?**, **?**, **?**, **?**, **?**]). Direktne i povratne bisimulacione ekvivalencije na nedeterminističkim automatima su proučavali Ilie, Yu i drugi [**?**, **?**, **?**, **?**], gde su ih redom zvali *desno* i *levo invariantne ekvivalencije*. U drugačijem kontekstu, direktne bisimulacione ekvivalencije je razmatrao Calude [**?**], gde ih je nazvao *"well-behaved equivalences"*. Oba pomenuta tipa ekvivalencija su takođe korišćena za redukciju broja stanja nedeterminističkih automata.

Sledeća teorema može biti izvedena iz Teoreme 4.2 [**?**], ali mi dajemo direktan dokaz.

Teorema 4.4.8. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat. Skup svih direktnih bisimulacionih ekvivalencija na $\mathcal{A}$, $\mathcal{E}^{\mathrm{fb}}(\mathcal{A})$, čini kompletnu mrežu. Ova mreža je podpolumreža u odnosu na uniju, mreže $\mathcal{E}(A)$ svih ekvivalencija na A.*

Dokaz. Kako $\mathcal{E}^{\mathrm{fb}}(\mathcal{A})$ sadrži najmanje jedan element od $\mathcal{E}(A)$, tj. relaciju jednakosti na A, pa je dovoljno pokazati da je $\mathcal{E}^{\mathrm{fb}}(\mathcal{A})$ kompletna podpolumreža u odnosu na uniju, mreže $\mathcal{E}(A)$.

Neka je $\{E_i\}_{i \in I}$ proizvoljna neprazna familija direktnih bisimulacionih ekvivalencija na $\mathcal{A}$ i neka je E unija elemenata ove familije u mreži $\mathcal{E}(A)$. Dobro je poznato da se E može predstaviti kao unija relacija iz $\langle E_i \mid i \in I \rangle$, gde smo sa $\langle E_i \mid i \in I \rangle$ označili podpolugrupu generisanu familijom $\{E_i\}_{i \in I}$, polugrupe svih binarnih relacija na A. To znači da se svaka relacija iz $\langle E_i \mid i \in I \rangle$ može predstaviti kao kompozicija neke konačne kolekcije relacija iz $\{E_i\}_{i \in I}$, pa na osnovu Leme **??**, zaključujemo da je svaka relacija iz $\langle E_i \mid i \in I \rangle$ direktna bisimulacija. Zato je E direktna bisimulacija, pošto je unija svih navedenih relacija. Dakle, imamo da važi $E \in \mathcal{E}^{\mathrm{fb}}(\mathcal{A})$, što znači da je $\mathcal{E}^{\mathrm{fb}}(\mathcal{A})$ kompletna podpolumreža u odnosu na uniju, od $\mathcal{E}(A)$. □

4.5 Uniformne direktne bisimulacije

Teorema 4.5.1. *Neka su* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *automati i* $\varphi \subseteq A \times B$ *uniformna relacija. Tada je* φ *direktna bisimulacija ako i samo ako važe sledeće jednakosti:*

$$\sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}, \qquad \sigma^A \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi, \tag{4.62}$$

$$\delta_x^A \circ \varphi \circ \varphi^{-1} = \varphi \circ \delta_x^B \circ \varphi^{-1}, \quad \varphi^{-1} \circ \delta_x^A \circ \varphi = \delta_x^B \circ \varphi^{-1} \circ \varphi, \qquad \text{za svako } x \in X, \tag{4.63}$$

$$\tau^A = \varphi \circ \tau^B, \qquad \varphi^{-1} \circ \tau^A = \tau^B. \tag{4.64}$$

Dokaz. Neka je φ direktna bisimulacija. Prema (**??**), (**??**) i (**??**), dobijamo $\sigma^A \circ \varphi \subseteq \sigma^B \circ \varphi^{-1} \circ \varphi \subseteq \sigma^A \circ \varphi \circ \varphi^{-1} \circ \varphi \subseteq \sigma^A \circ \varphi$, pa je $\sigma^A \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi$. Na osnovu poslednjeg sledi da je $\sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1} \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}$.

Dalje, na osnovu Teoreme **??** i Leme **??** dobijamo da je $\varphi \circ \varphi^{-1}$ direktna bisimulaciona ekvivalencija na $\mathcal{A}$, pa na osnovu (**??**), za svako $x \in X$ imamo

$$\varphi \circ \delta_x^B \circ \varphi^{-1} \subseteq \delta_x^A \circ \varphi \circ \varphi^{-1} = \varphi \circ \varphi^{-1} \circ \delta_x^A \circ \varphi \circ \varphi^{-1} \subseteq \varphi \circ \delta_x^B \circ \varphi^{-1} \circ \varphi \circ \varphi^{-1} = \varphi \circ \delta_x^B \circ \varphi^{-1}.$$

Zato je $\delta_x^A \circ \varphi \circ \varphi^{-1} = \varphi \circ \delta_x^B \circ \varphi^{-1}$. Na sličan način pokazujemo da je $\varphi^{-1} \circ \delta_x^A \circ \varphi = \delta_x^B \circ \varphi^{-1} \circ \varphi$.

Konačno, kako je $\varphi \circ \varphi^{-1}$ direktna bisimulaciona ekvivalencija na $\mathcal{A}$, na osnovu (**??**), (**??**), (**??**) i (**??**), dobijamo $\tau^A = \varphi \circ \varphi^{-1} \circ \tau^A \subseteq \varphi \circ \tau^B \subseteq \tau^A$, pa je $\tau^A = \varphi \circ \tau^B$. Slično pokazujemo da je $\varphi^{-1} \circ \tau^A = \tau^B$.

Na ovaj način smo dokazali da su tvrđenja (**??**)–(**??**) tačna.

Obrnuto, neka važi (**??**)–(**??**). Na osnovu refleksivnosti relacije $\varphi \circ \varphi^{-1}$ i (**??**) imamo da je $\sigma^A \subseteq \sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}$, te zato važi (**??**). Takođe iz refleksivnosti $\varphi \circ \varphi^{-1}$, (**??**) i (**??**), za svako $x \in X$ imamo da je

$$\varphi^{-1} \circ \delta_x^A \subseteq \varphi^{-1} \circ \delta_x^A \circ \varphi \circ \varphi^{-1} = \delta_x^B \circ \varphi^{-1} \circ \varphi \circ \varphi^{-1} = \delta_x^B \circ \varphi^{-1},$$

odakle je $\varphi^{-1} \circ \delta_x^A \subseteq \delta_x^B \circ \varphi^{-1}$. Slično je i $\varphi \circ \delta_x^B \subseteq \delta_x^A \circ \varphi$. Konačno, iz (**??**) i (**??**) sledi (**??**). Dakle, dokazali smo da je φ direktna bisimulacija. □

Zbog simetričnosti zapisa smo u (**??**) uključili obe jednakosti, mada je dovoljna samo jedna od njih. Na primer, ako je $\sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}$ onda je i $\sigma^A \circ \varphi = \sigma^A \circ \varphi \circ \varphi^{-1} \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi$. Slično pokazujemo da iz druge jednakosti sledi prva.

Teorema 4.5.2. *Neka su* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *automati i* $\varphi \subseteq A \times B$ *uniformna relacija. Tada je* φ *direktna bisimulacija ako i samo ako su zadovoljeni sledeći uslovi:*

(i) E_A^φ *je direktna bisimulaciona ekvivalencija na* $\mathcal{A}$*;*

(ii) E_B^φ *je direktna bisimulaciona ekvivalencija na* $\mathcal{B}$*;*

(iii) $\widetilde{\varphi}$ *je izomorfizam faktor automata* $\mathcal{A}/E_A^\varphi$ *i* $\mathcal{B}/E_B^\varphi$*.*

Dokaz. Zbog jednostavnijeg zapisa stavićemo da je $E_A^\varphi = E$ i $E_B^\varphi = F$.

Neka je φ direktna bisimulacija. Kako je φ uniformna relacija tada je na osnovu Teoreme **??**, $E = \varphi \circ \varphi^{-1}$ i $F = \varphi^{-1} \circ \varphi$, pri čemu su ove relacije ekvivalencije. Relacija φ je direktna bisimulacija, pa na osnovu Leme **??** imamo da su i E i F direktne bisimulacije, čime smo dokazali tvrđenja (i) i (ii).

Po Teoremi **??**, $\widetilde{\varphi}$ je bijekcija. Dalje, kako je $E = \varphi \circ \varphi^{-1}$, korišćenjem jednakosti (**??**), za bilo koje $a_1, a_2 \in A$, $x \in X$ i $f \in FD(\varphi)$ imamo da je

$$\begin{aligned}
(E_{a_1}, E_{a_2}) \in \delta_x^{A/E} &\iff (a_1, a_2) \in E \circ \delta_x^A \circ E \iff (a_1, a_2) \in \varphi \circ \delta_x^B \circ \varphi^{-1} \\
&\iff (\exists b_1, b_2 \in B)\big((a_1, b_1) \in \varphi \wedge (b_1, b_2) \in \delta_x^B \wedge (a_2, b_2) \in \varphi\big) \\
&\iff (\exists b_1, b_2 \in B)\big((f(a_1), b_1) \in F \wedge (b_1, b_2) \in \delta_x^B \wedge (f(a_2), b_2) \in F\big) \\
&\iff (f(a_1), f(a_2)) \in F \circ \delta_x^B \circ F \iff (F_{f(a_1)}, F_{f(a_2)}) \in \delta_x^{B/F} \\
&\iff (\widetilde{\varphi}(E_{a_1}), \widetilde{\varphi}(E_{a_2})) \in \delta_x^{B/F},
\end{aligned}$$

i za bilo koje $a \in A$ i $f \in FD(\varphi)$ važi

$$\begin{aligned}
E_a \in \sigma^{A/E} &\iff a \in \sigma^A \circ E \iff (\exists a' \in A)\big(a' \in \sigma^A \wedge (a', a) \in E\big) \\
&\iff (\exists a' \in A)\big(a' \in \sigma^A \wedge (a', f(a)) \in \varphi\big) \\
&\iff f(a) \in \sigma^A \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi = \sigma^B \circ F \\
&\iff F_{f(a)} \in \sigma^{B/F} \iff \widetilde{\varphi}(E_a) \in \sigma^{B/F}, \\
E_a \in \tau^{A/E} &\iff a \in E \circ \tau^A \iff (\exists a' \in A)\big((a, a') \in E \wedge a' \in \tau^A\big) \\
&\iff (\exists a' \in A)\big((f(a), a') \in \varphi^{-1} \wedge a' \in \tau^A\big) \\
&\iff f(a) \in \varphi^{-1} \circ \tau^A = \varphi^{-1} \circ \varphi \circ \tau^B = F \circ \tau^B \\
&\iff F_{f(a)} \in \tau^{B/F} \iff \widetilde{\varphi}(E_a) \in \tau^{B/F}.
\end{aligned}$$

Dakle, $\widetilde{\varphi}$ je izomorfizam automata $\mathcal{A}/E$ i $\mathcal{B}/F$.

Obrnuto, neka važe (i), (ii) i (iii). Prema (i), za svako $x \in X$ imamo

$$E \circ \delta_x^A \circ E = \delta_x^A \circ E = \delta_x^A \circ \varphi \circ \varphi^{-1},$$

a prema (iii), za proizvoljne $a_1, a_2 \in A$ i $f \in FD(\varphi)$ dobijamo da je

$$\begin{aligned}
(a_1, a_2) \in \delta_x^A \circ \varphi \circ \varphi^{-1} &\iff (a_1, a_2) \in E \circ \delta_x^A \circ E \iff (E_{a_1}, E_{a_2}) \in \delta_x^{A/E} \\
&\iff (\widetilde{\varphi}(E_{a_1}), \widetilde{\varphi}(E_{a_2})) \in \delta_x^{B/F} \iff (F_{f(a_1)}, F_{f(a_2)}) \in \delta_x^{B/F} \\
&\iff (f(a_1), f(a_2)) \in F \circ \delta_x^B \circ F \\
&\iff (\exists b_1, b_2 \in B)\big((f(a_1), b_1) \in F \wedge (b_1, b_2) \in \delta_x^B \wedge (f(a_2), b) \in F\big) \\
&\iff (\exists b_1, b_2 \in B)\big((a_1, b_1) \in \varphi \wedge (b_1, b_2) \in \delta_x^B \wedge (a_2, b) \in \varphi\big) \\
&\iff (a_1, a_2) \in \varphi \circ \delta_x^B \circ \varphi^{-1}.
\end{aligned}$$

Dakle, prva jednakost u (**??**) je zadovoljena. Na sličan način dokazujemo drugu jednakost u (**??**).

Dalje, za svaki $a \in A$ imamo

$$\begin{aligned}
a \in \sigma^A \circ \varphi \circ \varphi^{-1} &\iff a \in \sigma^A \circ E \iff E_a \in \sigma^{A/E} \iff \widetilde{\varphi}(E_a) \in \sigma^{B/F} \iff F_{f(a)} \in \sigma^{B/F} \\
&\iff f(a) \in \sigma^B \circ F \iff (\exists b \in B)\big(b \in \sigma^B \wedge (f(a), b) \in F\big) \\
&\iff (\exists b \in B)\big(b \in \sigma^B \wedge (a, b) \in \varphi\big) \iff a \in \sigma^B \circ \varphi^{-1},
\end{aligned}$$

odakle je $\sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}$, te je zato, $\sigma^A \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi$. Za svako $a \in A$ imamo takođe

$$\begin{aligned}
a \in \tau^A &\iff a \in E \circ \tau^A \iff E_a \in \tau^{A/E} \iff \widetilde{\varphi}(E_a) \in \tau^{B/F} \iff F_{f(a)} \in \tau^{B/F} \\
&\iff f(a) \in F \circ \tau^B \iff (\exists b \in B)\big((f(a), b) \in F \wedge b \in \tau^B\big) \\
&\iff (\exists b \in B)\big((a, b) \in \varphi \wedge b \in \tau^B\big) \iff a \in \varphi \circ \tau^B,
\end{aligned}$$

odakle je $\tau^A = \varphi \circ \tau^B$. Na isti način je i $\tau^B = \varphi^{-1} \circ \tau^A$. Ovim smo dokazali da jednakosti (**??**) i (**??**) važe, pa je zbog toga φ direktne bisimulacija. □

Teorema 4.5.3. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i E i F direktne bisimulacione ekvivalencije na $\mathcal{A}$ i $\mathcal{B}$, redom.*

Tada postoji uniformna direktna bisimulacija $\varphi \subseteq A \times B$ takva da je $E_A^\varphi = E$ i $E_B^\varphi = F$ ako i samo ako su faktor automati $\mathcal{A}/E$ i $\mathcal{B}/F$ izomorfni.

Dokaz. Direktan smer tvrđenja teoreme dobija se neposrednom primenom Teoreme **??**.

Obratno, neka je $\phi : A/E \to B/F$ izomorfizam između faktor automata $\mathcal{A}/E$ i $\mathcal{B}/F$. Definišimo $\varphi \subseteq A \times B$ kao u (**??**), tj.

$$(a, b) \in \varphi \iff \phi(E_a) = F_b, \quad \text{za svako } a \in A \text{ i } b \in B.$$

Na osnovu dokaza Teoreme **??**, φ je uniformna relacija takva da je $E = E_A^\varphi$, $F = E_B^\varphi$ i $\phi = \widetilde{\varphi}$, pa je po Teoremi **??**, φ direktna bisimulacija. □

Teorema 4.5.4. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat i E direktna bisimulaciona ekvivalencija na $\mathcal{A}$, a F ekvivalencija A takva da je $E \subseteq F$.*

Tada je F direktna bisimulaciona ekvivalencija na $\mathcal{A}$ ako i samo ako je F/E direktna bisimulaciona ekvivalencija na $\mathcal{A}/E$.

Dokaz. Kao u dokazu Teoreme **??**, neka je $F/E = P$. Za proizvoljne $a_1, a_2 \in A$ i $x \in X$, na osnovu dokaza Teoreme **??** dobijamo da je

$$(E_{a_1}, E_{a_2}) \in P \circ \delta_x^{A/E} \circ P \iff (a_1, a_2) \in F \circ \delta_x^A \circ F.$$

Takođe je i

$$\begin{aligned}
(E_{a_1}, E_{a_2}) \in \delta_x^{A/E} \circ P &\iff (\exists a_3 \in A)\ \big((E_{a_1}, E_{a_3}) \in \delta_x^{A/E} \wedge (E_{a_3}, E_{a_2}) \in P\big) \\
&\iff (\exists a_3 \in A)\ \big((a_1, a_3) \in E \circ \delta_x^A \circ E \wedge (a_3, a_2) \in F\big) \\
&\iff (a_1, a_2) \in E \circ \delta_x^A \circ E \circ F \\
&\iff (a_1, a_2) \in \delta_x^A \circ F,
\end{aligned}$$

jer je $E \circ \delta_x^A \circ E \circ F = \delta_x^A \circ E \circ F = \delta_x^A \circ F$, zbog (**??**) i $E \subseteq F$. Zaključujemo da je

$$P \circ \delta_x^{A/E} \circ P = \delta_x^{A/E} \circ P \iff F \circ \delta_x^A \circ F = \delta_x^A \circ F.$$

Štaviše, za proizvoljno $a \in A$ imamo da je

$$\begin{aligned}
E_a \in P \circ \tau^{A/E} &\iff (\exists a' \in A)\ (E_a, E_{a'}) \in P \wedge E_{a'} \in \tau^{A/E} \\
&\iff (\exists a' \in A)\ (a, a') \in F \wedge a' \in E \circ \tau^A \\
&\iff a \in F \circ E \circ \tau^A = F \circ \tau^A,
\end{aligned}$$

pa na osnovu (**??**) i (**??**), $E_a \in \tau^{A/E} \iff a \in E \circ \tau^A = \tau^A$. Odavde je

$$P \circ \tau^{A/E} = \tau^{A/E} \iff F \circ \tau^A = \tau^A,$$

što dokazuje tvrdnju. □

U svetlu Teoreme **??**, pravilo $F \mapsto F/E$ definiše izomorfizam između mreža $\mathcal{E}_E(A)$ i $\mathcal{E}(A/E)$, za svako $E \in \mathcal{E}(A)$. Na osnovu Teoreme **??**, isto pravilo određuje izomorfizam između mreža $\mathcal{E}_E^{\mathrm{fb}}(\mathcal{A})$ i $\mathcal{E}^{\mathrm{fb}}(\mathcal{A}/E)$, gde je $\mathcal{E}_E^{\mathrm{fb}}(\mathcal{A}) = \{F \in \mathcal{E}^{\mathrm{fb}}(\mathcal{A}) \mid E \subseteq F\}$, za svako $E \in \mathcal{E}^{\mathrm{fb}}(\mathcal{A})$.

Kao posledicu prethodnog razmatranja dobijamo sledeće tvrđenje.

Posledica 4.5.5. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat i neka su E i F direktne bisimulacione ekvivalencije na $\mathcal{A}$ takve da je $E \subseteq F$.*

Tada je F najveća direktna bisimulaciona ekvivalencija na $\mathcal{A}$ ako i samo ako je F/E najveća direktna bisimulaciona ekvivalencija na $\mathcal{A}/E$.

Dokaz. Tvrđenje direktno sledi iz Teorema **??** i **??** (**??**). □

4.6 Direktno bisimulaciono ekvivalentni automati

Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati. Ako postoji kompletna i sirjektivna direktne bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$, onda kažemo da su $\mathcal{A}$ i $\mathcal{B}$ *direktno bisimulaciono ekvivalentni*, ili skraćeno *FB-ekvivalentni* i pišemo $\mathcal{A} \sim_{FB} \mathcal{B}$. Primetimo da uslovi kompletnosti i sirjekcije direktnih bisimulacija znače da je svako stanje iz $\mathcal{A}$ ekvivalentno nekom stanju u $\mathcal{B}$, kao i obrnuto. Za automate $\mathcal{A}$, $\mathcal{B}$ i $\mathcal{C}$ imamo da je

$$\mathcal{A} \sim_{FB} \mathcal{A}; \quad \mathcal{A} \sim_{FB} \mathcal{B} \implies \mathcal{B} \sim_{FB} \mathcal{A}; \quad \big(\mathcal{A} \sim_{FB} \mathcal{B} \wedge \mathcal{B} \sim_{FB} \mathcal{C}\big) \implies \mathcal{A} \sim_{FB} \mathcal{C}. \tag{4.65}$$

Slično, za $\mathcal{A}$ i $\mathcal{B}$ kažemo da su *povratno bisimulaciono ekvivalentni* ili skraćeno *BB-ekvivalentni*, i pišemo $\mathcal{A} \sim_{BB} \mathcal{B}$, ako postoji kompletna i sirjektivna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$.

Teorema 4.6.1. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat, E ekvivalencija na A, φ_E prirodno preslikavanje iz A u A/E i $\mathcal{A}/E = (A/E, \delta^{A/E}, \sigma^{A/E}, \tau^{A/E})$ faktor automat automata $\mathcal{A}$ u odnosu na E.*

Tada je φ_E direktna i povratna simulacija.

Takođe imamo da su sledeći uslovi ekvivalentni:

(i) *E je direktne bisimulacija na $\mathcal{A}$;*

(ii) *φ_E je direktna bisimulacija;*

(iii) *φ_E povratna-direktne bisimulacija.*

Dokaz. Uočimo da za proizvoljne $a_1, a_2 \in A$ imamo da je $\varphi_E(a_1) = E_{a_2}$ (tj. $(a_1, E_{a_2}) \in \varphi_E$) ako i samo ako je $(a_1, a_2) \in E$.

Za proizvoljne $x \in X$ i $a_1, a_2 \in A$ imamo da je

$$\begin{aligned}
(a_1, E_{a_2}) \in \delta_x^A \circ \varphi_E &\iff (\exists a_3 \in A)\ \big((a_1, a_3) \in \delta_x^A \wedge (a_3, E_{a_2}) \in \varphi_E\big) \\
&\iff (\exists a_3 \in A)\ \big((a_1, a_3) \in \delta_x^A \wedge (a_3, a_2) \in E\big) \\
&\iff (a_1, a_2) \in \delta_x^A \circ E \\
&\implies (a_1, a_2) \in E \circ \delta_x^A \circ E = E \circ E \circ \delta_x^A \circ E \\
&\iff (\exists a_3 \in A)\ \big((a_1, a_3) \in E \wedge (a_3, a_2) \in (E \circ \delta_x^A \circ E)\big) \\
&\iff (\exists a_3 \in A)\ \big((a_1, E_{a_3}) \in \varphi_E \wedge (E_{a_3}, E_{a_2}) \in \delta_x^{A/E}\big) \\
&\iff (a_1, E_{a_2}) \in \varphi_E \circ \delta_x^{A/E},
\end{aligned} \tag{4.66}$$

te je otuda $\delta_x^A \circ \varphi_E \subseteq \varphi_E \circ \delta_x^{A/E}$. Na sličan način možemo pokazati da je $\varphi_E^{-1} \circ \delta_x^A \subseteq \delta_x^{A/E} \circ \varphi_E^{-1}$.

Štaviše, za bilo koje $a \in A$ važi da je

$$a \in \sigma^A \implies E_a \in \sigma^{A/E} \wedge (E_a, a) \in \varphi_E^{-1} \implies a \in \sigma^{A/E} \circ \varphi_E^{-1},$$

odakle je $\sigma^A \subseteq \sigma^{A/E} \circ \varphi_E^{-1}$. Dalje imamo da je

$$E_a \in \sigma^A \circ \varphi_E \iff (\exists a' \in A)\ a' \in \sigma^A \wedge (a', E_a) \in \varphi_E \iff (\exists a' \in A)\ a' \in \sigma^A \wedge (a', a) \in E$$
$$\iff a \in \sigma^A \circ E \iff E_a \in \sigma^{A/E},$$

odakle proizilazi da je $\sigma^A \circ \varphi_E \subseteq \sigma^{A/E}$. Slično pokazujemo da je $\varphi_E^{-1} \circ \tau^A \subseteq \tau^{A/E}$ i $\tau^A \subseteq \varphi_E \circ \tau^{A/E}$.

Ovim smo dokazali da je φ_E direktna i povratna simulacija.

Suprotan smer u (**??**) (tj. φ_E^{-1} je direktna simulacija) važi ako i samo ako je E direktna bisimulacija na $\mathcal{A}$. Ovim smo dokazali ekvivalenciju uslova (i), (ii) i (iii). □

Teorema 4.6.2. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i E i F najveće direktne bisimulacione ekvivalencije na $\mathcal{A}$ i $\mathcal{B}$.*

Tada su $\mathcal{A}$ i $\mathcal{B}$ FB-ekvivalentni ako i samo ako su faktori automata $\mathcal{A}/E$ i $\mathcal{B}/F$ izomorfni.

Dokaz. Neka su $\mathcal{A}$ i $\mathcal{B}$ FB-ekvivalentni automati, tj. neka postoji kompletna i sirjektivna direktna bisimulacija $\psi \subseteq A \times B$. Na osnovu Teoreme **??**, postoji i najveća direktne bisimulacija φ iz $\mathcal{A}$ u $\mathcal{B}$, pri čemu je φ i parcijalna uniformna relacija. Kako je ψ kompletna i sirjektivna i važi da je $\psi \subseteq \varphi$, onda je φ takođe kompletna i sirjektivna, što znači da je φ uniformna direktna bisimulacija.

Prema Teoremi **??**, E_A^φ i E_B^φ su direktne bisimulacione ekvivalencije na $\mathcal{A}$ i $\mathcal{B}$, i $\widetilde{\varphi}$ je izomorfizam faktor automata $\mathcal{A}/E_A^\varphi$ i $\mathcal{B}/E_B^\varphi$. Neka P i Q označavaju redom najveće direktne bisimulacione ekvivalencije na $\mathcal{A}/E_A^\varphi$ i $\mathcal{B}/E_B^\varphi$. Na osnovu činjenice da je $\widetilde{\varphi}$ izomorfizam $\mathcal{A}/E_A^\varphi$ na $\mathcal{B}/E_B^\varphi$ dobijamo da za P i Q važi sledeća veza

$$(\alpha_1, \alpha_2) \in P \iff \big(\widetilde{\varphi}(\alpha_1), \widetilde{\varphi}(\alpha_2)\big) \in Q, \quad \text{za svako } \alpha_1, \alpha_2 \in A/E_A^\varphi,$$

pa možemo definisati izomorfizam $\xi : (\mathcal{A}/E_A^\varphi)/P \to (\mathcal{B}/E_B^\varphi)/Q$ sa $\xi(P_\alpha) = Q_{\widetilde{\varphi}(\alpha)}$, za svako $\alpha \in A/E_A^\varphi$.

Sada, prema Posledici **??**, $P = E/E_A^\varphi$ i $Q = F/E_B^\varphi$, te na osnovu Teoreme **??** dobijamo da je

$$\mathcal{A}/E \cong (\mathcal{A}/E_A^\varphi)/P \cong (\mathcal{B}/E_B^\varphi)/Q \cong \mathcal{B}/F,$$

što je i trebalo dokazati.

Suprotan smer sledi direktno iz Theorem **??**. □

Posledica 4.6.3. *Neka je $\mathcal{A}$ automat, E najveća direktna bisimulaciona ekvivalencija na $\mathcal{A}$ i $\mathbb{FB}(A)$ klasa automata koji su FB-ekvivalentni sa $\mathcal{A}$.*

Tada je $\mathcal{A}/E$ jedinstveni (do na izomorfizam) minimalni automat u $\mathbb{FB}(A)$.

Dokaz. Neka je $\mathcal{B}$ minimalni automat iz $\mathbb{FB}(A)$ i F najveća direktna bisimilaciona ekvivalencija na $\mathcal{B}$. Prema Teoremi **??** i (**??**), $\mathcal{B}/F$ takođe pripada $\mathbb{FB}(A)$. Kako je $\mathcal{B}$ minimalan u klasi $\mathbb{FB}(A)$, odavde sledi da je F relacija jednakosti. Sada, po Teoremi **??** dobijamo da je $\mathcal{B} \cong \mathcal{B}/F \cong \mathcal{A}/E$, što je trebalo dokazati. □

Prema Lemi **??**, FB-ekvivalentni automati raspoznaju iste jezike, ali obrat ne važi, kako ćemo pokazati sledećim primerom.

Primer 4.6.1. Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati gde je $|A| = 3$, $|B| = 2$ i $X = \{x\}$. Tranziciona relacija i skupovi inicijalnih i završnih stanja su predstavljeni sledećim Bulovim matricama i vektorima:

$$\delta_x^A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \sigma^A = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}, \quad \tau^A = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \quad \delta_x^B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \sigma^B = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad \tau^B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Ovi automati raspoznaju isti jezik, tj. $L = \{x\}$. Sa druge strane najveće direktne bisimulacione ekvivalencije E na $\mathcal{A}$ i F na $\mathcal{B}$ su relacije jednakosti, tj. $\mathcal{A}/E \cong \mathcal{A}$ i $\mathcal{B}/F \cong \mathcal{B}$. Ali, $\mathcal{A}$ i $\mathcal{B}$ imaju različiti broj stanja, te zato nisu izomorfni. Zaključujemo, prema Teoremi **??**, da $\mathcal{A}$ i $\mathcal{B}$ nisu FB-ekvivalentni.

4.7 Uniformne povratne-direktne bisimulacije

Teorema 4.7.1. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i neka je $\varphi \subseteq A \times B$ uniformna relacija. Tada je φ povratna-direktna bisimulacija ako i samo ako su zadovoljeni sledeći uslovi:*

(i) *E_A^φ je direktna bisimulaciona ekvivalencija na $\mathcal{A}$;*

(ii) *E_B^φ je povratna bisimulaciona ekvivalencija na $\mathcal{B}$;*

(iii) *$\widetilde{\varphi}$ je izomorfizam faktor automata $\mathcal{A}/E_A^\varphi$ i $\mathcal{B}/E_B^\varphi$.*

Dokaz. Zbog jednostavnijeg zapisa stavićemo, kao i do sada, da je $E = E_A^\varphi$ i $F = E_B^\varphi$. Na osnovu Teoreme **??**, imamo da je $E = \varphi \circ \varphi^{-1}$ i $F = \varphi^{-1} \circ \varphi$.

Neka je φ povratna-direktna bisimulacija. Tada je

$$E \circ \delta_x^A \circ E = \varphi \circ \varphi^{-1} \circ \delta_x^A \circ \varphi \circ \varphi^{-1} = \varphi \circ \varphi^{-1} \circ \varphi \circ \delta_x^B \circ \varphi^{-1} = \varphi \circ \delta_x^B \circ \varphi^{-1} = \delta_x^A \circ \varphi \circ \varphi^{-1} = \delta_x^A \circ E,$$
$$E \circ \tau^A = \varphi \circ \varphi^{-1} \circ \tau^A = \varphi \circ \varphi^{-1} \circ \varphi \circ \tau^B = \varphi \circ \tau^B = \tau^A,$$
$$F \circ \delta_x^B \circ F = \varphi^{-1} \circ \varphi \circ \delta_x^B \circ \varphi^{-1} \circ \varphi = \varphi^{-1} \circ \delta_x^A \circ \varphi \circ \varphi^{-1} \circ \varphi = \varphi^{-1} \circ \delta_x^A \circ \varphi = \varphi^{-1} \circ \varphi \circ \delta_x^B = F \circ \delta_x^B,$$
$$\sigma^B \circ F = \sigma^B \circ \varphi^{-1} \circ \varphi = \sigma^A \circ \varphi \circ \varphi^{-1} \circ \varphi = \sigma^A \circ \varphi = \sigma^B.$$

Otuda imamo da je $E = E_A^\varphi$ direktna bisimulaciona ekvivalencija na $\mathcal{A}$ i $F = E_B^\varphi$ povratna bisimulaciona ekvivalencija na $\mathcal{B}$. Kao i u dokazu Teoreme **??** može se pokazati da je $\widetilde{\varphi}$ izomorfizam automata $\mathcal{A}/E$ i $\mathcal{B}/F$.

Obrnuto, neka važe uslovi (i), (ii), i (iii). Za svako $\psi \in FD(\varphi)$, $\xi \in FD(\varphi^{-1})$, $a_1, a_2 \in A$, $b_1, b_2 \in B$ i $x \in X$, kao i u dokazu Teoreme **??** može se zaključiti da je

$$(a_1, a_2) \in (E \circ \delta_x^A \circ E) \Leftrightarrow (\psi(a_1), \psi(a_2)) \in (F \circ \delta_x^B \circ F),$$
$$(b_1, b_2) \in (F \circ \delta_x^B \circ F) \Leftrightarrow (\xi(b_1), \xi(b_2)) \in (E \circ \delta_x^A \circ E),$$

pa na osnovu (i) i (ii) dobijamo da je

$$\delta_x^A \circ \varphi = \delta_x^A \circ \varphi \circ \varphi^{-1} \circ \varphi = \delta_x^A \circ E \circ \varphi = E \circ \delta_x^A \circ E \circ \varphi = E \circ \delta_x^A \circ \varphi,$$
$$\varphi \circ \delta_x^B = \varphi \circ \varphi^{-1} \circ \varphi \circ \delta_x^B = \varphi \circ F \circ \delta_x^B = \varphi \circ F \circ \delta_x^B \circ F = \varphi \circ \delta_x^B \circ F.$$

Sada, za svako $a \in A$ i $b \in B$ dobijamo da je

$$\begin{aligned}(a,b) \in \delta_x^A \circ \varphi &\Leftrightarrow (a,b) \in E \circ \delta_x^A \circ \varphi \Leftrightarrow (\exists a_1 \in A)\ ((a,a_1) \in E \circ \delta_x^A \wedge (a_1,b) \in \varphi)\\ &\Leftrightarrow (\exists a_1 \in A)\ ((a,a_1) \in E \circ \delta_x^A \wedge (a_1,\xi(b)) \in E) \Leftrightarrow (a,\xi(b)) \in E \circ \delta_x^A \circ E\\ &\Leftrightarrow (\psi(a),\psi(\xi(b))) \in F \circ \delta_x^B \circ F \Leftrightarrow (\psi(a),b) \in F \circ \delta_x^B \circ F\\ &\Leftrightarrow (\exists b_1 \in B)\ ((\psi(a),b_1) \in F \wedge (b_1,b) \in \delta_x^B \circ F)\\ &\Leftrightarrow (\exists b_1 \in B)\ ((a,b_1) \in \varphi \wedge (b_1,b) \in \delta_x^B \circ F)\\ &\Leftrightarrow (a,b) \in \varphi \circ \delta_x^B \circ F\\ &\Leftrightarrow (a,b) \in \varphi \circ \delta_x^B,\end{aligned}$$

te je zato $\delta_x^A \circ \varphi = \varphi \circ \delta_x^B$. Kao i u dokazu Teoreme **??** analogno dobijamo da je $\tau^A = \varphi \circ \tau^B$ i $\sigma^A \circ \varphi = \sigma^B$. Zato je φ direktna-povratna bisimulacija. □

Teorema 4.7.2. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati, E direktna bisimulaciona ekvivalencija na $\mathcal{A}$ i F povratna bisimulaciona ekvivalencija na $\mathcal{B}$.*

Tada postoji uniformna povratna-direktna bisimulacija $\varphi \subseteq A \times B$ takva da je $E_A^\varphi = E$ i $E_B^\varphi = F$ ako i samo ako su faktor automati $\mathcal{A}/E$ i $\mathcal{B}/F$ isomorfni.

Dokaz. Ova teorema se na isti način dokazuje kao i Teorema **??**. □

U Teoremi **??** smo pokazali da za proizvoljnu ekvivalenciju E, prirodno preslikavanje φ_E je direktna bisimulacija ako i samo ako je povratna-direktna bisimulacija. Sada ćemo pokazati nešto opštije tvrđenje koje važi za proizvoljnu funkciju.

Teorema 4.7.3. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati, $\varphi : A \to B$ funkcija i $E = E_A^\varphi$ jezgro preslikavanja φ. Tada su sledeći uslovi ekvivalentni:*

(i) *φ je direktna bisimulacija;*

(ii) *φ je povratna-direktna bisimulacija;*

(iii) *E je direktna bisimulaciona ekvivalencija $\mathcal{A}$ i preslikavanje $\phi : A/E \to B$ definisano sa $\phi(E_a) = \varphi(a)$, za svako $a \in A$, je monomorfizam faktor automa $\mathcal{A}/E$ u $\mathcal{B}$.*

Dokaz. Posmatrajmo podautomat $\mathcal{C} = (C, \delta^C, \sigma^C, \tau^C)$ automata $\mathcal{B}$, gde je $C = \operatorname{Im}\varphi$.

(i) $\Longrightarrow$ (iii). Na osnovu Leme **??** imamo da je $\varphi \subseteq A \times C$ i φ predstavlja direktnu bisimulaciju iz $\mathcal{A}$ u $\mathcal{C}$. Takođe imamo da je φ sirjektivna funkcija iz A na C, pa je ona uniformna relacija iz A u C. Sada prema Teoremi **??** zaključujemo da je $E = E_A^\varphi$ direktna bisimulaciona ekvivalencija na $\mathcal{A}$, E_C^φ relacija jednakosti na C i $\widetilde{\varphi}$ izomorfizam iz $\mathcal{A}/E$ u $\mathcal{C}/E_B^\varphi \cong \mathcal{C}$. Ako identifikujemo $\mathcal{C}/E_B^\varphi$ i $\mathcal{C}$, onda se lako vidi da se $\widetilde{\varphi}$ može prestaviti preslikavanjem ϕ, gde je ϕ definisano u (iii), pa je ϕ monomorfizam iz $\mathcal{A}/E$ u $\mathcal{B}$.

(iii) $\Longrightarrow$ (i). Ovo je direktna posledica Teoreme **??**, jer je E_C^φ relacija jednakosti, a $\widetilde{\varphi}$ i ϕ se mogu identifikovati.

(i) $\Longleftrightarrow$ (ii). Ovo tvrđenje direktno važi iz Teorema **??** i **??**, jer je E_C^φ relacija jednakosti na C, pa je u isto vreme direktna i povratna bisimulaciona ekvivalencija. □

4.8 Slabe simulacije i bisimulacije

Neka je dat automat $\mathcal{A} = (A, X, \delta^A, \sigma^A, \tau^A)$. Za svako $u \in X^*$ definišimo podskupove σ_u^A i τ_u^A od A na sledeći način:

$$\sigma_u^A = \sigma^A \circ \delta_u^A, \qquad \tau_u^A = \delta_u^A \circ \tau^A. \tag{4.67}$$

Štaviše, za svako $a \in A$, *desni jezik* $\overrightarrow{L}_{\mathcal{A}}(a)$ i *levi jezik* $\overleftarrow{L}_{\mathcal{A}}(a)$ u odnosu na stanje a su jezici definisani sa

$$\overrightarrow{L}_{\mathcal{A}}(a) = \{u \in X^* \mid a \in \tau_u^A\}, \qquad \overleftarrow{L}_{\mathcal{A}}(a) = \{u \in X^* \mid a \in \sigma_u^A\}. \tag{4.68}$$

Drugim rečima, desni jezik od a je jezik raspoznat automatom dobijenim iz $\mathcal{A}$, tako što je σ^A zamenjeno sa $\{a\}$, a levi jezik od a je jezik raspoznat automatom dobijenim iz $\mathcal{A}$ tako što je τ^A zamenjeno sa $\{a\}$. Kada je jasno iz konteksta da se radi o jezicima automata $\mathcal{A}$, izostavićemo indeks $\mathcal{A}$ i pisati samo $\overrightarrow{L}(a)$ i $\overleftarrow{L}(a)$.

Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i $\varphi \subseteq A \times B$ neprazna relacija. Relaciju φ zovemo *slaba direktna simulacija* iz $\mathcal{A}$ u $\mathcal{B}$ ako važi da je

$$\varphi^{-1} \circ \tau_u^A \subseteq \tau_u^B, \quad \text{za svako } u \in X^*, \tag{4.69}$$
$$\sigma^A \subseteq \sigma^B \circ \varphi^{-1}, \tag{4.70}$$

takođe φ nazivamo *slaba povratna simulacija* iz $\mathcal{A}$ u $\mathcal{B}$ ako

$$\sigma_u^A \circ \varphi \subseteq \sigma_u^B, \quad \text{za svako } u \in X^*, \tag{4.71}$$
$$\tau^A \subseteq \varphi \circ \tau^B. \tag{4.72}$$

Dalje, φ je *slaba direktna bisimulacija* ako su φ i φ^{-1} slabe direktne simulacije, tj. ukoliko zadovoljavaju uslove (**??**), (**??**) i

$$\varphi \circ \tau_u^B \subseteq \tau_u^A, \quad \text{za svako } u \in X^*, \tag{4.73}$$
$$\sigma^B \subseteq \sigma^A \circ \varphi. \tag{4.74}$$

Slično, φ je *slaba povratna bisimulacija* ako su obe relacije φ i φ^{-1} slabe povratna simulacije, tj. ako zadovoljavaju relacije (**??**), (**??**) i

$$\sigma_u^B \circ \varphi^{-1} \subseteq \sigma_u^A, \quad \text{za svako } u \in X^*, \tag{4.75}$$
$$\tau^B \subseteq \varphi^{-1} \circ \tau^A. \tag{4.76}$$

Jednostavnosti radi, φ ćemo zvati *slaba simulacija* ako je ona slaba direktna ili slaba povratna simulacija i *slaba bisimulacija* ako je ona slaba direktna ili slaba povratna bisimulacija.

Lema 4.8.1. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i $\varphi \subseteq A \times B$ relacija. Tada važe sledeća tvrđenja*

(a) *Ako je φ slaba simulacija, onda je $L(\mathcal{A}) \subseteq L(\mathcal{B})$.*

(b) *Ako je φ slaba bisimulacija, onda je $L(\mathcal{A}) = L(\mathcal{B})$.*

(c) *Ako je φ direktna (povratna) simulacija, onda je ona i slaba direktna (povratna) simulacija.*

Dokaz. (a) Neka je φ slabe direktna simulacija. Tada za svako $u \in X^*$ imamo da je

$$\sigma^A \circ \delta_u^A \circ \tau^A = \sigma^A \circ \tau_u^A \subseteq \sigma^B \circ \varphi^{-1} \circ \tau_u^A \subseteq \sigma^B \circ \tau_u^B = \sigma^B \circ \delta_u^B \circ \tau^B,$$

i na osnovu (**??**) dobijamo da je $L(\mathcal{A}) \subseteq L(\mathcal{B})$. Slično, ako je φ slaba povratna simulacija, onda je $L(\mathcal{A}) \subseteq L(\mathcal{B})$.

(b) Ovaj deo dokaza direktno sledi iz (a).

(c) Neka je φ direktna simulacija. Korišćenjem Leme **??**, uslova (**??**) i **??** imamo da je

$$\varphi^{-1} \circ \tau_u^A = \varphi^{-1} \circ \delta_u^A \circ \tau^A \subseteq \delta_u^B \circ \varphi^{-1} \circ \tau^A \subseteq \delta_x^B \circ \tau^B = \tau_u^B.$$

Na sličan način dokazujemo iskaz vezan za povratne simulacije. □

Lema 4.8.2. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati. Relacija $\varphi \subseteq A \times B$ je slaba povratna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$ ako i samo ako je ona slaba direktna bisimulacija iz $\bar{\mathcal{A}}$ u $\bar{\mathcal{B}}$.*

Dokaz. Dokazaćemo tvrđenje za slučaj slabih simulacija, odakle direktno sledi tvrđenje teoreme. Na osnovu svojstava relacija (**??**) i (**??**) imamo

$$\sigma^A \circ \delta_u^A \circ \varphi \subseteq \sigma^B \circ \delta_u^B \iff (\varphi^{-1} \circ \overline{\delta_u^A} \circ \sigma^A)^{-1} \subseteq (\overline{\delta_u^B} \circ \sigma^B)^{-1} \iff \varphi^{-1} \circ \overline{\delta_u^A} \circ \sigma^A \subseteq \overline{\delta_u^B} \circ \sigma^B,$$

što je i trebalo dokazati. □

Prema prethodnoj lemi, za svaki iskaz validan za nedeterminističke automate, a odnosi se na slabe direktne bisimulacije, postoji odogovarajući iskaz za slabe povratne bisimulacije. Iz tog razloga, u nastavku ćemo razmatrati samo slabe direktne bisimulacije.

Sledeće tvrđenje se lako može pokazati.

Lema 4.8.3. *Kompozicija dve slabe direktne simulacije (bisimulacije) i unija proizvoljne familije slabih direktnih simulacija (bisimulacija) je takođe slaba direktna simulacija (bisimulacija).*

Sledećom teoremom dokazujemo fundamentalni rezultat vezan za slabe direktne simulacije i bisimulacije.

Teorema 4.8.4. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati takvi da postoji najmanje jedna slaba direktna simulacija iz $\mathcal{A}$ u $\mathcal{B}$.*

Tada postoji najveća slaba direktna simulacija λ iz $\mathcal{A}$ u $\mathcal{B}$ definisa sa

$$(a, b) \in \lambda \;\Leftrightarrow\; (\forall u \in X^*)\,(a \in \tau_u^A \;\Rightarrow\; b \in \tau_u^B), \tag{4.77}$$

za svako $a \in A$ i $b \in B$.

Dokaz. Neka je φ proizvoljna slaba direktna simulacija iz $\mathcal{A}$ u $\mathcal{B}$ i $(a, b) \in \varphi$. Za proizvoljno $u \in X^*$, ako je $a \in \tau_u^A$ onda je $b \in \varphi^{-1} \circ \tau_u^A \subseteq \tau_u^B$. Na ovaj način smo dokazali da je $(a, b) \in \lambda$, odakle zaključujemo da je svaka slaba direktna simulacija iz $\mathcal{A}$ u $\mathcal{B}$ sadržana u λ.

Takođe, ako je φ proizvoljna slaba direktna simulacija iz $\mathcal{A}$ u $\mathcal{B}$, onda je $\sigma^A \subseteq \sigma^B \circ \varphi^{-1} \subseteq \sigma^B \circ \lambda^{-1}$. Takođe, ako je $b \in \lambda^{-1} \circ \tau_u^A$, onda postoji $a \in \tau_u^A$ takvo da je $(b, a) \in \lambda^{-1}$, pa na osnovu (**??**) dobijamo da je $b \in \tau_u^B$. Zato je $\lambda^{-1} \circ \tau_u^A \subseteq \tau_u^B$, čime smo dokazali da je λ slaba direktna simulacija iz $\mathcal{A}$ u $\mathcal{B}$. Sada je jasno da je λ najveća slaba direktna simulacija iz $\mathcal{A}$ u $\mathcal{B}$. □

Posledica 4.8.5. *Neka su dati automati* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *takvi da postoji bar jedna slaba direktna simulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$ *i neka je* λ *najveća slaba direktna simulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$*. Tada je*

$$(a, b) \in \lambda \;\Leftrightarrow\; \overrightarrow{L}(a) \subseteq \overrightarrow{L}(b), \tag{4.78}$$

za svako $a \in A$ *i* $b \in B$*.*

Dokaz. Ovo je direktna posledica relacije (**??**) i činjenice da je $u \in \overrightarrow{L}(a)$ ako i samo ako je $a \in \tau_u^A$. □

Teorema 4.8.6. *Neka su* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *automati takvi da postoji bar jedna slaba direktna bisimulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$*.*

Tada postoji najveća slaba direktna bisimulacija μ *iz* $\mathcal{A}$ *u* $\mathcal{B}$ *definisana sa*

$$(a, b) \in \mu \;\Leftrightarrow\; (\forall u \in X^*)\,(a \in \tau_u^A \;\Leftrightarrow\; b \in \tau_u^B), \tag{4.79}$$

za svako $a \in A$ *i* $b \in B$*. Takođe je najveća slaba direktna bisimulacija* μ *i parcijalna uniforma relacija.*

Dokaz. Ova teorema se može dokazati na isti način kao i Teorema **??**. □

Posledica 4.8.7. *Neka su* $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ *i* $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ *automati takvi da postoji bar jedna slaba direktna bisimulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$ *i neka je* μ *najveća slaba direktna bisimulacija iz* $\mathcal{A}$ *u* $\mathcal{B}$*. Tada je*

$$(a, b) \in \mu \;\Leftrightarrow\; \overrightarrow{L}(a) = \overrightarrow{L}(b), \tag{4.80}$$

za svako $a \in A$ *i* $b \in B$*.*

Dokaz. Ova posledica se dokazuje na sličan način kao i Posledica **??**. □

Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ proizvoljni automat. Slabu direktnu bisimulaciju iz skupa $\mathcal{A}$ na samog sebe nazvaćemo *slaba direktna bisimulacija na* $\mathcal{A}$ (analogno definišemo *slabu povratnu bisimulaciju na* $\mathcal{A}$). Familija svih slabih direktnih bisimulacija na $\mathcal{A}$ je neprazna (sadrži relaciju jednakosti), pa prema Teoremi **??**, postoji najveća slaba direktna bisimulacija na $\mathcal{A}$, koja se definiše sa (**??**), pri čemu se lako može dokazati da je ona ekvivalencija. Slabu direktnu bisimulaciju na $\mathcal{A}$ koja je ekvivalencija nazvaćemo *slaba direktna bisimulaciona ekvivalencija* (analogno definišemo *slabu povratnu bisimulacionu ekvivalenciju*). Skup svih slabih direktnih bisimulacionih ekvivalencija na $\mathcal{A}$ označićemo sa $\mathcal{E}^{\mathrm{wfb}}(\mathcal{A})$.

Primetimo da je uslov (**??**) zadovoljen kada je $A = B$ i φ refleksivna relacija, pa je onda takođe zadovoljen kada je $A = B$ i φ ekvivalencija. Zato je ekvivalencija E na A slaba direktna bisimulacija na $\mathcal{A}$ ako i samo ako je

$$E \circ \tau_u^A \subseteq \tau_u^A, \quad \text{za svako } u \in X^*, \tag{4.81}$$

ili ekvivalentno

$$E \circ \tau_u^A = \tau_u^A, \quad \text{za svako } u \in X^*. \tag{4.82}$$

Analogno, ekvivalencija E na A je slaba povratna bisimulacija na $\mathcal{A}$ ako i samo ako je

$$\sigma_u^A \circ E \subseteq \sigma_u^A, \quad \text{za svako } u \in X^*, \tag{4.83}$$

ili ekvivalentno

$$\sigma_u^A \circ E = \sigma_u^A, \quad \text{za svako } u \in X^*. \tag{4.84}$$

Sledeća teorema se može dokazati na isti način kao i Teorema **??**.

Teorema 4.8.8. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat. Skup $\mathcal{E}^{\mathrm{wfb}}(\mathcal{A})$ svih slabih direktnih bisimulacionih ekvivalencija na $\mathcal{A}$ čini kompletnu mrežu. Ova mreža je kompletna podpolumreža u odnosu na uniju, mreže $\mathcal{E}(A)$ svih ekvivalencija na A.*

4.9 Uniformne slabe direktne bisimulacije

Teorema 4.9.1. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ dati automati i $\varphi \subseteq A \times B$ uniformna relacija. Tada je φ slaba direktna bisimulacija ako i samo ako važe sledeći uslovi:*

$$\sigma^A \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi, \qquad \sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}, \tag{4.85}$$

$$\varphi^{-1} \circ \tau_u^A = \tau_u^B, \quad \text{za svako } u \in X^*, \qquad \tau_u^A = \varphi \circ \tau_u^B, \quad \text{za svako } u \in X^*. \tag{4.86}$$

Dokaz. Neka je φ slaba direktna bisimulacija. Na osnovu (**??**) i (**??**) imamo da je

$$\sigma^A \circ \varphi \subseteq \sigma^B \circ \varphi^{-1} \circ \varphi \subseteq \sigma^A \circ \varphi \circ \varphi^{-1} \circ \varphi = \sigma^A \circ \varphi,$$

i zato $\sigma^A \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi$. Na sličan način dokazujemo da je $\sigma^B \circ \varphi^{-1} = \sigma^A \circ \varphi \circ \varphi^{-1}$.

Dalje, na osnovu refleksivnosti relacije $\varphi^{-1} \circ \varphi$, za svako $u \in X^*$ imamo da je

$$\tau_u^B \subseteq \varphi^{-1} \circ \varphi \circ \tau_u^B \subseteq \varphi^{-1} \circ \tau_u^A,$$

pa na osnovu ove inkluzije i (**??**) dobijamo da je $\tau_u^B = \varphi^{-1} \circ \tau_u^A$. Slično dokazujemo da je $\tau_u^A = \varphi \circ \tau_u^B$.

Obrnuto, neka važe (**??**) i (**??**). Jasno je da iz (**??**) slede (**??**) i (**??**). Takođe, na osnovu refleksivnosti $\varphi \circ \varphi^{-1}$ i $\varphi^{-1} \circ \varphi$ dobijamo

$$\sigma^A \subseteq \sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}, \qquad \sigma^B \subseteq \sigma^B \circ \varphi^{-1} \circ \varphi = \sigma^A \circ \varphi,$$

odakle važe (**??**) i (**??**). Zaključujemo da je φ slaba direktna bisimulacija. □

Lema 4.9.2. *Neka je dat automat $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$, ekvivalencija E na A i faktor automat $\mathcal{A}/E = (A/E, \delta^{A/E}, \sigma^{A/E}, \tau^{A/E})$ automata $\mathcal{A}$ u odnosu na ekvivalenciju E. Ako je E slaba direktna bisimulaciona ekvivalencija, onda je*

$$E_a \in \tau_u^{A/E} \;\Leftrightarrow\; a \in \tau_u^A, \tag{4.87}$$

za svako $u \in X^*$ i $a \in A$.

Dokaz. Tvrđenje ćemo dokazati indukcijom po dužini reči u.

Prema (**??**) i hipoteze leme, tvrđenje je tačno ako je u prazna reč. Pretpostavimo da je tvrđenje tačno za neku reč u i neka je $x \in X$ i $a \in A$. Tada imamo da je

$$\begin{aligned} E_a \in \tau_{xu}^{A/E} = \delta_x^{A/E} \circ \tau_u^{A/E} &\;\Leftrightarrow\; (\exists a' \in A)\ (\,(E_a, E_{a'}) \in \delta_x^{A/E} \;\wedge\; E_{a'} \in \tau_u^{A/E}\,) \\ &\;\Leftrightarrow\; (\exists a' \in A)\ (\,(a, a') \in E \circ \delta_x^A \circ E \;\wedge\; a' \in \tau_u^A\,) \\ &\;\Leftrightarrow\; a \in E \circ \delta_x^A \circ E \circ \tau_u^A = E \circ \delta_x^A \circ \tau_u^A = E \circ \tau_{xu}^A = \tau_{xu}^A. \end{aligned}$$

Dakle, tvrđenje je tačno za svako $u \in X^*$ i $a \in A$. □

Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ autommati i $\phi : A \to B$ bijektivno preslikavanje. Ako ϕ zadovoljava

$$a \in \sigma^A \;\Leftrightarrow\; \phi(a) \in \sigma^B, \qquad \text{za svako } a \in A, \tag{4.88}$$

$$a \in \tau^A_u \;\Leftrightarrow\; \phi(a) \in \tau^B_u, \qquad \text{za svako } u \in X^* \text{ and } a \in A, \tag{4.89}$$

onda ćemo preslikavanje ϕ nazvati *slabi direktni izomorfizam* između $\mathcal{A}$ i $\mathcal{B}$. Slično, ako ϕ zadovoljava

$$a \in \sigma^A_u \;\Leftrightarrow\; \phi(a) \in \sigma^B_u, \qquad \text{za svako } u \in X^* \text{ i } a \in A, \tag{4.90}$$

$$a \in \tau^A \;\Leftrightarrow\; \phi(a) \in \tau^B, \qquad \text{za svako } a \in A, \tag{4.91}$$

onda ćemo preslikavanje ϕ zvati *slabi povratni izomorfizam* između $\mathcal{A}$ i $\mathcal{B}$.

Teorema 4.9.3. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i $\varphi \subseteq A \times B$ uniformna relacija. Tada je φ slaba direktna bisimulacija ako i samo ako su sledeći uslovi zadovoljeni:*

(i) *E^φ_A je slabe direktna bisimulaciona ekvivlencija na $\mathcal{A}$;*

(ii) *E^φ_B je slaba direktna bisimulacija ekvivalencija na $\mathcal{B}$;*

(iii) *$\widetilde{\varphi}$ je slabi direktni izomorfizam faktor automata $\mathcal{A}/E^\varphi_A$ i $\mathcal{B}/E^\varphi_B$.*

Dokaz. Radi jednostavnijeg zapisa stavljamo da je $E^\varphi_A = E$ i $E^\varphi_B = F$. Takođe, neka je $f \in FD(\varphi)$ proizvoljni funkcionalni deskriptor relacije φ.

Neka je φ slaba direktna bisimulacija. Kako je $E = \varphi \circ \varphi^{-1}$ i $F = \varphi^{-1} \circ \varphi$, to su ove relacije direktne bisimulacione ekvivalencije, na osnovu Leme **??**.

Dalje, za proizvoljno $a \in A$ imamo da je

$$\begin{aligned} E_a \in \sigma^{A/E} \;&\Leftrightarrow\; a \in \sigma^A \circ E = \sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1} \;\Leftrightarrow\; (\exists b \in B)\,(\, b \in \sigma^B \;\wedge\; (a,b) \in \varphi\,) \\ &\Leftrightarrow\; (\exists b \in B)\,(\, b \in \sigma^B \;\wedge\; (f(a),b) \in F\,) \;\Leftrightarrow\; f(a) \in \sigma^B \circ F \;\Leftrightarrow\; F_{f(a)} \in \sigma^{B/F}, \end{aligned}$$

a za proizvoljno $u \in X^*$ i $a \in A$, na osnovu Leme **??** dobijamo da je

$$\begin{aligned} E_a \in \tau^{A/E}_u \;&\Leftrightarrow\; a \in \tau^A_u = \varphi \circ \tau^B_u \;\Leftrightarrow\; (\exists b \in B)\,(\,(a,b) \in \varphi \;\wedge\; b \in \tau^B_u\,) \\ &\Leftrightarrow\; (\exists b \in B)\,(\,(f(a),b) \in F \;\wedge\; b \in \tau^B_u\,) \;\Leftrightarrow\; f(a) \in F \circ \tau^B_u = \tau^B_u \;\Leftrightarrow\; F_{f(a)} \in \tau^{B/F}_u. \end{aligned}$$

Dakle, dokazali smo da je $\widetilde{\varphi} : E_a \mapsto F_{f(a)}$ slabi direktni izomorfizam između automata $\mathcal{A}/E^\varphi_A$ i $\mathcal{B}/E^\varphi_B$.

Obrnuto, neka važi (i), (ii) i (iii). Za proizvoljno $a \in A$ imamo da je

$$\begin{aligned} a \in \sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^A \circ E \;&\Leftrightarrow\; E_a \in \sigma^{A/E} \;\Leftrightarrow\; \widetilde{\varphi}(E_a) \in \sigma^{B/F} \;\Leftrightarrow\; F_{f(a)} \in \sigma^{B/F} \\ &\Leftrightarrow f(a) \in \sigma^B \circ F \Leftrightarrow\; (\exists b \in B)\,(\, b \in \sigma^B \;\wedge\; (b, f(a)) \in F\,) \\ &\Leftrightarrow (\exists b \in B)\,(\, b \in \sigma^B \;\wedge\; (a,b) \in \varphi\,) \;\Leftrightarrow\; a \in \sigma^B \circ \varphi^{-1}, \end{aligned}$$

te je $\sigma^A \circ \varphi \circ \varphi^{-1} = \sigma^B \circ \varphi^{-1}$, odakle sledi $\sigma^A \circ \varphi = \sigma^A \circ \varphi \circ \varphi^{-1} \circ \varphi = \sigma^B \circ \varphi^{-1} \circ \varphi$. Takođe, za proizvoljno $u \in X^*$ i $a \in A$ imamo da je

$$\begin{aligned} a \in \tau^A_u \;&\Leftrightarrow\; E_a \in \tau^{A/E}_u \;\Leftrightarrow\; \widetilde{\varphi}(E_a) \in \tau^{B/F}_u \;\Leftrightarrow\; F_{f(a)} \in \tau^{B/F}_u \\ &\Leftrightarrow\; f(a) \in \tau^B_u = F \circ \tau^B_u \Leftrightarrow\; (\exists b \in B)\,(\,(f(a),b) \in F \;\wedge\; b \in \sigma^B\,) \\ &\Leftrightarrow\; (\exists b \in B)\,(\,(a,b) \in \varphi \;\wedge\; b \in \sigma^B\,) \;\Leftrightarrow\; a \in \varphi \circ \tau^B_u. \end{aligned}$$

Zaključujemo da je $\tau_u^A = \varphi \circ \tau_u^B$, odakle sledi $\varphi^{-1} \circ \tau_u^A = \varphi^{-1} \circ \varphi \circ \tau_u^B = F \circ \tau_u^B = \tau_u^B$. Konačno, na osnovu Teoreme **??**, φ je slaba direktna bisimulacija. □

Teorema 4.9.4. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati, a E i F slabe direktne bisimulacione ekvivalencije na $\mathcal{A}$ i $\mathcal{B}$.*

Tada postoji uniformna slaba direktna bisimulacija $\varphi \subseteq A \times B$ takva da je $E_A^\varphi = E$ i $E_B^\varphi = F$ ako i samo ako postoji slabi direktni izomorfizam između faktor automata $\mathcal{A}/E$ i $\mathcal{B}/F$.

Dokaz. Ova teorema se dokazuje na isti način kao i Teorema **??**. □

Teorema 4.9.5. *Neka je $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ automat, E slaba direktna bisimulaciona ekvivalencija na $\mathcal{A}$ i F ekvivalencija na A takva da je $E \subseteq F$.*

Tada je F slaba direktna bisimulacion ekvivalencija na $\mathcal{A}$ ako i samo ako je F/E slaba direktna bisimulaciona ekvivalencija na $\mathcal{A}/E$.

Posledica 4.9.6. *Neka je dat automat $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i slabe direktne bisimulacione ekvivalencije E i F na $\mathcal{A}$, takve da je $E \subseteq F$.*

Tada je F najveća slaba direktna bisimulaciona ekvivalencija na $\mathcal{A}$ ako i samo ako je F/E najveća slaba direktna bisimulaciona ekvivalencija na $\mathcal{A}/E$.

Neka je dat automat $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i neka je $A_N = \{\sigma_u^A \mid u \in X^*\}$, za koji definišemo $\delta^{A_N} : A_N \times X \to A_N$ i $\tau^{A_N} \subseteq A_N$ sa

$$\delta^{A_N}(\sigma_u^A, x) = \sigma_{ux}^A, \tag{4.92}$$

$$\sigma_u^A \in \tau^{A_N} \;\Leftrightarrow\; \sigma_u^A \circ \tau^A = 1 \;\Leftrightarrow\; \sigma_u^A \cap \tau^A \neq \emptyset, \tag{4.93}$$

za svako $u \in X^*$ i $x \in X$. Tada je $\mathcal{A}_N = (A_N, \delta^{A_N}, \sigma_\varepsilon^A, \tau^{A_N})$ deterministički automat koji je jezički ekvivalentan sa $\mathcal{A}$, tj. $L(\mathcal{A}_N) = L(\mathcal{A})$ i naziva se *Nerodov automat* automata $\mathcal{A}$.

Takođe, neka je $\bar{A}_N = \{\tau_u^A \mid u \in X^*\}$ skup stanja za koji definišemo funkciju prelaza $\delta^{\bar{A}_N} : \bar{A}_N \times X \to \bar{A}_N$ i skup završnih stanja $\tau^{\bar{A}_N} \subseteq \bar{A}_N$ sa

$$\delta^{\bar{A}_N}(\tau_u^A, x) = \tau_{xu}^A, \tag{4.94}$$

$$\tau_u^A \in \tau^{\bar{A}_N} \;\Leftrightarrow\; \sigma^A \circ \tau_u^A = 1 \;\Leftrightarrow\; \sigma^A \cap \tau_u^A \neq \emptyset, \tag{4.95}$$

za svako $u \in X^*$ i $x \in X$. Tada je $\bar{\mathcal{A}}_N = (\bar{A}_N, \delta^{\bar{A}_N}, \tau_\varepsilon^A, \tau^{\bar{A}_N})$ deterministički automat izomorfan Nerodovom automatu reverzibilnog automata $\bar{\mathcal{A}}$ od $\mathcal{A}$, pa se naziva *reverzibilni Nerodov automat* od $\mathcal{A}$.

Sledeća teorema daje karakterizaciju uniformnih slabih direktnih bisimulacije u smislu reverzibilnog Nerodovog automata. Primetimo da analogna teorema data u terminima Nerodovog automata, karakteriše uniformne slabe povratne bisimulacije.

Teorema 4.9.7. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ automati i $\varphi \subseteq A \times B$ uniformna relacija.*

*Tada je φ slaba direktna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$ ako i samo ako su zadovoljeni uslovi (**??**) i (**??**), i funkcije*

$$\tau_u^A \mapsto \varphi^{-1} \circ \tau_u^A, \qquad \tau_u^B \mapsto \varphi \circ \tau_u^B, \tag{4.96}$$

moraju biti međusobno inverzni izomorfizni između reverzibilnih Nerodovih automata $\bar{\mathcal{A}}_N$ i $\bar{\mathcal{B}}_N$, za svako $u \in X^*$.

Dokaz. Posmatrajmo funkcije $\Phi : \bar{A}_N \to \mathcal{P}(B)$ i $\Psi : \bar{B}_N \to \mathcal{P}(A)$ date sa $\Phi(\tau_u^A) = \varphi^{-1} \circ \tau_u^A$ i $\Psi(\tau_u^B) = \varphi \circ \tau_u^B$, za svaki $u \in X^*$.

Neka je φ slaba direktna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$. Po definiciji imamo da ove funkcije zadovoljavaju (**??**) i (**??**). Na osnovu Teoreme **??**, za svako $u \in X^*$ imamo da je $\Phi(\tau_u^A) = \tau_u^B \in \bar{B}_N$ i $\Psi(\tau_u^B) = \tau_u^A \in \bar{A}_N$, što znači da Φ slika $\bar{A}_N$ u $\bar{B}_N$ i Ψ slika $\bar{B}_N$ u $\bar{A}_N$. Prema istoj teoremi, za svako $u \in X^*$ imamo da je $\Psi(\Phi(\tau_u^A)) = \varphi \circ \varphi^{-1} \circ \tau_u^A = \tau_u^B$ i $\Phi(\Psi(\tau_u^B)) = \varphi^{-1} \circ \varphi \circ \tau_u^B = \tau_u^B$, pa su zato Φ i Ψ međusobno inverzne bijekcije iz $\bar{A}_N$ u $\bar{B}_N$ i obrnuto.

Jasno da važi $\Phi(\tau^A) = \tau^B$ i $\Psi(\tau^B) = \tau^A$. Dalje, za proizvoljne $x \in X$ i $u \in X^*$ imamo da je

$$\Phi(\delta^{\bar{A}_N}(\tau_u^A, x)) = \Phi(\tau_{xu}^A) = \tau_{xu}^B = \delta^{\bar{B}_N}(\tau_u^B, x) = \delta^{\bar{B}_N}(\Phi(\tau_u^A), x).$$

Po Teoremi **??**, za svako $u \in X^*$ imamo da je $\sigma^A \circ \tau_u^A = \sigma^A \circ \varphi \circ \varphi^{-1} \circ \tau_u^A = \sigma^B \circ \varphi^{-1} \circ \tau_u^A = \sigma^B \circ \tau_u^B$, pa je zato

$$\tau_u^A \in \tau^{\bar{A}_N} \;\Leftrightarrow\; \sigma^A \circ \tau_u^A = 1 \;\Leftrightarrow\; \sigma^B \circ \tau_u^B = 1 \;\Leftrightarrow\; \tau_u^B \in \tau^{\bar{B}_N} \;\Leftrightarrow\; \Phi(\tau_u^A) \in \tau^{\bar{B}_N}.$$

Na ovaj način smo dokazali da je Φ izomorfizam iz $\bar{\mathcal{A}}_N$ u $\bar{\mathcal{B}}_N$. Slično dokazujemo da je Ψ izomorfizam iz $\bar{\mathcal{B}}_N$ u $\bar{\mathcal{A}}_N$.

Obrnuto, neka važi (**??**) i (**??**) i neka su Φ i Ψ međusobno inverzni izomorfizmi iz $\bar{\mathcal{A}}_N$ u $\bar{\mathcal{B}}_N$ i iz $\bar{\mathcal{B}}_N$ u $\bar{\mathcal{A}}_N$, redom. Kako su τ^A i τ^B jedinstvena inicijalna stanja automata $\bar{\mathcal{A}}_N$ i $\bar{\mathcal{B}}_N$, imamo da je $\Phi(\tau^A) = \tau^B$, te je zato $\varphi^{-1} \circ \tau^A = \tau^B$ i $\varphi \circ \tau^B = \tau^A$. Pretpostavimo da je $\Phi(\tau_u^A) = \tau_u^B$, za neko $u \in X^*$ i neka je $x \in X$. Tada je

$$\Phi(\tau_{xu}^A) = \Phi(\delta^{\bar{A}_N}(\tau_u^A, x)) = \delta^{\bar{B}_N}(\Phi(\tau_u^A), x) = \delta^{\bar{B}_N}(\tau_u^B, x) = \tau_{xu}^B.$$

Sada, indukcijom po dužini reči u dobijamo da je $\Phi(\tau_u^A) = \tau_u^B$ i $\Psi(\tau_u^B) = \tau_u^A$, za svako $u \in X^*$, odakle sledi jednakost (**??**). Konačno, na osnovu Teoreme **??** dobijamo da je φ slaba direktna bisimulacija. □

4.10 Slabo direktno bisimulaciono ekvivalentni automati

Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ dati automati. Ako postoji kompletna i sirjektivna slaba direktna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$, onda kažemo da su $\mathcal{A}$ i $\mathcal{B}$ *slabo direktno bisimulaciono ekvivalentni*, ili kraće *WFB-ekvivalentni* i pišemo $\mathcal{A} \sim_{WFB} \mathcal{B}$. Primetimo da svojstva kompletnosti i sirjektivnosti direktnih bisimulacija znače da je svako stanje iz $\mathcal{A}$ ekvivalentno nekom stanju u $\mathcal{B}$ i obrnuto. Za proizvoljne automate $\mathcal{A}$, $\mathcal{B}$ i $\mathcal{C}$ imamo da je

$$\mathcal{A} \sim_{WFB} \mathcal{A}; \quad \mathcal{A} \sim_{WFB} \mathcal{B} \implies \mathcal{B} \sim_{WFB} \mathcal{A}; \quad \big(\mathcal{A} \sim_{WFB} \mathcal{B} \wedge \mathcal{B} \sim_{WFB} \mathcal{C}\big) \implies \mathcal{A} \sim_{WFB} \mathcal{C}. \tag{4.97}$$

Slično, kažemo da su $\mathcal{A}$ i $\mathcal{B}$ *slabo povratno bisimulaciono ekvivalentni* ili kraće *WBB-ekvivalentni*, i pišemo $\mathcal{A} \sim_{WBB} \mathcal{B}$, ako postoji kompletna i sirjektivna slaba povratna bisimulacija iz $\mathcal{A}$ u $\mathcal{B}$.

Sledeća tvrđenja se na sličan način pokazuju kao i odgovarajuća tvrđenja Teorema **??** i Posledica **??**, za FB-ekvivalentne automate.

Teorema 4.10.1. *Neka su $\mathcal{A} = (A, \delta^A, \sigma^A, \tau^A)$ i $\mathcal{B} = (B, \delta^B, \sigma^B, \tau^B)$ dati automati i neka su E i F najveće slabe direktne bisimulacione ekvivalencije na $\mathcal{A}$ i $\mathcal{B}$.*

Tada su $\mathcal{A}$ i $\mathcal{B}$ WFB-ekvivalentni ako i samo ako postoji slabi direktni izomorfizam između faktor automata $\mathcal{A}/E$ i $\mathcal{B}/F$.

Posledica 4.10.2. *Neka je $\mathcal{A}$ automat, E najveća slaba direktna bisimulaciona ekvivalencija na $\mathcal{A}$ i $\mathbb{WFB}(A)$ klasa svih automata koji su WFB-ekvivalentni sa $\mathcal{A}$.*

Tada je $\mathcal{A}/E$ minimal automat u $\mathbb{WFB}(A)$. Štaviše, ako je $\mathcal{B}$ bilo koji minimalni automat u $\mathbb{WFB}(A)$, onda postoji slabi direktni izomorfizam između $\mathcal{A}/E$ i $\mathcal{B}$.

Glava 5

Prilog

U disertaciji su korišćeni razni programi za verifikaciju hipoteza i proveravanje rezultata. Pomoćni programi su razvijani u programskom paketu MATHEMATICA i u programskom jeziku *Java* (nalaženje energija grafa i PST, dijametra, komponenata povezanosti, klike, optimalnog bojenja grafa, itd).

5.1 MATHEMATICA kod za izračunanje i crtanje funkcije $F(t) = \exp(-\imath At)$

```
(* Calculating the exponential function $F(t)$ *)
 Options[createF] = {WorkingPrecision -> $MachinePrecision};
createF[HG_, t_, ops___] := Module[{wrprec, la, u, F, vec, proj},
      {wrprec} = {WorkingPrecision} /. {ops} /. Options[createF];
      Block[{$MinPrecision = wrprec},
        {la, u} = Eigensystem[N[HG, wrprec]];
        u = LinearAlgebra`Orthogonalization`GramSchmidt[u];
        proj = Table[vec = u[[i]];

            Table[vec[[j]]vec[[k]], {j, 1, Length[u]}, {k, 1, Length[u]}], {i,
               1, Length[u]}];
        F =
          Expand[Plus @@
             Table[Exp[I t la[[i]]]proj[[i]], {i, 1, Length[u]}]];
        ];
      Return[F];
      ];


(* Calculating the exponential function $F(t)$ between the vertices
u and v *)
 Options[FF] = {WorkingPrecision -> $MachinePrecision}; FF[HG_,
t_, u_, v_, ops___] := Module[{},
      Return[createF[HG, t, ops, Sequence @@ Options[F]][[u + 1, v + 1]]];
      ];

(* Visualization of the exponential function $F(t)$ between the
vertices u and v *)

 Plot[Abs[f], {t, 0, 10}, AxesOrigin -> {0, 0}]
```

5.2 MATHEMATICA kod za računanje energija ICG-ova

```
(* Ramanujan's function *)
c[i_,n_]:=MoebiusMu[n/GCD[i,n]]*(EulerPhi[n] /EulerPhi[n/GCD[i,n]]);

(* Calculating the energy of ICG *)
ICG [n_,Divs_]:=Module[
  {i,j,L,energy,lambda},
  energy=0;
  L={};
  For[i=1,i<=n,i++,
    lambda=0;
    For[j=1,j<=Length[Divs],j++,
      lambda+=c[i,n/Divs[[j]]];
    ];
    energy+=Abs[lambda];
    L=AppendTo[L,lambda];
  ];
  Print[energy," ",Mod[energy,4]];
  Return[L];
];

(* Generating all subsets *)
n=2*3*5;
Divs=Divisors[n];
S=Subsets[Divisors[n]];
A={};
For[i=1,i<=Length[S],i++,
  d=n;
  y=0;
  For[j=1,j<=Length[S[[i]]],j++,
    d=GCD[d,S[[i,j]]];
    If[n==S[[i,j]],y=1];
  ];
  If[d==1&&y==0,
    Print[S[[i]]];
    Print[ICG[n,S[[i]]]];
  ];
];

(* Calculating distance matrix i distance energy *)
DICG[n_, Divs_] := Module[
  {A, i, j, k, ZZ, DE, EE},
  A = {};
  For[i = 1, i <= n, i++,
   AA = {};
   For[j = 1, j <= n, j++,
```

```
    ok = 0;
    For[k = 1, k <= Length[Divs], k++,
     If[GCD[Abs[i - j], n] == Divs[[k]],
       ok = 1;
       Break[];
       ];
     ];
    If[ok == 1, AA = AppendTo[AA, 1], AA = AppendTo[AA, 0]];
    ];
   A = AppendTo[A, AA];
   ];
  ZZ = Eigenvalues[A];
  EE = 0;
  For[i = 1, i <= n, i++,
   EE = EE + Abs[ZZ[[i]]];
   ];

  (* FloydWarshall algorithm *)
  DD = A;
  For[k = 1, k <= n, k++,
   For[i = 1, i <= n, i++,
     If[DD[[i, k]] > 0,
       For[j = 1, j <= n, j++,
         If[DD[[k, j]] > 0,
           If[i != j,

             If[DD[[i, j]] == 0 ||
                DD[[i, j]] > DD[[i, k]] + DD[[k, j]],
               DD[[i, j]] = DD[[i, k]] + DD[[k, j]];
               ];
             ];
           ];
         ];
       ];
     ];
   ];

  ZZ = Eigenvalues[DD];
  DE = 0;
  For[i = 1, i <= n, i++,
   DE = DE + Abs[ZZ[[i]]];
   ];
  Print[Divs, " ", EE, " ", DE];
  ];
```

5.3 MATHEMATICA kod za generisanje ICG-ova sa PST

```
(* Calculating the eigenvalues of ICG_v(DD) *) Eigens[n_, DD_] :=
Module[{L, i, l, ev, t, cc, m, c},
      m = Length[DD];
      For[i = 1, i <= m, i++, c[i] = 1];
      L = Table[0, {n}];
      For[l = 1, l <= n, l++,
        ev = 0;
        For[i = 1, i <= m, i++,
```

```
          t = n/(DD[[i]]*GCD[n/DD[[i]], l - 1]);
          cc = MoebiusMu[t]*EulerPhi[n/DD[[i]]]/EulerPhi[t];
          (*If[l == 3, Print[cc]];*)
          ev = ev + c[i]*cc;
          ];
        L[[l]] = ev;
        ];
      Return[L];
      ];


(* Checking if ICG_n(DD) have PST *)
Ch[n_, DD_] := Module[{L, L1},
      L = Eigens[n, DD];
      L1 = Table[L[[i + 1]] - L[[i]], {i, Length[L] - 1}];
      (*Print[IntegerExponent[#, 2] & /@ L1];
        Print[Table[1, {Length[L] - 1}]*IntegerExponent[L1[[1]], 2]];*)
      Return[
        IntegerExponent[#, 2] & /@ L1 ==
          Table[1, {Length[L] - 1}]*IntegerExponent[L1[[1]], 2]];
      ];


(* List of all ICG having PST up to 100 vertices *)
 Module[{DD, SS, n, i, count},
  count = Table[{i, 0}, {i, 1, 100}];
  For [n = 2, n <= 100, n++,
    DD = Divisors[n] // Drop[#, -1] &;
    If [Length[DD] > 18, Print["Skipping ", n],
      SS = Subsets[DD];
      For [i = 2, i <= Length[SS], i++,
        If [GCD @@ (SS[[i]]~Join~{n}) == 1,
            If [Ch[n, SS[[i]]],
                count[[n, 2]]++;
                Print[n, " ", SS[[i]]];
                ];
            ];
        ];
      Print["Za ", n, "= ima svega ", count[[n, 2]]];
      ];
    ];
  count // TableForm
  ]
```

5.4 Java kod za nalaženje nekih parametara grafa

```
//testing the connectivity of a graph
public class Connected {
    private int n;
    private int [][] a;
    private int [] mark;
    private int components;
```

```
    public Connected (int n, int [][] a)
    {
        this.n = n;
        this.a = a;
        mark = new int [n];
    }

    private void DFS (int i)
    {
        mark [i] = components;
        for (int j = 1; j <= a [i][0]; j++)
        {
            if (mark [a [i][j]] == 0)
                DFS (a [i][j]);
        }
    }

    public void run ()
    {
        for (int i = 0; i < n; i++)
            mark [i] = 0;
        components = 0;
        for (int i = 0; i < n; i++)
        {
            if (mark [i] == 0)
            {
                components++;
                DFS (i);
            }
        }
    }

    public int [] solution()
    {
        return mark;
    }

    public int connected ()
    {
        return components;
    }

}


// calculating the diameter of a graph

import java.util.Vector;


public class Diameter {
    private int n;
    private int [][] a;
    private int diameter;

    public Diameter(int n, int [][] a)
```

```
    {
        this.n = n;
        this.a = a;
    }

    public void run ()
    {
        diameter = 0;
        int [] c = new int [n];
        Vector<Integer> queue = new Vector<Integer>();
        for (int start = 0; start < n; start++)
        {
            queue.clear();
            for (int i = 0; i < n; i++)
                c [i] = 0;
            queue.add(start);
            c [start] = 1;
            while (queue.size() > 0)
            {
                int i = queue.get(0);
                queue.remove(0);
                for (int j = 1; j <= a [i][0]; j++)
                {
                    if (c [a [i][j]] == 0)
                    {
                        queue.add(a [i][j]);
                        c [a [i][j]] = c [i] + 1;
                    }
                }
            }
            for (int i = 0; i < n; i++)
                if (c [i] > diameter)
                    diameter = c [i];
        }
    }

    public int diameter()
    {
        return diameter - 1;
    }

}

// finding clique

import java.util.Vector;

public class Clique {
    private int n;
    private int [][] a;
    private int cliqueNumber;
    private Vector<Integer> solution;
    private long startTime;

    public Clique(int n, int [][] a)
    {
```

```
        this.n = n;
        this.a = a;
        solution = new Vector<Integer>();
        cliqueNumber = 0;
    }

    private void find (Vector<Integer> clique, Vector<Integer> nSet, Vector<Integer> dSet)
    {
        if (System.currentTimeMillis() - startTime > 30000)
            return;
        if (nSet.size() == 0)
        {
            if (clique.size() > cliqueNumber)
            {
                solution.clear();
                for (int i = 0; i < clique.size(); i++)
                    solution.add(clique.get(i));
                cliqueNumber = solution.size();
            }
        }
        else
        {
            int v = nSet.get(0);
            nSet.remove(0);

            Vector<Integer> cliqueNew = new Vector<Integer>();
            for (int i = 0; i < clique.size(); i++)
                cliqueNew.add(clique.get(i));
            cliqueNew.add(v);
            Vector<Integer> nSetNew = new Vector<Integer>();
            for (int i = 1; i <= a [v][0]; i++)
                if (nSet.contains(a [v][i]))
                    nSetNew.add(a [v][i]);
            Vector<Integer> dSetNew = new Vector<Integer>();
            for (int i = 1; i <= a [v][0]; i++)
                if (dSet.contains(a [v][i]))
                    dSetNew.add(a [v][i]);
            find(cliqueNew, nSetNew, dSetNew);

            dSet.add(v);
            Vector<Integer> nodes = new Vector<Integer>();
            for (int i = 0; i < nSet.size(); i++)
            {
                boolean exist = false;
                for (int j = 1; j <= a [v][0]; j++)
                    if (a [v][j] == nSet.get(i))
                    {
                        exist = true;
                        break;
                    }
                if (exist == false)
                    nodes.add(nSet.get(i));
            }
            while (nodes.size() > 0)
            {
                int u = nSet.get(0);
```

```
                nSet.remove(0);
                int index = nodes.indexOf(u);
                if (index >= 0)
                    nodes.remove(index);

                cliqueNew.clear();
                for (int i = 0; i < clique.size(); i++)
                    cliqueNew.add(clique.get(i));
                cliqueNew.add(u);
                nSetNew.clear();
                for (int i = 1; i <= a [u][0]; i++)
                    if (nSet.contains(a [u][i]))
                        nSetNew.add(a [u][i]);
                dSetNew.clear();
                for (int i = 1; i <= a [u][0]; i++)
                    if (dSet.contains(a [u][i]))
                        dSetNew.add(a [u][i]);
                find(cliqueNew, nSetNew, dSetNew);
                dSet.add(u);
            }
        }
    }

    @SuppressWarnings("unchecked")
    public boolean run ()
    {
        startTime = System.currentTimeMillis();
        boolean completeGraph = true;
        for (int i = 0; i < n; i++)
            for (int j = 0; j < n; j++)
                if (a [i][0] < n - 1)
                {
                    completeGraph = false;
                    break;
                }
        if (completeGraph == true)
        {
            cliqueNumber = n;
            for (int i = 0; i < n; i++)
                solution.add(i);
            return true;
        }

        Vector<Integer> clique = new Vector<Integer>();
        Vector<Integer> nSet = new Vector<Integer>();
        Vector<Integer> dSet = new Vector<Integer>();
        for (int i = 0; i < n; i++)
        {
            clique.clear();
            nSet.clear();
            dSet.clear();
            clique.add(i);
            for (int j = 1; j <= a [i][0]; j++)
                nSet.add(a [i][j]);
            find (clique, nSet, dSet);
            if (System.currentTimeMillis() - startTime > 30000)
```

```
                return false;
        }
        return true;
    }

    public int cliqueNumber()
    {
        return cliqueNumber;
    }
    public Vector<Integer> solution()
    {
        return solution;
    }

}

// finding chromatic number

import java.util.Vector;

public class Chromatic {
    private int n;
    private int [][] a;
    private int chromaticNumber;
    private int [] solution;
    private int [] currentColor;
    private long startTime;
    private int limit;

    public Chromatic(int n, int [][] a, int limit)
    {
        this.n = n;
        this.a = a;
        this.solution = new int [n];
        this.limit = limit;
    }

    private int maxDSatur()
    {
        int node = -1;
        int max = -1;
        int [] mark = new int [n + 1];
        for (int i = 0; i < n; i++)
            if (currentColor [i] == 0)
            {
                for (int j = 0; j < n + 1; j++)
                    mark [j] = 0;
                int degree = 0;
                for (int k = 1; k <= a [i][0]; k++)
                {
                    int j = a [i][k];
                    if (currentColor [j] != 0)
                    {
                        mark [currentColor [j]]++;
                        if (mark [currentColor [j]] == 1)
                            degree++;
```

```
                }
            }
            if ((degree > max) || ((degree == max) && (a [i][0] > a [node][0])))
            {
                node = i;
                max = degree;
            }
        }
    return node;
}

@SuppressWarnings("unchecked")
public boolean run ()
{
    boolean completeGraph = true;
    for (int i = 0; i < n; i++)
        for (int j = 0; j < n; j++)
            if (a [i][0] < n - 1)
            {
                completeGraph = false;
                break;
            }
    if (completeGraph == true)
    {
        chromaticNumber = n;
        for (int i = 0; i < n; i++)
            solution [i] = i + 1;
        return true;
    }

    int start = 0;
    chromaticNumber = n + 1;
    currentColor = new int [n];
    int [] diffColors = new int [n];
    for (int i = 0; i < n; i++)
        currentColor [i] = 0;
    int [] p = new int [n];
    for (int i = 0; i < n; i++)
        p [i] = i;

    Vector<Integer> [] freeColor = new Vector [n];
    for (int i = 0; i < n; i++)
        freeColor [i] = new Vector<Integer>();

    int node = 0;
    Vector<Integer> nodeColors = new Vector<Integer>();
    nodeColors.add(1);
    freeColor [node].add(1);
    boolean mark [] = new boolean [n + 1];
    startTime = System.currentTimeMillis();

    while ((start >= 0) && (chromaticNumber > limit))
    {
        if (System.currentTimeMillis() - startTime > 30000)
            return false;
```

```
boolean backtrack = false;

for (int i = start; i < n; i++)
{
    if (i > start)
    {
        node = maxDSatur();
        p [i] = node;
        nodeColors.clear();
        for (int j = 0; j < n + 1; j++)
            mark [j] = true;
        for (int k = 1; k <= a [node][0]; k++)
            mark [currentColor [a [node][k]]] = false;
        for (int j = 1; j < chromaticNumber; j++)
            if (mark [j] == true)
                nodeColors.add(j);
    }
    if (nodeColors.size() > 0)
    {
        int newColor = nodeColors.get(0);
        currentColor [node] = newColor;
        nodeColors.remove(0);
        freeColor [node].clear();
        for (int j = 0; j < nodeColors.size(); j++)
            freeColor [node].add(nodeColors.get(j));
        if (i == 0)
            diffColors [i] = newColor;
        else
            diffColors [i] = Math.max(newColor, diffColors [i - 1]);
    }
    else
    {
        /* backtrack one position */
        start = i - 1;
        backtrack = true;
        break;
    }
}
if (backtrack == true)
{
    if (start >= 0)
    {
        node = p [start];
        currentColor [node] = 0;
        nodeColors = (Vector<Integer>)freeColor [node].clone();
    }
}
else
{
    for (int i = 0; i < n; i++)
        solution [i] = currentColor [i];
    chromaticNumber = diffColors [n - 1];
    for (int i = 0; i < n; i++)
        if (solution [p [i]] == chromaticNumber)
        {
            start = i - 1;
```

```
                    break;
                }
            if (start < 0)
                break;

            for (int i = start; i < n; i++)
                currentColor [p [i]] = 0;
            for (int i = 0; i <= start; i++)
            {
                node = p [i];
                for (int j = 0; j < freeColor[node].size(); j++)
                    if (freeColor [node].get (j) >= chromaticNumber)
                    {
                        freeColor [node].remove(j);
                        j--;
                    }
            }
            node = p [start];
            nodeColors = (Vector<Integer>)freeColor [node].clone();
        }
    }
    return true;
}

public int chromaticNumber()
{
    return chromaticNumber;
}

public int [] solution ()
{
    return solution;
}

}

//Graph visualisation

import java.awt.*; import java.util.Vector; import
javax.swing.JPanel;

public class CayleyGraph extends JPanel {
    private Color [] colors = {Color.BLUE, Color.RED, Color.YELLOW, Color.GREEN};
    private static final long serialVersionUID = 1L;
    private int n;
    private Vector<Integer> divisors;
    private Vector<Integer>[] adjList;
    private Vector<Integer>[] edgeColor;
    private int [] x;
    private int [] y;
    private int [] xx;
    private int [] yy;
    private int centerx, centery, r;

    public CayleyGraph ()
    {
```

```
        this.setBackground (Color.WHITE);
    }

    @SuppressWarnings("unchecked")
    public void setGraph(int n, Vector<Integer> divisors)
    {
        this.n = n;
        this.divisors = divisors;
        adjList = new Vector [n];
        for (int i = 0; i < n; i++)
            adjList [i] = new Vector<Integer>();
        edgeColor = new Vector [n];
        for (int i = 0; i < n; i++)
            edgeColor [i] = new Vector<Integer>();
    }

    public void makeGraph ()
    {
        for (int i = 0; i < n; i++)
            for (int j = 0; j < n; j++)
                if ((i > j) && (divisors.contains(Number.gcd (i - j, n)) == true))
                {
                    adjList [i].add(j);
                    adjList [j].add(i);
                    int tmp = divisors.indexOf(Number.gcd (i - j, n));
                    edgeColor [i].add(tmp);
                    edgeColor [j].add(tmp);
                }
        x = new int [n];
        y = new int [n];
        xx = new int [n];
        yy = new int [n];
        centerx = getSize().width / 2;
        centery = getSize().height / 2;
        r = Math.min(centerx, centery) - (int)(0.05 * getSize().width);

        double phi = (2 * Math.PI) / n;
        for (int i = 0; i < n; i++)
        {
            x [i] = centerx + (int)(r * Math.sin(phi * i));
            y [i] = centery + (int)(r * Math.cos(phi * i));
            xx [i] = centerx + (int)(r * 1.05 * Math.sin(phi * i));
            yy [i] = centery + (int)(r * 1.05 * Math.cos(phi * i));
        }
    }

    public int [][] getAdjList()
    {
        int [][] toReturn = new int [n][n + 1];
        for (int i = 0; i < n; i++)
        {
            for (int j = 0; j < adjList [i].size(); j++)
                toReturn [i][j + 1] = adjList [i].get(j);
            toReturn [i][0] = adjList [i].size();
        }
        return toReturn;
```

```
    }

    public void paintComponent(Graphics graphics)
    {
        Graphics2D g = (Graphics2D)graphics;
        super.paintComponent(g);
        g.setFont(new Font("Arial", Font.BOLD, 12));

        g.setColor(Color.BLACK);
        g.drawRect(0, 0, getSize().width - 1, getSize().height - 1);
        for (int i = 0; i < n; i++)
        {
            g.fillOval(x [i] - 2, y [i] - 2, 4, 4);
            g.drawString(Integer.toString(i), xx [i], yy [i]);
        }

        for (int i = 0; i < n; i++)
            for (int j = 0; j < adjList [i].size(); j++)
            {
                g.setColor(colors [edgeColor [i].get(j) % 4]);
                g.drawLine(x [i], y [i], x [adjList [i].get(j)], y [adjList [i].get(j)]);
            }
    }

    public void print()
    {
        for (int i = 0; i < n; i++)
        {
            System.out.println(i + ": ");
            for (int j = 0; j < adjList [i].size(); j++)
                System.out.print(adjList [i].get(j) + " ");
            System.out.println();
        }
    }

}




// conjecture testing

import java.util.Vector;

public class Number {

    public static Vector<Integer> findDivisors(int n)
    {
        Vector<Integer> divisors = new Vector<Integer>();
        for (int i = 1; i <= n; i++)
            if (n % i == 0)
                divisors.add(i);
        return divisors;
    }

    public static Vector<Integer> findPrimes (int n)
```

```
{
    Vector<Integer> primes = new Vector<Integer>();
    int m = n;
    for (int i = 2; i <= m; i++)
        if (n % i == 0)
        {
            primes.add(i);
            while (n % i == 0)
                n = n / i;
        }
    return primes;
}

public static int phi (int n)
{
    int toReturn = n;
    int p = 2;
    int limit = 1 + (int)Math.sqrt(n);
    while (p < limit)
    {
        if (n % p == 0)
        {
            toReturn = (p - 1) * (toReturn / p);
            while (n % p == 0)
                n = n / p;
        }
        p++;
        if (p % 2 == 0)
            p++;
    }
    if (n > 1)
        toReturn = (n - 1) * (toReturn / n);
    return toReturn;
}

public static int gcd (int a, int b)
{
    if (b == 0)
        return a;
    else
        return gcd (b, a % b);
}

private static int [] index;
private static int [] tuple;
private static int n;
private static int k;
private static Vector<int []> toReturn;

private static void find (int i)
{
    if (i == k)
        toReturn.add(tuple.clone());
    else
    {
        int min = 0;
```

```
            if (i > 0)
                min = tuple [i - 1];
            for (int j = min; j < n; j++)
                if (index [j] == 0)
                {
                    tuple [i] = j;
                    index [j] = 1;
                    find (i + 1);
                    index [j] = 0;
                    tuple [i] = 0;
                }
        }
    }


    public static int [][] subsets (Vector<Integer> set, int kk)
    {
        n = set.size();
        k = kk;
        index = new int [n];
        tuple = new int [k];
        for (int i = 0; i < n; i++)
            index [i] = 0;
        for (int i = 0; i < k; i++)
            tuple [i] = 0;
        toReturn = new Vector<int[]>();

        find (0);
        int [][] subsets = new  int [toReturn.size()][k];
        for (int i = 0; i < toReturn.size(); i++)
            for (int j = 0; j < k; j++)
                subsets [i][j] = set.get(toReturn.get(i)[j]);
        return subsets;
    }


    public static int minPrime (int n)
    {
        for (int i = 2; i <= n; i++)
            if (n % i == 0)
                return i;
        return 1;
    }


    public static int hypothesis (int n, Vector<Integer> set)
    {
        System.out.println("HIPOTEZA");
        int d = set.get(1);
        if (d == 1)
            d = set.get(0);

        Vector<Integer> nPrimes = findPrimes(n);
        Vector<Integer> dPrimes = findPrimes(d);
        if (nPrimes.size() == dPrimes.size())
            return minPrime(n) * minPrime(n / d);
```

```
        else if (d % minPrime(n) != 0)
            return minPrime(n);
        else
            return Math.max(minPrime(n), minPrime(n / d));
    }

    public static void test (int n, int d, int [] a, int [] b)
    {
        System.out.println(n + " " + d);
        int [] numbers = new int [a.length * b.length];
        int k = 0;
        for (int i = 0; i < a.length; i++)
            for (int j = 0; j < b.length; j++)
            {
                numbers [k] = a [i] * d + b [j];
                k++;
            }
        for (int i = 0; i < k; i++)
            for (int j = i + 1; j < k; j++)
                System.out.println(numbers [i] + " " + numbers [j] + " : " +
                 gcd (Math.abs(numbers [i] - numbers [j]), n));
    }

}
```

```
import java.util.Vector; import java.awt.*; import java.awt.event.*;
import java.io.BufferedWriter; import java.io.FileWriter; import
java.io.PrintWriter;

import javax.swing.*;

public class Main extends JPanel implements ActionListener {
    private static final long serialVersionUID = 1L;
    private static int n;
    private static int k;
    private static Vector<Integer> divisors;
    private static CayleyGraph graph;
    private static Chromatic chromatic;
    private static Clique clique;
    private static Diameter diameter;
    private static Connected connected;

    private JLabel nodeLabel;
    private JTextField nodeField;
    private JLabel divisorLabel;
    private JTextField divisorField;
    private JButton runButton;
    private JButton statButton;

    private JPanel createPanel()
    {
```

```
        JPanel panel = new JPanel();

        JPanel nodePanel = new JPanel();
        nodePanel.setPreferredSize(new Dimension(120, 60));
        nodeLabel = new JLabel("Nodes: ");
        nodeField = new JTextField(10);
        nodePanel.add(nodeLabel);
        nodePanel.add(nodeField);

        JPanel divisorPanel = new JPanel();
        divisorPanel.setPreferredSize(new Dimension(120, 60));
        divisorLabel = new JLabel("Divisors: ");
        divisorField = new JTextField(10);
        divisorPanel.add(divisorLabel);
        divisorPanel.add(divisorField);

        JPanel runPanel = new JPanel(new BorderLayout());
        runPanel.setPreferredSize(new Dimension(120, 60));
        runButton = new JButton("Run");
        runButton.setActionCommand("run");
        runButton.addActionListener(this);
        runPanel.add(runButton, BorderLayout.CENTER);

        JPanel statPanel = new JPanel(new BorderLayout());
        statPanel.setPreferredSize(new Dimension(120, 60));
        statButton = new JButton("Statistics");
        statButton.setActionCommand("statistics");
        statButton.addActionListener(this);
        statPanel.add(statButton, BorderLayout.CENTER);

        panel.add(nodePanel);
        panel.add(divisorPanel);
        panel.add(runPanel);
        panel.add(statPanel);
        return panel;
    }

    private void printVector (PrintWriter output, Vector<Integer> a)
    {
        output.print("{ ");
        for (int i = 0; i < a.size(); i++)
        {
            if (i < a.size() - 1)
                output.print(a.get(i) + ", ");
            else
                output.print(a.get(i));
        }
        output.println(" }");
    }

    private void printArray (PrintWriter output, int [] a)
    {
        output.print("{ ");
        for (int i = 0; i < a.length; i++)
        {
            if (i < a.length - 1)
```

```
            output.print(a [i] + ", ");
        else
            output.print(a [i]);
    }
    output.println(" }");
}

public Main()
{
    super();
    setPreferredSize(new Dimension (520, 600));
    divisors = new Vector<Integer>();
    graph = new CayleyGraph();
    graph.setPreferredSize(new Dimension(500, 500));
    this.add(graph);
    this.add(createPanel());
}

public void actionPerformed(ActionEvent action)
{
    if (action.getActionCommand().equals("run"))
    {
        try
        {
            divisors.clear();
            String [] tmp = divisorField.getText().split(" ");
            for (int i = 0; i < tmp.length; i++)
                divisors.add(Integer.parseInt(tmp [i]));

            PrintWriter output =
            new PrintWriter(new BufferedWriter(new FileWriter("result.txt")));
            n = Integer.parseInt(nodeField.getText());
            output.println("Number of nodes: " + n);
            printVector(output, divisors);
            output.println();

            graph.setGraph(n, divisors);
            graph.makeGraph();
            graph.repaint();
            //graph.print();
            boolean ok = true;
            System.out.println("PRINT");

            System.out.println("CLIQUE");
            clique = new Clique(n, graph.getAdjList());
            ok = ok & clique.run();
            chromatic = new Chromatic(n, graph.getAdjList(), clique.cliqueNumber());
            ok = ok & chromatic.run();
            System.out.println("CHROMATIC");
            diameter = new Diameter(n, graph.getAdjList());
            diameter.run();
            System.out.println("DIAMETER");
            connected = new Connected (n, graph.getAdjList());
            connected.run();

            output.println("OK = " + ok);
```

```
            output.println("ChiNum = " + chromatic.chromaticNumber());
            printArray(output, chromatic.solution());
            output.println("Omega = " + clique.cliqueNumber() + "\t");
            printVector(output, clique.solution());
            output.println("Diameter = " + diameter.diameter());
            output.println("Connected = " + connected.connected());
            if (connected.connected() != 1)
                printArray (output, connected.solution());
            output.println();

            String result = "";
            result += "OK = " + ok + "\n";
            result += "ChiNum = " + chromatic.chromaticNumber() + "\n";
            result += "Omega = " + clique.cliqueNumber() + " " + "\n";
            result += "Diameter = " + diameter.diameter() + "\n";
            result += "Connected = " + connected.connected();
            JOptionPane.showMessageDialog(null, result,
            "Results", JOptionPane.INFORMATION_MESSAGE);
            output.close();
        }
        catch (Exception ex)
        {
            JOptionPane.showMessageDialog(null, "Input Error!",
            "Error", JOptionPane.ERROR_MESSAGE);
        }
    }
    else if (action.getActionCommand().equals("statistics"))
    {
        try
        {
            n = Integer.parseInt(nodeField.getText());
            k = Integer.parseInt(divisorField.getText());
            divisors = Number.findDivisors(n);

            PrintWriter output =
            new PrintWriter(new BufferedWriter(new FileWriter("statistics.txt")));
            output.println("Number of nodes: " + n);
            output.println("Number of divisors: " + k);
            printVector(output, divisors);
            output.println();

            int [][] subsets = Number.subsets(divisors, k);
            for (int i = 0; i < subsets.length; i++)
            {
                System.out.println(i);
                divisors.clear();
                for (int j = 0; j < k; j++)
                    divisors.add(subsets [i][j]);
                printVector(output, divisors);
                if (divisors.get(0) != 1)
                    continue;

                graph.setGraph(n, divisors);
                graph.makeGraph();
                boolean ok = true;
                clique = new Clique(n, graph.getAdjList());
```

```
                ok = ok & clique.run();
                chromatic = new Chromatic(n, graph.getAdjList(), clique.cliqueNumber());
                ok = ok & chromatic.run();
                diameter = new Diameter(n, graph.getAdjList());
                diameter.run();
                connected = new Connected (n, graph.getAdjList());
                connected.run();

                output.println("OK = " + ok);
                output.println("ChiNum = " + chromatic.chromaticNumber());
                printArray(output, chromatic.solution());
                output.println("Omega = " + clique.cliqueNumber() + "\t");
                printVector(output, clique.solution());
                output.println("Diameter = " + diameter.diameter());
                output.println("Connected = " + connected.connected());
                if (connected.connected() != 1)
                    printArray (output, connected.solution());
                output.println();
            }
            output.close();
            JOptionPane.showMessageDialog(null, "Done!",
            "Results", JOptionPane.INFORMATION_MESSAGE);
        }
        catch (Exception ex)
        {
            ex.printStackTrace();
            JOptionPane.showMessageDialog(null, "Input Error!",
            "Error", JOptionPane.ERROR_MESSAGE);
        }
    }
}

private static void createAndShowGUI()
{
    JFrame frame = new JFrame("Cayley Graphs");
    frame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);

    Main ContentPanel = new Main();
    ContentPanel.setOpaque(true);
    frame.setContentPane(ContentPanel);

    frame.pack();
    frame.setLocationRelativeTo(null);
    frame.setVisible(true);
}

public static void main(String[] args)
{
    javax.swing.SwingUtilities.invokeLater(new Runnable()
    {
        public void run()
        {
            createAndShowGUI();
        }
    }
}
```

```
}
```

Literatura

[1] L. Aceto, A. Ingolfsdottir, K. G. Larsen, J. Srba, *Reactive Systems: Modelling, Specification and Verification*, Cambridge University Press, Cambridge, 2007.

[2] A. Ahmadi, R. Belk, C. Tamon and C. Wendler, *On mixing of continuoustime quantum walks on some circulant graphs*, Quantum Information & Computation 3 (2003) 611-618.

[3] G. Arfken, *Mathematical Methods for Physicists*, 3rd ed. Orlando, FL: Academic Press, pp. 211–212, 1985.

[4] K. Balinska, D. Cvetković, Z. Radosavljević, S. Simić, D. Stevanović, *A survey on integral graphs*, Univerzitet Beograd, Publ. Elektrotehn. Fak. Ser. Mat., (13), 2002, 42–65.

[5] W. Bandler, L.J. Kohout, *Fuzzy relational products as a tool for analysis and synthesis of the behaviour of complex natural and artificial systems*, in: S.K. Wang, P.P. Chang (Eds.), Fuzzy Sets: Theory and Application to Policy Analysis and Information Systems, Plenum Press, New York, 1980, pp. 341–367.

[6] R. B. Bapat, S. Pati, *Energy of a graph is never an odd integer*, Bulletin of Kerala Mathematics Association 1 (2004) 129–132.

[7] M. Bašić, *Perfect state transfer between non-antipodal vertices in integral circulant graphs*, Ars Combinatoria (to appear).

[8] M. Bašić, *Characterization of circulant graphs having perfect state transfer*, Quantum Information & Computation (to appear).

[9] M. Bašić, *Which weighted circulant networks have perfect state transfer?*, (submitted manuscript).

[10] M. Bašić, A. Ilić, *On the clique number of integral circulant graphs*, Applied Mathematics Letters, Volume 22, Issue 9, September 2009, Pages 1406-1411.

[11] M. Bašić, A. Ilić, *On the authomorphism group of integral circulant graphs*, The Electronic Journal of Combinatorics (to appear).

[12] M. Bašić, M.D. Petković, *Some classes of integral circulant graphs allowing and not allowing perfect state transfer*, Applied Mathematics Letters, Volume 22, Issue 10, October 2009, Pages 1609-1615.

[13] M. Bašić, M.D. Petković, *Perfect state transfer in integral circulant graphs with non square-free order*, Linear Algebra and its Application, Volume 433, Issue 1, July 2010, Pages 149-163.

[14] M. Bašić, M.D. Petković, D. Stevanović, *Perfect state transfer in integral circulant graphs*, Applied Mathematics Letters, Volume 22, Issue 7, July 2009, Pages 1117-1121.

[15] P. Berrizbeitia, R.E. Giudic, *On cycles in the sequence of unitary Cayley graphs*, Discrete Mathematics 282 (2004), 239–243.

[16] E. Bertram, P. Horak, *Some applications of graph theory to other parts of mathematics*, The Mathematical Intelligencer (Springer-Verlag, New York) (1999) 6-11.

[17] S. L. Bloom, Z. Ésik, *Iteration Theories: The Equational Logic of Iterative Processes*, EATCS Monographs on Theoretical Computer Science, Springer, Berlin-Heilderberg, 1993.

[18] T. Brihaye, *Words and bisimulations of dynamical systems*, Discrete Mathematics and Theoretical Computer Science 9 (2) (2007) 11–32.

[19] P. Buchholz, *Bisimulation relations for weighted automata*, Theoretical Computer Science 393 (2008) 109–123.

[20] S. Burris, H. P. Sankappanavar, *A Course in Universal Algebra*, Springer-Verlag, New York, 1981.

[21] C. S. Calude, E. Calude, B. Khoussainov, *Finite nondeterministic automata: Simulation and minimality*, Theoretical Computer Science 242 (2000) 219–235.

[22] P. Cameron, *Permutation Groups*, London Mathematical Society Student Texts, 45, Cambridge University Press, ISBN 978-0-521-65378-7, (1999).

[23] C. Câmpeanu, N. Sântean, S. Yu, *Mergible states in large NFA*, Theoretical Computer Science 330 (2005) 23–34.

[24] R.J. Angeles-Canul, R.M. Norton, M.C. Opperman, C.C. Paribello, M.C. Russell, C. Tamonk, *Perfect state transfer, integral ciculants and join of graphs*, Quantum Information & Computation 10 (2010) 325-342.

[25] R.J. Angeles-Canul, R.M. Norton, M.C. Opperman, C.C. Paribello, M.C. Russell, C. Tamonk, *Quantum perfect state transfer on weighted join graphs*, International Journal of Quantum Information 7 (2009), 1429–1445.

[26] C. G. Cassandras, S. Lafortune, *Introduction to Discrete Event Systems*, Springer, 2008.

[27] J.-M. Champarnaud, F. Coulon, *NFA reduction algorithms by means of regular inequalities*, Theoretical Computer Science 327 (2004) 241–253.

[28] A. Childs, E. Farhi, S. Gutmann, *An example of the difference between quantum and classical random walks*, Quantum Information Processing 1, 35 (2002).

[29] M. Ćirić, M. Droste, J. Ignjatović, H. Vogler, *Determinization of weighted finite automata over strong bimonoids*, Information Sciences 180 (2010) 3497–3520.

[30] M. Ćirić, J. Ignjatović, M. Bašić, I. Jančić, *Bisimulations for non-deterministic automata*, (submitted manuscript).

[31] M. Ćirić, J. Ignjatović, S. Bogdanović, *Uniform fuzzy relations and fuzzy functions*, Fuzzy Sets and Systems 160 (2009) 1054–1081.

[32] M. Ćirić, J. Ignjatović, N. Damljanović, M. Bašić, *Bisimulations for fuzzy automata*, Fuzzy Sets and Systems (to appear).

[33] M. Ćirić, A. Stamenković, J. Ignjatović, T. Petković, *Factorization of fuzzy automata*, In: Csuhaj-Varju, E., Ésik, Z. (eds.), FCT 2007, Springer, Heidelberg, Lecture Notes in Computer Science 4639 (2007) 213–225.

[34] M. Ćirić, A. Stamenković, J. Ignjatović, T. Petković, *Fuzzy relation equations and reduction of fuzzy automata*, Journal of Computer and System Sciences 76 (2010) 609–633.

[35] M. Christandl, N. Datta, A. Ekert, A.J. Landahl, *Perfect state transfer in quantum spin networks*, Physical Review Letters 92 (2004), 187902 [quant-ph/0309131].

[36] M. Christandl, N. Datta, T.C. Dorlas, A. Ekert, A. Kay, A.J. Landahl, *Perfect transfer of arbitrary states in quantum spin networks*, Physical Review Letters A 71 (2005), 032312.

[37] T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to Algorithms*, Second edition, MIT Press. New York, 2001.

[38] D. Cvetković, M. Doob, H. Sachs, *Spectra of graphs – Theory and Application*, Johann Ambrosius Barth Verlag, Third edition, 1995.

[39] D. Cvetković, P. Rowlinson, S. Simić, *Eigenspaces of Graphs*, Cambridge University Press, Cambridge, 1997.

[40] H. Davenport, The Heigher Arithmetic, 7th ed., Cambrige University Press, 1999.

[41] B. De Baets, E. Kerre, *The cutting of compositions*, Fuzzy Sets and Systems 62 (1994) 295–309.

[42] M. De Cock, E. E. Kerre, *Fuzzy modifiers based on fuzzy relations*, Information Sciences 160 (2004) 173–199.

[43] P. Diaconis, *Asymptotic Expansions for the Mean and Variance of the Number of Prime Factors of a Number*, Dept. Statistics Tech. Report 96, Stanford, CA: Stanford University, 1976.

[44] E. Dobson, I. Kovács, *Automorphism groups of Cayley digraphs of* Z_p^3, The Electronic Journal of Combinatorics 16 (2009) #R149.

[45] E. Dobson, *Automorphism groups of metacirculant graphs of order a product of two distinct primes*, Combinatorics Probability and Computing 15 (2006) 105–130.

[46] E. Dobson, J. Morris, *On automorphism groups of circulant digraphs of square-free order*, Discrete Mathematics, 299 (2005) 79–98.

[47] A. Dovier, C. Piazza, A. Policriti, *An efficient algorithm for computing bisimulation equivalence*, Theoretical Computer Science 311 (2004) 221–256.

[48] M. Dugić, *Osnove kvantne informatike i kvantnog računanja*, Prirodno-matematički fakulet, Kragujevac, 2009.

[49] E. Farhi, S. Gutmann, *Quantum computation and decision trees*, Physical Review Letters A 58, 915 (1998), quant-ph/9706062.

[50] S. Finch, *Two Asymptotic Series*, http://algo.inria.fr/bsolve/.

[51] E. Fuchs, *Longest induced cycles in circulant graphs*, The Electronic Journal of Combinatorics 12 (2005), 1–12.

[52] M. R. Garey, D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, Freeman, San Francisco, 1979.

[53] Y. Ge, *Elementary Properties of Cyclotomic Polynomials*, Mathematical Reflections 2 (2008).

[54] R. Gentilini, C. Piazza, A. Policriti, *From bisimulation to simulation: Coarsest partition problems*, Journal of Automated Reasoning 31 (2003) 73–103.

[55] C. Godsil, *Periodic Graphs*, arXiv:0806.2074v1 [math.CO] 12 Jun 2008.

[56] C. Godsil, G. Royle, *Algebraic Graph Theory*, New York: Springer-Verlag, 2004.

[57] D. Griffiths, *Introduction to Elementary Particles*, New York: Wiley, 1987.

[58] G.R. Grimmett and D.R. Stirzaker , *Probability and Random Processes*, Oxford University Press, 1984.

[59] I. Gutman, *Uvod u hemijsku teoriju grafova*, Prirodno-matematički fakulet, Kragujevac, 2003.

[60] F. Harary, *Graph Theory*, MA: Addison-Wesley, 1994.

[61] F. Harary, A. Schwenk, *Which graphs have integral spectra?*, in: R. Bari, F. Harary (Eds.), Graphs and Combinatorics, Springer, Berlin, 1974, p. 45.

[62] G.H. Hardy, E.M. Wright, *An introduction to the Theory of Numbers*, 5th ed, Clarendon Press, Oxford University Press, New York, 1979.

[63] T. A. Henzinger, P. W. Kopke, A. Puri, P. Varaiya, *What's decidable about hybrid automata?* Journal of Computer and System Sciences 57 (1998) 94–124.

[64] F. Herbut, *Kvantna mehanika*, Prirodno-matematički fakultet, Beograd, 1984.

[65] J. Högberg, A. Maletti, J. May, *Backward and forward bisimulation minimisation of tree automata*, in: J. Holub, J. Žďárek (eds.), IAA07, Springer, Heidelberg, Lecture Notes in Computer Science 4783 (2007) 109–121.

[66] J. Högberg, A. Maletti, J. May, *Backward and forward bisimulation minimisation of tree automata*, Theoretical Computer Science 410 (2009) 3539–3552.

[67] F.K. Hwang, *A survey on multi-loop networks*, Theoretical Computer Science 299 (2003), 107–121.

[68] J. Ignjatović, M. Ćirić, S. Bogdanović, *Determinization of fuzzy automata with membership values in complete residuated lattices*, Information Sciences 178 (2008) 164–180.

[69] J. Ignjatović, M. Ćirić, S. Bogdanović, *Fuzzy homomorphisms of algebras*, Fuzzy Sets and Systems 160 (2009), 2345–2365.

[70] J. Ignjatović, M. Ćirić, S. Bogdanović, T. Petković, *Myhill-Nerode type theory for fuzzy languages and automata*, Fuzzy Sets and Systems 161 (2010) 1288-1324.

[71] A. Ilić, *The energy of unitary Cayley graphs*, Linear Algebra and its Applications 431 (2009), 1881–1889.

[72] A. Ilić, *Distance spectra and Distance energy of integral circulant graphs*, Linear Algebra Appl. 433 (2010), 1005–1014.

[73] A. Ilić, M. Bašić, *On the chromatic number of integral circulant graphs*, Computers & Mathematics with Applications 60 (2010), 144–150.

[74] A. Ilić, M. Bašić, I Gutman, *Triply Equienergetic Graphs*, MATCH Commun. Math. Comput. Chem. 64 (2010) 189–200.

[75] A. Ilić, M. Bašić, *New results on the energy of integral circulant graphs*, submitted manuscript.

[76] L. Ilie, S. Yu, *Algorithms for computing small NFAs*, in: K. Diks et al. (eds): MFCS 2002, Lecture Notes in Computer Science 2420 (2002) 328–340.

[77] L. Ilie, S. Yu, *Reducing NFAs by invariant equivalences*, Theoretical Computer Science 306 (2003) 373–390.

[78] L. Ilie, G. Navarro, S. Yu, *On NFA reductions*, in: J. Karhumäki et al. (eds): Theory is Forever, Lecture Notes in Computer Science 3113 (2004) 112–124.

[79] L. Ilie, R. Solis-Oba, S. Yu, *Reducing the size of NFAs by using equivalences and preorders*, in: A. Apostolico, M. Crochemore, and K. Park (Eds): CPM 2005, Lecture Notes in Computer Science 3537 (2005) 310–321.

[80] M.A. Jafarizadeh, R. Sufiani, *Perfect state transfer over distance- regular spin networks*, Physical Review A 77, 022315 (2008).

[81] B.E. Kane, Nature 393, 133 (2003)

[82] P. C. Kannellakis, S. A. Smolka, *CCS expressions, finite state processes, and three problems of equivalence*, Information and Computation 86 (1990) 43–68.

[83] J. Kempe, *Quantum Random Walks Hit Exponentially Faster*, Probability Theory and Related Fields 133(2005), 215–235.

[84] H. J. Kim: *Finding Clique using Backtracking Algorithm*, `http://www.ibluemojo.com/school/clique_algorithm.html`.

[85] F. Klawonn, *Fuzzy points, fuzzy relations and fuzzy functions*, in: V. Novâk and I. Perfilieva (Eds.), Discovering World with Fuzzy Logic, Physica-Verlag, Heidelberg, 2000, pp. 431–453.

[86] M. Klin, I. Kovács, *Automorphism groups of rational circulant graphs through the use of Schur rings*, arXiv:1008.0751 [math.CO], 2010.

[87] W. Klotz, *Graph Coloring Algorithms*, Mathematik-Bericht 5 (2002), 1–9.

[88] W. Klotz, T. Sander, *Some properties of unitary Cayley graphs*, The Electronic Journal Of Combinatorics 14 (2007), #R45.

[89] W. Klotz, T. Sander, *Integral Cayley graphs over abelian groups*, Electron. J. Combin. 17 (2010), #R81.

[90] D.E. Knuth, *Selected Papers on Analysis of Algorithms*, Stanford, CA: CSLI Publications, 2000, pp. 338–339.

[91] Lj. Kočinac, *Linearna algebra i analitička geometrija*, Prosveta, Niš, 1997.

[92] I. Kovács, *On automorphisms of circulant digraphs on p^m vertices, p an odd prime*, Linear Algebra Appl. 356 (2002) 231–252.

[93] D. C. Kozen, *Automata and Computability*, Springer, 1997.

[94] C. H. Li, *On isomorphisms of connected Cayley graphs*, Discrete Math. 178 (1998) 109–122.

[95] L. Lovasz, L. Pyber, D. J. A. Welsh and G. M. Ziegler, *Combinatorics in pure mathematics, in Handbook of Combinatorics*, Elsevier Sciences B. V., Amsterdam (1996).

[96] N. Lynch, F. Vaandrager, *Forward and backward simulations: Part I. Untimed systems*, Information and Computation 121 (1995), 214–233.

[97] O.Mandel, M.Greiner, A. Widera, T.Rom, T. W. Hansch, and I. Bloch, Nature 425, 937 (2003)

[98] R. Milner, *A calculus of communicating systems*, Lecture Notes in Computer Science, vol. 92, Springer, Berlin, 1980.

[99] R. Milner, *Communication and Concurrency*, Prentice-Hall International, 1989.

[100] R. Milner, *Communicating and Mobile Systems: the π-Calculus*, Cambridge University Press, Cambridge, 1999.

[101] C. Moore, A. Russell , *Quantum Walks on the Hypercube*, in Proceedings of the 6th Int. Workshop on Randomization and Approximation in Computer Science (RANDOM02), 2002.

[102] J. Morris, *Automorphism groups of circulant graphs – a survey*, in A. Bondy, J. Fonlupt, J.-L. Fouquet, J. C. Fournier, and J. L. Ramirez Alfonsin (Eds.), Graph Theory in Paris (Trends in Mathematics), Birkhäuser, 2007.

[103] M. E. Muzychuk, *A solution of the isomorphism problem for circulant graphs*, Proc. London Math. Soc. (3) 88 (2004) 1–41.

[104] T. J. Osborne (2003), *Statics and Dynamics of Quantum XY and Heisenberg Systems on Graphs*, quant-ph/0312126.

[105] P. Östergård, *Cliquer algorithm*, http://users.tkk.fi/ pat/cliquer.html

[106] R. Paige, R. E. Tarjan, *Three partition refinement algorithms*, SIAM Journal on Computing 16 (6) (1987) 973–989.

[107] D. Park, *Concurrency and automata on infinite sequences*, in: P. Deussen (ed.), Proc. 5th GI Conf., Karlsruhe, Germany, Lecture Notes in Computer Science 104 (1981), Springer-Verlag, pp. 167–183.

[108] P. J. Pemberton-Ross, A. Kay, S. G. Schirmer, *Quantum Control Theory for State Transformations: Dark States and their Enlightenment*, 2010. Available from: http://arxiv.org/abs/1003.4290.

[109] M.D. Petković, M. Bašić, *Further results on perfect state transfer in integral circulant graphs*, Computer & Mathematics with Application, doi:10.1016/j.camwa.2010.11.005.

[110] V. Rakočević, *Funkcionalna analiza*, Naučna knjiga, Beograd, 1994.

[111] F. Ranzato, F. Tapparo, *Generalizing the Paige-Tarjan algorithm by abstract interpretation*, Information and Computation 206 (2008) 620–651.

[112] M. Roggenbach, M. Majster-Cederbaum, *Towards a unified view of bisimulation: a comparative study*, Theoretical Computer Science 238 (2000) 81-130.

[113] D. Saha, *An incremental bisimulation algorithm*, In: V. Arvind, S. Prasad (eds.), FSTTCS 2007, Springer, Heidelberg, Lecture Notes in Computer Science 4855 (2007), 204–215.

[114] D. Sangiorgi, *On the origins of bisimulation and coinduction*, ACM Transactions on Programming Languages and Systems 31 (4) (2009), 111–151.

[115] N. Saxena, S. Severini, I. Shparlinski, *Parameters of integral circulant graphs and periodic quantum dynamics*, International Journal of Quantum Information 5 (2007), 417–430.

[116] R. Sroul, *Programming for Mathematicians*, Berlin: Springer-Verlag, pp. 278-279, 2000.

[117] S. Skiena, *Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica*, MA: Addison-Wesley, pp. 215 and 217-218, 1990.

[118] S. Skiena, *The Algorithm Design Manual*, New York: Springer-Verlag, pp. 144 and 312-314, 1997.

[119] W. So, *Integral circulant graphs*, Discrete Mathematics 306 (2006), 153–158.

[120] A. Stamenković, M. Ćirić, J. Ignjatović, *Reduction of fuzzy automata by means of fuzzy quasi-orders*, Information Sciences (to appear).

[121] D. Stevanović, M. Petković, M. Bašić, *On the diametar of integral circulant graphs*, Ars Combinatoria (to appear).

[122] E. W. Weisstein, *Distinct Prime Factors*, From MathWorld-A Wolfram Web Resource, http://mathworld.wolfram.com/DistinctPrimeFactors.html.

[123] D. B. West, *Introduction to Graph Theory*, Prentice Hall, New Jersey, Second edition, 2001.

[124] S. Yu, *Regular languages*, in: G. Rozenberg, A. Salomaa (Eds.), Handbook of Formal Languages, vol. 1, Springer-Verlag, Berlin, Heidelberg, 1997, pp. 41–110.