Paul Erdös i dokazi iz Knjige

Perić, Martina

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:783396

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Martina Perić

PAUL ERDÖS I DOKAZI IZ KNJIGE

Diplomski rad

Voditelj rada:
dr. sc. Boris Muha, izv. prof.

Zagreb, veljača 2019.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Mađarski matematičar iz 20. stoljeća Paul Erdös ostavio je iza sebe matematičko naslijeđe velikih razmjera. Svoj je život posvetio otkrivanju matematičkih istina koje su se, prema njegovim riječima, nalazile u svijesti Boga. Bog posjeduje *Knjigu* u kojoj se nalaze svi najelegantniji matematički dokazi. U prvom dijelu svog diplomskog rada prikazat ću Erdösev život i istaknuti njegove matematičke doprinose. U drugom dijelu rada iznijet ću odabrane dokaze iz *Knjige*. Ti dokazi su iz triju matematičkih područja kojma se Erdös najviše bavio, odnosno iz teorije brojeva, kombinatorike i teorije grafova.

Poglavlje 1

Paul Erdös

1.1 Život i djelo

My brain is open! rečenica je koju je mađarski matematičar Paul Erdös izgovarao kada se pojavljivao pred vratima svojih poznanika matematičara kako bi zajednički razmišljali o matematici. Zahvaljujući bogatoj matematičkoj suradnji s drugima, objavio je oko 1500 znanstvenih radova zbog čega ga se, uz Leonarda Eulera, smatra najplodnijim matematičarem ikad. Koliko je njegovo matematičko djelovanje ujedno bilo i socijalna aktivnost, potvrđuje i njegova izreka *another roof, another proof* (vidi [12], str. 6).

Paul Erdös (mađ. Pál Erdős) rođen je 26. ožujka 1913. u Budimpešti. Roditelji su mu bili srednjoškolski učitelji matematike te su ga odmalena poučavali o matematici. Stoga je već kao četverogodišnjak bio upoznat s negativnim brojevima te je znao množiti četveroznamenkaste brojeve. Zabavljao je majčine prijatelje napamet preračunavajući njihove godine starosti u sekunde (vidi [4], str. 67). Za sebe je govorio da je još kao dijete imao vrlo dobar osjećaj za brojeve. Na pitanje zašto su brojevi lijepi, odgovarao je: *To je kao da pitate zašto je Beethovenova Deveta sim-*

fonija lijepa. Ako oni nisu lijepi, onda ništa nije lijepo (vidi [12], str. 43). U dobi od 16 godina otac ga je poučavao o beskonačnim nizovima i teoriji skupova. Kao srednjoškolac rješavao je matematičke zadatke koji su se nalazili u časopisu KőMaL. Pozivajući čitatelje da predaju svoja rješenja na postavljene matematičke zadatke, uredništvo časopisa najbolje je među njima objavljivalo pod imenom osobe koja ih je riješila. U tom su časopisu tako objavljeni i Erdösevi rezultati iz ravninske geometrije. Njegova usmjerenost prema rješavanju problema, a ne prema razvijanju teorije, stoga se nazire već u srednjoškolskim danima. Unatoč svom židovskom porijeklu, kao pobjednik nacionalnog matematičkog natjecanja prihvaćen je direktno na Sveučilište Pázmány koje je imalo ograničenu upisnu kvotu Židova zbog antisemitskog zakona (vidi [4], str. 67). Tamo je upoznao desetak vršnjaka posvećenih matematici s kojima se sastajao kako bi raspravljali o matematici i politici. Među tim vršnjacima bili su poznati matematičari: Paul Turán, Tibor Gallai, George Szekeres, Esther Klein, Márta Svéd i drugi. Surađivali su s Erdösem gotovo cijeli njegov život (vidi [12], str. 71-74).

S obzirom na to da su sastanci skupina tijekom diktature Miklósa Horthya bili zabranjeni, a nije se moglo ni slobodno govoriti, Erdös je počeo smišljati vlastiti jezik. Svi oni koji nisu podupirali Horthyevu diktaturu u to su doba smatrani komunistima, a u javnosti je bilo zabranjeno čak i izgovarati riječ komunist. Tako su, prema Erdösu, komunisti *oni duge valne duljine* dok su ljudi privrženi vladavini Hortya *oni kratke valne duljine*. Djecu je nazivao *epsilonima*, a tu je riječ koristio i za neke male stvari. Unuke je nazivao *epsilonima na kvadrat*, alkohol *otrovom*, glazbu *bukom*. Kada bi poželio gutljaj vina, rekao bi: *Želim epsilon otrova*. Razvio je posebne nazive za muškarce i žene. Muškarce je nazivao *robovima*, a žene *šefovima*, suprotno od onog kako su žene u Mađarskoj nazivale svoje muževe. Svu djecu nazivao je *šefovima*. U šali je rekao da muška djeca postaju *robovi* kada počnu trčati za *šefovima* odnosno

ženama. Za vjenčane parove koristio je riječ *zarobljeni*. Njegov je jezik bio vrlo zarazan te se proširio među matematičarima, čak i nakon Horthyevog režima. Erdös je s vremenom osmislio i nove riječi, primjerice *Sam* za Sjedinjene Američke Države i *Joe* za Sovjetski Savez (vidi [12], str. 72-73). Boga je 1940-ih počeo nazivati *SF-om* (*Supreme Fascist*). Govorio je da ga je *SF* uvijek mučio skrivajući mu njegove naočale i kradući mu mađarsku putovnicu. *SF nas je stvorio da uživa u našim patnjama. Što prije umremo, prije ćemo prkositi Njegovim planovima* (vidi [12], str. 4).

Za vrijeme studentskog života na njega su najviše utjecali sveučilišni profesor Leopold Fejér, Dénes König (profesor na tehničkom sveučilištu koji je objavio prvu monografiju iz teorije grafova) i László Kalmár (logičar i teoretičar brojeva) (vidi [4], str. 68). Već tada Erdös je najviše radio na teoriji brojeva ostvarujući više značajnih rezultata. Istaknuo se već u svojoj dvadesetoj godini nakon što je objavio dokaz Bertrandovog postulata, odnosno dokazavši da između svakog prirodnog broja i njegovog dvostrukog broja postoji prosti broj. Dokaz tog postulata bio je poznat i otprije (dokazao ga je Pafnuty Chebyshev za svaki n), ali elegancija Erdöseva dokaza odjeknula je među vodećim poznatim matematičarima. Diplomiravši (1934) na tom dokazu pod mentorstvom Fejéra, postao je poznat među vodećim matematičarima teorije brojeva (vidi [4], str. 68).

Nakon što je diplomirao, otišao je iz Mađarske u Manchester. Dobio je dozvolu za istraživanje te je ubrzo započeo pisati radove zapanjujućom brzinom. Bavio se uglavnom teorijom brojeva, ali i kombinatorikom te Ramseyevom teorijom, surađujući s matematičarem Richardom Radom. Iz te suradnje proizašao je poznati Erdös-Ko-Rado teorem, jedan od ključnih rezultata u teoriji ekstremalnih skupova tog razdoblja. Nakon što je otišao u Manchester, Erdös je nastavio surađivati sa svojim prijateljima iz Budimpešte. Elementarnu geometriju i Ramseyevu teoriju Erdös je povezao u jednom od svojih najranijih radova (1935) u suradnji s Georgeom Szekere-

som. Njih dvojica su dokazali da za dovoljno točaka u ravnini postoji k točaka koje tvore konveksni k-poligon. Teorem je postao poznat pod nazivom Erdös-Szekeresov teorem. Erdös je prepoznao ogromnu domenu koju je otvorio Ramseyev teorem, a to je generaliziracija *Principa golubinjaka*. U studiji iz 1935, napisane u suradnji sa Szekeresom, Erdös je prvi proučavao Ramseyeve brojeve za grafove što je prethodilo izgradnji Ramseyeve teorije. Transfinitna Ramseyeva teorija postala je temelj moderne teorije skupova (vidi [3], str. 24). U suradnji s Turánom i Gallaiem bavio se analizom, a u suradnji s Gézom Grünwaldiem bavio se teorijom grafova (vidi [4], str. 68). U Engleskoj je proveo četiri godine na poslijedoktorskim studijima. Već se tijekom tog razdoblja počeo nazirati njegov specifični stil života. Jedva da je ikada spavao u istom krevetu sedam uzastopnih noći, a od osobnih stvari nosio je samo poluprazni kovčeg. Novac je dijelio u humanitarne svrhe te rodbini i poznanicima (vidi [4], str. 66).

Godine 1938. prihvatio je stipendiju koju mu je ponudio Institut za napredna istraživanja u Princetonu. Nakon godinu dana boravka u Sjedinjenim Američkim Državama stipendiju su mu produžili na samo šest mjeseci, smatrajući ga čudnim i nekonvencionalnim, no tamo je proveo gotovo deset godina. To mu je bilo matematički najproduktivnije razdoblje. Osim teorijom brojeva, najviše se bavio i kombinatorikom (uključujući teoriju grafova), kombinatornom geometrijom, teorijom skupova, matematičkom analizom, teorijom algoritama, teorijom aproksimacija i teorijom vjerojatnosti. Sudjelovao je u stvaranju novih matematičkih područja kao što su kombinatorna teorija brojeva, Ramseyeva teorija, transfinitna kombinatorika, ekstremalna teorija skupova i proučavanje slučajnih struktura. Da je teorija brojeva bila glavno područje njegovog interesa, vidljivo je iz objavljenih rezultata koji obuhvaćaju gotovo polovicu od ukupnog broja objavljenih radova (vidi [3], str. 19). Prema njegovim riječima, najbolja godina je bila 1938/1939. Tada je objavio dva rada o distribuciji

vrijednosti aditivnih funkcija u suradnji s Marcom Kacom i Aurelom Wintnerom. U suradnji s Kacom uspostavio je središnji granični teorem za klasu aditivnih funkcija. *Tako bismo s malo drskosti rekli da je rođena vjerojatnosna teorija brojeva*, napisao je Erdös 1995. komentirajući to otkriće. U kratkom roku riješio je tada važni neriješeni problem teorije dimenzija: dimenzija racionalnog skupa točaka u Hilbertovom prostoru. Stručnjaci su očekivali da je dimenzija racionalnog skupa točaka u Hilbertovom prostoru jednaka nuli ili da je beskonačna, jer je taj prostor homeomorfan svome korijenu. Erdös je dokazao da je dimenzija jednaka 1. Godine 1942. napisao je *On the law of the iterated logarithm*, prve rezultate o nedostižnim kardinalima, a u suradnji s Alfredom Tarskim 1943. objavio je rad u kojem se nalaze rezultati vezani uz *nedostižne (nedostižive) kardinale*, temeljne za modernu teoriju skupova. Potrebno je spomenuti i Erdös-Stoneov teorem kojim je otvoreno polje teorije ekstremalnih grafova (vidi [4], str. 69). Godine 1947. dokazao je da postoji graf koji ima određeno Ramsey svojstvo, a da ga zapravo nije ni konstruirao. Drugim riječima, pokazao je da bi prikladno definirani slučajni graf imao svojstvo s pozitivnom vjerojatnošću i da stoga mora postojati takav graf (vidi [4], str. 65). Ratne godine za njega su bile izrazito teške jer je bio daleko od doma, a imao je poteškoća s kontaktiranjem roditelja u Budimpešti. Vijesti koje su dopirale do njega nisu bile dobre. Erdösev otac Lajos umro je 1942. od srčanog udara, a baka mu je umrla dvije godine nakon toga (vidi [4], str. 69).

Odlaskom iz Princetona započela su njegova putovanja. U potrazi za novim matematičkim talentima i matematičkim istinama puno je putovao, bio je čest posjetitelj dvadeset i pet zemalja širom svijeta. Tragajući za novim matematičarima, posjećivao je matematičke centre, fakultete te osnovne i srednje škole. Kada bi naišao na dijete talentirano za matematiku, pobrinuo bi se da mu osigura dobrog mentora kako njegov talent ne bi propao. U komunikaciji je uvijek postavljao prava pitanja te je znao pro-

cijeniti težinu problema koji postavlja pred sugovornika. Poznat je po velikodušnosti u dijeljenju svojih matematičkih ideja. Njegov cilj bilo je otkrivanje novih dokaza, s njim ili bez njega (vidi [12]). Radio je na mnogim problemima odjednom, s više ljudi u isto vrijeme. Okupio bi ih sve na jednom mjestu i sa svakim od njih raspravljao bi o drugom matematičkom problemu. Kada bi primijetio da nekome od njih zalutaju misli, opominjao bi ih riječima: *Bez nedozvoljenih misli.* Kako bi razlikovali stupanj matematičke suradnje s Erdösem, matematičari su osmislili pojam *Erdösev broj.* Naime, Erdösev broj 1 pripada osobi koja je s njime objavila rad, broj dva pripada osobi koja je objavila rad s njegovim suradnikom, broj 3 pripada osobi koja je objavila rad sa suradnikom njegovog suradnika itd. Matematičari koji ni na koji od tih načina nisu povezani s njime, imaju Erdösev broj beskonačno, a samom Erdösu dodijeljen je broj nula. Dodjeljivanjem novčane nagrade za rješenje matematičkih problema koji dotad nisu bili dokazani ili opovrgnuti, Erdös je promicao matematičko djelovanje. Još uvijek postoje mnoga otvorena pitanja za koja je zaslužan sam Erdös, a novčana se nagrada nastavila dodjeljivati i nakon njegove smrti pa sve do danas (vidi [12]).

Godine 1954. napustio je Sjedinjene Američke Države kako bi otišao na Internacionalni kongres matematičara u Amsterdamu. Sjedinjene Američke Države nisu mu izdale dozvolu za povratak s obrazloženjem da planira otići u Mađarsku. Izrael mu je odlučio pomoći nudeći mu putovnicu i posao sveučilišnog profesora na Hebrejskom sveučilištu u Jeruzalemu. U Izrael je došao 1954. godine, a 1959. ipak je dobio dozvolu za povratak u Sjedinjene Američke Države. Tijekom svog života bio je zaposlen na dva sveučilišta, Purdue i Notre Dame. Dvije godine nakon Staljinove smrti, odnosno 1955, nakratko se uspio vratiti u Mađarsku, a već od sljedeće godine mogao se vraćati u Mađarsku kad god bi htio (vidi [12], str. 127-130). To mu je omogućilo lakšu suradnju s mađarskim matematičarima. U suradnji s Rényiem stvorio je fascinantnu novu sintezu kombinatorike i vjerojatnosti, izloženu u njihovoj značajnoj studiji *The*

evolution of random graphs (1960/1961). U suradnji s Turánom proučavao je interpolaciju i osmislio statističku teoriju grupa. U suradnji s Andrásom Hajnalom izložio je kombinatornu teoriju skupova (vidi [4], str. 71). S Ronom Grahamom susreo se 1963. nakon čega je postao jedan od njegovih najbližih suradnika u teoriji brojeva i kombinatorici. Zajedno s Atleom Selbergom 1951. godine dobio je nagradu *Cole Prize* za dokaz Teorema o prostim brojevima. Teorem o prostim brojevima dokazali su elementarnim metodama koristeći Eratostenovo sito (vidi [12], str. 40).

Među matematičarima s kojima je Erdös surađivao jesu i: Kai Lai Chung, Ivan Niven, Arye Dvoretzky, Shizuo Kakutani, Arthur A. Stone, Leon Alaoglu, Irving Kaplansky, Alfred Tarski, Gabor Szegő, William Feller, Fritz Herzog, George Piranian, Paul Turán, Harold Devenport, Tibor Gallai i drugi (vidi [12]). Surađivao je i sa Stanislawom Ulamom, matematičarem koji se bavio teorijom skupova. Ulam se prisjeća: *U njegovim očima se vidjelo da je uvijek razmišljao o matematici, proces koji je mogao biti prekinut samo njegovim pesimističnim izjavama o događajima u svijetu, politici...* (vidi [12], str. 97).

Godine 1971. umrla mu je majka Anna koja ga je nakon smrti svoga supruga pratila na putovanjima. *Bio sam vrlo depresivan, a Paul Turán, stari prijatelj, podsjetio me da je veliko uporište naša matematika*, rekao je Erdös (vidi [12], str. 143). Matematikom se tada bavio i do devetnaest sati dnevno, pišući radove koji su mijenjali matematičku povijest. Proširio je i krug matematičara s kojima je surađivao. Jedan od njih je Joel Spencer s kojim je napisao dvije knjige, *The Art Of Counting* (1973) i *Probabilistic Methods in Combinatorics* (1974). Ta dva djela približila su konačnu kombinatoriku široj publici. Godine 1980. u suradnji s Peterom Vértesiem objavio je spektakularni teorem o interpolaciji: *Za bilo koji skup točaka postoji neprekidna funkcija f tako da niz Lagrangeovih interpolacijskih polinoma f na danom skupu točaka divergira gotovo svugdje* (vidi [4], str. 71). Nakon smrti Erdöseve majke za njega su se

brinuli veliki matematičari Ronald Graham i Fan Chung (vidi [12], str. 15). Graham je nakon Erdöseve smrti nastavio isplaćivati novčane nagrade za rješenja Erdösevih problema, a Fan je sastavila popis svih njegovih otvorenih problema iz teorije grafova (vidi [12], str. 17).

Tijekom posljednjih desetljeća svog života Erdös je primio puno priznanja. Dobio je najmanje petnaest počasnih doktorata. Postao je član nacionalnih znanstvenih akademija u osam zemalja, uključujući američku Nacionalnu akademiju znanosti (1979) i Kraljevsko društvo (1989). Neposredno prije svoje smrti odrekao se svog počasnog zvanja na Sveučilištu Waterloo zbog nepoštenog postupanja prema kombinatoristu Johnu Adrianu Bondyu (vidi [4], str. 71).

U posljednjoj godini svoga života, 1966. godine, na godišnjem Internacionalnom simpoziju iz kombinatorike, teorije grafova i računarstva, Erdös se srušio. Dok je osiguranje pokušavalo isprazniti prostor u kojem su bili sudionici simpozija, Erdös je rekao: *Reci im da ne idu, imam još dva problema o kojima im trebam govoriti* (vidi [12], str. 244-245). Umro je od srčanog udara u dobi od 83 godine, 20. rujna 1996. godine, za vrijeme radionice o teoriji grafova u hotelskoj sobi u Banach Centru u Varšavi. Za sebe je govorio da želi umrijeti kao Euler. *Želim izlagati svoje predavanje, dovršavati važan dokaz na ploči, a kada netko iz publike dobaci „Što je s generalizacijom?", ja bih se okrenuo prema publici, nasmijao i rekao „Ostavit ću to sljedećoj generaciji" i tada bih se srušio* (vidi [12], str. 201).

Prije nego što je umro uspio je razmišljati o više problema nego ijedan matematičar u povijesti matematike. U zadnjim godinama svoga života objavljivao je i do 50 radova godišnje. Naslijeđe koje je ostavio iza sebe ogromnih je razmjera.

1.2 Ravno iz *Knjige*

Na pitanje otkrivaju li se matematičke istine ili se stvaraju, Paul Erdös bi rekao da ako se vjeruje u SF odgovor je jasan. Matematičke istine su tada u svijesti SF-a i potrebno ih je samo otkriti. Iako se Erdös nije izjašnjavao o svojem stajalištu o postojanju Boga smatrajući da nije kvalificiran za to, ipak je i sam sumnjao u njegovo postojanje. Međutim, kao pravi matematičar vjerovao je u postojanje *Knjige*, transfinitne knjige s najelegantnijim i savršenim matematičkim dokazima svih teorema koju posjeduje sam SF. Tako je najveći kompliment koji je Erdös mogao dati svojim prijateljima matematičarima bio: *To je ravno iz* Knjige*!* (vidi [12], str. 26).

Potaknuti idejom postojanja *Knjige*, dvojica matematičara, Martin Aigner i Günter M. Ziegel, predložili su Erdösu da zajedno napišu knjigu koja bi sadržavala sve najelegantije dokaze iz matematike. Prihvativši tu ideju, Erdös je ubrzo počeo zapisivati prijedloge dokaza. Međutim, zbog svoje iznenadne smrti nije dočekao objavljivanje knjige na svoj rođendan 1998, čime su ga Aigner i Ziegler namjeravali iznenaditi. Knjiga je unatoč navedenim okolnostima objavljena pod nazivom *Proofs from THE BOOK*, ali samo s potpisom dvojice autora (vidi [2], *Predgovor*). Knjigu su posvetili uspomeni na Erdösa koji je u velikoj mjeri utjecao na odabir dokaza i područja koji se u knjizi obrađuju. Četvrto izdanje knjige sastoji se od pet poglavlja: teorija brojeva, geometrija, analiza, kombinatorika, teorija grafa. U drugom poglavlju ovoga rada dani su dokazi iz te knjige iz triju matematičkih područja kojima se Erdös najviše bavio. To su teorija brojeva, kombinatorika i teorija grafa. Osim njegovih dokaza, dan je i dokaz Teorema Erdös-Ko-Rado kojega je on iznio u suradnji s drugim matematičarima.

Poglavlje 2

Dokazi iz knjige

2.1 Teorija brojeva

Beskonačnost skupa prostih brojeva

Dokaz da je skup prostih brojeva beskonačan nalazi se već u Euklidovoj knjizi *Elementi* (o. 300. pr. n. e.). Iako se u knjizi *Proofs from THE BOOK* nalazi ukupno šest dokaza (među kojima je i Euklidov), u nastavku rada prikazan je Erdösev dokaz koji, osim što dokazuje beskonačnost skupa prostih brojeva, pokazuje i da red recipročnih prostih brojeva divergira.

Teorem 1. *Postoji beskonačno mnogo prostih brojeva.*

Dokaz. Tvrdnja se dokazuje svođenjem na kontradikciju. Neka je $p_1,\ p_2,\ p_3,\ \ldots$ rastući niz prostih brojeva i neka vrijedi pretpostavka da $\sum_{p\in\mathbb{N}} \frac{1}{p_i}$ konvergira. Tada postoji prirodan broj k takav da $\sum\limits_{i\geq k+1} \dfrac{1}{p_i} < \dfrac{1}{2}$. Za proizvoljni prirodni broj N vrijedi

$$\sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{2.1}$$

Za lakše snalaženje uvodi se terminologija: neka su $p_1, \ldots, p_k$ *mali* prosti brojevi, a $p_{k+1}, p_{k+2}, \ldots$ *veliki* prosti brojevi. Neka je N_b broj prirodnih brojeva $n \leq N$ koji su djeljivi s barem jednim velikim prostim brojem, a neka je N_s broj svih prirodnih brojeva $n \leq N$ čiji su djelitelji *samo* mali prosti brojevi. Za tako definirane N_b i N_s proizlazi očita jednakost $N_b + N_s = N$. U nastavku će se pokazati da vrijedi i nejednakost $N_b + N_s < N$ čime se dobiva kontradikcija s prethodnom jednakosti. Kako bi se to postiglo dovoljno je ocijeniti brojeve N_b i N_s da bi se dobila ocjena i za njihov zbroj.

Za ocjenu N_s koristi se rastav na proste faktore onih prirodnih brojeva n_s koje N_s prebrojava. Rastav se takvih prirodnih brojeva $n_s \leq N$ sastoji od samo *malih* prostih faktora. Dakle, rastav je oblika

$$\begin{aligned} n_s &= p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \\ &= \alpha_1^2 p_1^{l_1} \cdot \alpha_2^2 p_2^{l_2} \cdots \alpha_k^2 p_k^{l_k} \\ &= (\alpha_1 \alpha_2 \cdots \alpha_k)^2 \cdot p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k} \\ &= \alpha^2 \cdot p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}, \end{aligned}$$

gdje je svaki α_i^2 najveći kvadrirani broj kojeg $p_i^{m_i}$ sadržava kao faktora[1], a svaki l_j je jednak ili 1 ili 0.

Kako bi se ocijenio broj svih n_s, a time i N_s, dovoljno je ocijeniti faktore α^2 i $p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$.

Kako je $a \leq N$ i $\alpha^2 \leq a$ tako je i $\alpha^2 \leq N$, odnosno $\alpha \leq \sqrt{N}$.

Kako vrijednost svakog $p_i^{l_i}$ može biti jedna od dvije mogućnosti (ili je jednaka p_i ili je jednaka 1) tako je broj svih $p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$ najviše 2^k.

Dakle, broj svih n_s je

$$N_s \leq \sqrt{N} \cdot 2^k. \tag{2.2}$$

[1] Svaki $p_i^{l_i}$ je kvadratno slobodan, odnosno najveći potpuni kvadrat koji ga dijeli jednak je 1

Za ocjenu broja N_b u odnosu na N potrebno je primijetiti da $\left\lfloor \frac{N}{p_i} \right\rfloor$ broji samo višekratnike prostog broja p_i manje ili jednake broju N. Iz početne nejednakosti (2.1) sada slijedi

$$N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2},$$

odnosno

$$N_b < \frac{N}{2}. \tag{2.3}$$

Konačno, iz ocjena (2.3) i (2.2) za N_s i N_b, za odabrani $N = 2^{2k+2}$ slijedi

$$\begin{aligned} N_s + N_b &< 2^k \sqrt{N} + \frac{N}{2} \\ &= 2^k \sqrt{2^{2k+2}} + \frac{2^{2k+2}}{2} \\ &= 2^k \sqrt{2^{2(k+1)}} + \frac{2^{2k+1} \cdot 2}{2} \\ &= 2^{2k+1} \cdot 2^{2k+1} \\ &= 2^{2k+2} \\ &= N \end{aligned}$$

Dakle, vrijedi $N_s + N_b < N$.

Kako po definiciji N_s i N_b mora vrijediti $N_s + N_b = N$, dolazi se do kontradikcije s prethodnom nejednakosti.

To znači da početna pretpostavka da $\sum_{p \in \mathbb{N}} \frac{N}{p_i}$ konvergira nije točna, odnosno $\sum_{p \in \mathbb{N}} \frac{N}{p_i}$ divergira što povlači da postoji beskonačno mnogo prostih brojeva.

□

Bertrandov postulat

U prethodnom dijelu ovoga rada pokazano je da je niz prostih brojeva $2,\ 3,\ 5,\ 7, \ldots$ beskonačan. Kako bi se pokazalo da veličina udaljenosti među prostim brojevima nije

ograničena, dovoljno je za svaki $k \in \mathbb{N}_0$ pronaći k uzastopnih složenih brojeva. To bi zapravo značilo da za svaki takav k postoje dva susjedna prosta broja međusobno udaljena za najmanje $k+1$.

Neka je $k \in N$ i $N := 2 \cdot 3 \cdot 5 \cdots p$ umnožak svih prostih brojeva manjih od $k+2$. Tada niti jedan od k brojeva

$$N+2,\ N+3,\ N+4, \ldots,\ N+k,\ N+(k+1)$$

nije prost. Naime, svaki prirodni broj $2 \leq i \leq k+1$ ima prosti faktor q_i manji od $k+2$. S obzirom na to da je q_i prosti faktor i od N, q_i dijeli $N+i$ što znači da je $N+i$ složen.

Na primjer, s $k = 12$ zadan je umnožak $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ (što je jednako 30030) pa u odgovarajućem nizu od četrnaest uzastopnih prirodnih brojeva 30032, 30033, 30034, ..., 30043 niti jedan broj nije prost.

Ipak, postoji gornja granica za udaljenosti između prostih brojeva. Udaljenost do prvog sljedećeg prostog broja ne može biti veća od broja kojim smo započeli traženje. Preciznije, za svaki prirodni broj postoji prosti broj p takav da je $n < p \leq 2n$. Tvrdnju je, kao slutnju, 1845. iskazao francuski matematičar Joseph Bertrand, a ta je tvrdnja poznata pod nazivom Bertrandov postulat. Bertrand je svoju tvrdnju provjerio za $n < 3\ 000\ 000$, a Pafnuty Chebyshev prvi ju je dokazao za sve n. Prvi jednostavniji dokaz dao je indijski matematički genij Srinivasa Ramanujan. U nastavku rada dan je Erdösev dokaz koji je objavio kada je imao samo 19 godina, 1932. u svom prvom članku *Beweis eines Satzes von Tschebyschef* (vidi [2], str. 7). Dokaz se temelji na nekoliko pomoćnih tvrdnji koje govore o svojstvima rastava binomnog koeficijenta $\binom{2n}{n}$ na proste faktore te na ocjenama tog binomnog koeficijenta.

Prema *Osnovnom teoremu aritmetike* prirodni broj n može se zapisati u obliku

$$n = \prod_{\substack{p \leq n \\ p\ prost}} p^{k(n,\ p)},\ k(n,\ p) \in \mathbb{N}_0. \tag{2.4}$$

Drugim riječima, prirodni broj n može se zapisati kao umnožak prostih brojeva na jedinstven način do na poredak faktora.

Ako prosti broj p ne dijeli n, vrijedi $k(n,\ p) = 0$ (i obrnuto), a ako p dijeli n, $p^{k(n,\ p)}$ je najveća potencija od p koja dijeli n. Odsada pa nadalje slovo p označava prosti broj.

Lema 1. ***Legendrov teorem*** *Rastav na proste faktore od* $n!$ *je oblika*

$$n! = \prod_{p \leq n} p^{k(n!,\ p),}$$

pri čemu je

$$k(n!,\ p) = \sum_{t=1}^{r} \left\lfloor \frac{n}{p^t} \right\rfloor,$$

gdje je $r = r(n,\ p)$ *broj za koji vrijedi* $p^r \leq n < p^{r+1}$.

Drugim riječima, broj $n!$ djeljiv je samo s prostim faktorima $p \leq n$ i prosti broj p se kao faktor pojavljuje točno $\sum\limits_{t=1}^{r} \left\lfloor \frac{n}{p^t} \right\rfloor$ puta.

Dokaz. Broj $n! = 1 \cdot 2 \cdots n$ sadrži točno $\left\lfloor \frac{n}{p} \right\rfloor$ faktora djeljivih s p pa $n!$ sadrži faktor p barem $\left\lfloor \frac{n}{p} \right\rfloor$ puta.
Faktor p^2 se pojavljuje $\left\lfloor \frac{n}{p^2} \right\rfloor$ puta što znači da se faktor p pojavljuje još $\left\lfloor \frac{n}{p^2} \right\rfloor$ puta. Postupak se nastavlja sve do faktora p^r koji se pojavljuje $\left\lfloor \frac{n}{p^r} \right\rfloor$ puta. Broj r je takav da $p^r \leq n < p^{r+1}$, jer već za faktor p^{r+1} vrijedi $\left\lfloor \frac{n}{p^{r+1}} \right\rfloor = 0$. Stoga je $k(n!,\ p)$ upravo $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^r} \right\rfloor = \sum\limits_{t=1}^{n} \left\lfloor \frac{n}{p^t} \right\rfloor$.

□

Lema 2. *Za sve realne brojeve $x \geq 2$ vrijedi*

$$\prod_{p \leq x} p \leq 4^{x-1}$$

Dokaz. Dovoljno je dokazati tvrdnju teorema za prirodne brojeve x jer ako je ona istinita za prirodne brojeve, onda za realne brojeve x vrijedi

$$\prod_{p \leq x} p = \prod_{p \leq \lfloor x \rfloor} p \leq 4^{\lfloor x-1 \rfloor} \leq 4^{x-1}.$$

Teorem je očito istinit za $x = 2$ i $x = 3$. Tvrdnja teorema za prirodne brojeve veće od 3 može se dokazati matematičkom indukcijom. U tu svrhu, neka je dana pretpostavka da nejednakost vrijedi za sve prirodne brojeve $x \leq k - 1$, za neki $k > 3$, odnosno da vrijedi

$$\prod_{p \leq k-1} p \leq 4^{k-2}, \text{ za neki } k > 3.$$

Cilj je pokazati da tada nejednakost vrijedi i za njegovog sljedbenika $x = k$. Ako je k parni broj, tvrdnja je očita jer pretpostavka za $k > 3$ povlači

$$\prod_{p \leq 2n} p \overset{k-paran}{=} \prod_{p \leq 2n-1} p \overset{pretp.}{\leq} 4^{2n-2} \leq 4^{2n-1} = 4^{k-1}.$$

Neka je k neparni broj, primjerice $k = 2n + 1$. Tada se promatrani produkt može napisati kao:

$$\prod_{p \leq 2n+1} p = \prod_{p \leq n+1} p \cdot \prod_{n+2 \leq p \leq 2n+1} p.$$

Po pretpostavci indukcije tvrdnja teorema vrijedi za $x \leq (2n + 1) - 1$, odnosno za $x \leq 2n$. Kako je $n + 1 \leq 2n$ iz pretpostavke slijedi veličina gornje granice jednog od faktora:

$$\prod_{p \leq n+1} p \leq 4^n$$

pa je dovoljno pronaći još gornju granicu drugog faktora $\prod_{n+2 \leq p \leq 2n+1} p$. Prosti brojevi između $n + 2$ i $2n + 1$, uključujući rubove, djelitelji su binomnog koeficijenta $\binom{2n+1}{n}$

što se vidi iz

$$\binom{2n+1}{n} = \frac{(n+1)! \cdot (n+2)(n+3)\cdots(2n+1)}{n!(n+1)!} = \frac{(n+2)(n+3)\cdots(2n+1)}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot n}.$$

Stoga je umnožak prostih brojeva između $n+2$ i $2n+1$, uključujući rubove, sigurno manji ili jednak tom binomnom koeficijentu. To znači da je dovoljno odrediti gornju granicu tom binomnom koeficijentu. Zapis binomnog koeficijenta može biti pojednostavljen dijeljenjem produkta parnih brojeva u brojniku s $n!$ u nazivniku, a zatim uspoređivanjem svakog neparnog broja u brojniku s prvim sljedećim parnim brojem.

$$\begin{aligned}
\binom{2n+1}{n} &= \frac{1 \cdot 2 \cdot 3 \cdots 2n \cdot 2n+1}{1 \cdot 2 \cdot 3 \cdots n \cdot (n+1)!} \\
&= \frac{(2 \cdot 4 \cdot 6 \cdots 2n)(3 \cdot 5 \cdot 7 \cdots 2n+1)}{1 \cdot 2 \cdot 3 \cdots n \cdot (n+1)!} \\
&= \frac{(2 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot \cdots \cdot 2 \cdot n)(3 \cdot 5 \cdot 7 \cdots 2n+1)}{1 \cdot 2 \cdot 3 \cdots n \cdot (n+1)!} \\
&= \frac{2^n(1 \cdot 2 \cdot 3 \cdots n)(3 \cdot 5 \cdot 7 \cdots 2n+1)}{1 \cdot 2 \cdot 3 \cdots n \cdot (n+1)!} \\
&= \frac{2^n(3 \cdot 5 \cdot 7 \cdots 2n+1)}{(n+1)!} \\
&= \frac{2^n(3 \cdot 5 \cdot 7 \cdots 2n+1)}{2 \cdot 3 \cdot 4 \cdots (n+1)} \\
&\leq 2^n \cdot \frac{4 \cdot 6 \cdot 8 \cdots 2n+2}{2 \cdot 3 \cdot 4 \cdots (n+1)} \\
&= 2^n \cdot 2^n \\
&= 4^n
\end{aligned} \tag{2.5}$$

Iz pretpostavke indukcije i gornje nejednakosti slijedi

$$\prod_{p\leq 2n+1} p = \prod_{p\leq n+1} p \cdot \prod_{n+2\leq p\leq 2n+1} p \leq 4^n \cdot \binom{2n+1}{n} \leq 4^n \cdot 4^n = 4^{2n} = 4^{k-1}$$

čime je tvrdnja dokazana i za neparan broj $k = 2n + 1$.

Dakle, nejednakost $\prod_{p\leq x} p \leq 4^x$ vrijedi za sve $x \geq 2$.

□

Lema 3. *Za sve prirodne brojeve n vrijedi*

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n}$$

Dokaz. Slično kao i u (2.5), binomni koeficijent $\binom{2n}{n}$ može se pojednostaviti dijeljenjem produkta parnih brojeva u brojniku s $n!$ nakon čega se uspoređuje svaki neparni broj u brojniku s prvim prethodnim parnim brojem.

$$\binom{2n}{n} = \frac{1\cdot 2\cdot 3\cdots 2n}{1\cdot 2\cdot 3\cdots n\cdot (n)!} = 2^n \frac{3\cdot 5\cdots (2n-1)}{n!} \geq 2^n \frac{2\cdot 4\cdots (2n-2)}{1\cdot 2\cdot \cdots \cdot n} = 2^n \frac{2^{n-1}}{n}$$

Dakle,

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n}$$

vrijedi za sve prirodne brojeve n.

□

Lema 4. *Neka prosti broj p dijeli $\binom{2n}{n}$. Tada je $p^{k\left(\binom{2n}{n},\, p\right)} \leq 2n$. Ako vrijedi i $p > \sqrt{2n}$, onda je $k\left(\binom{2n}{n},\, p\right) = 1$.*

Dokaz. S obzirom na to da p dijeli $\binom{2n}{n}$, vrijedi $k\left(\binom{2n}{n},\ p\right) \geq 1$. Prema Legendrovom teoremu (1) vrijedi

$$\begin{aligned} k\left(\binom{2n}{n},\ p\right) &= k((2n)!,\ p) - 2k(n!,\ p) \\ &= \sum_{i=1}^{r(2n,\,p)} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \sum_{i=1}^{r(n,\,p)} \left\lfloor \frac{n}{p^i} \right\rfloor \\ &= \sum_{i=1}^{r(2n,\,p)} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) \end{aligned} \tag{2.6}$$

Posljednji redak jednakosti slijedi iz činjenice da je $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$ za $r(n,\ p) < i \leq r(2n,\ p)$. Svaki od dobivenih pribrojnika jednak je najviše 1 što se vidi iz sljedeće nejednakosti:

$$\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor < \frac{2n}{p^i} - 2\left(\frac{n}{p^i} - 1\right) = 2.$$

Iz (2.6) slijedi

$$1 \leq k\left(\binom{2n}{n},\ p\right) \leq r(2n,\ p) = \max\{r : p^r \leq 2n\} \tag{2.7}$$

pa je $p^{k\left(\binom{2n}{n},\,p\right)} \leq 2n$, što je i trebalo pokazati.

Ako vrijedi i $p > \sqrt{2n}$, onda je $p^2 > 2n$ odnosno $\max\{r : p^r = 1\}$. Iz (2.7) sada vrijedi i $1 \leq k\left(\binom{2n}{n},\ p\right) \leq 1$ što povlači da je $k\left(\binom{2n}{n},\ p\right) = 1$.

□

Lema 5. *Neka je $n \geq 3$ prirodni broj i p prosti broj za koji vrijedi $\frac{2}{3}n < p \leq n$. Tada p ne dijeli $\binom{2n}{n}$.*

Dokaz. Neka je $n \geq 3$ prirodni broj i p prosti broj za koji vrijedi $\frac{2}{3}n < p \leq n$. Tada iz nejednakosti $3p > 2n \geq 2p$ slijedi da su p i $2p$ jedini višekratnici broja p manji ili jednaki $2n$. Budući da je $p \neq 2$ što se vidi iz nejednakosti $p > \frac{2}{3}n \geq 2$, broj $2p$ nije djeljiv s p^2. Stoga je brojnik

$$\binom{2n}{n} = \frac{1 \cdot 2 \cdots 2n}{1 \cdot 2 \cdots n \cdot n!}$$

djeljiv s p^2, ali ne i s p^3. S druge strane, s obzirom na to da vrijedi $p \leq n < \frac{3}{2}p < 2p$, nazivnik ima točno dva faktora p pa tvrdnja slijedi.

□

Teorem 2. ***Bertrandov postulat*** *Za svaki $n \geq 1$ postoji prosti broj p takav da je $n < p \leq 2n$.*

Dokaz. Potrebno je ocijeniti binomni koeficijent $\binom{2n}{n}$. Donja granica binomnog koeficijenta slijedi iz leme (3), odnosno za $n \geq 3$ vrijedi

$$\begin{aligned}
\frac{4^n}{2n} \overset{(3)}{\leq} \binom{2n}{n} &= \prod_{p \leq \sqrt{2n}} p^{k\left(\binom{2n}{n}, p\right)} \prod_{\sqrt{2n} < p \leq 2n} p^{k\left(\binom{2n}{n}, p\right)} \\
&\overset{(4)}{\leq} \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq 2n} p^{k\left(\binom{2n}{n}, p\right)} \\
&\leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq 2n} p^{k\left(\binom{2n}{n}, p\right)} \\
&= (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^{k\left(\binom{2n}{n}, p\right)} \prod_{\frac{2}{3}n < p \leq n} p^{k\left(\binom{2n}{n}, p\right)} \prod_{n < p \leq 2n} p^{k\left(\binom{2n}{n}, p\right)} \\
&\overset{(5)}{=} (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^{k\left(\binom{2n}{n}, p\right)} \prod_{n < p \leq 2n} p^{k\left(\binom{2n}{n}, p\right)} \\
&\overset{(4)}{=} (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p \\
&\leq (2n)^{\sqrt{2n}} \prod_{p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p \\
&\overset{(2)}{\leq} (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n} \prod_{n < p \leq 2n} p.
\end{aligned}$$

Dakle, ocjena binomnog koeficijenta $\binom{2n}{n}$ je

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \cdot \prod_{n < p \leq 2n} p.$$

Neka je dana pretpostavka da tvrdnja teorema ne vrijedi, odnosno da ne postoji prosti broj p takav da $n < p \leq 2n$. Tada $\prod_{n<p\leq 2n} p = 1$ pa je ocjena binomnog koeficijenta

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n}.$$

Množenjem gornje nejednakosti s $\frac{2n}{4^{\frac{2}{3}n}}$, dobiva se nejednakost

$$4^{\frac{1}{3}n} \leq (2n)^{\sqrt{2n}+1} \tag{2.8}$$

koja ne vrijedi za velike prirodne brojeve n.

U nastavku se određuje za koje prirodne brojeve nejednakost vrijedi.

Koristeći nejednakost $a + 1 < 2^a$, koja induktivno vrijedi za sve $a \geq 2$, dobiva se

$$2n = (\sqrt[6]{2n})^6 < (\lfloor \sqrt[6]{2n} \rfloor + 1)^6 < (2^{\lfloor \sqrt[6]{2n} \rfloor})^6 = 2^{6\lfloor \sqrt[6]{2n} \rfloor} < 2^{6\sqrt[6]{2n}}. \tag{2.9}$$

Nejednakost (2.8) ekvivalentna je nejednakosti $4^n \leq (2n)^{3(\sqrt{2n}+1)}$ što s nejednakosti (2.9) daje

$$4^n < 2^{6\sqrt[6]{2n}\cdot 3(\sqrt{2n}+1)},$$

a to je ekvivalentno s

$$4^n < 2^{\sqrt[6]{2n}\cdot(18\sqrt{2n}+18)}.$$

Za $n \geq 50$ je $18 < 2\sqrt{2n}$ pa vrijedi

$$\begin{aligned} 4^n &< 2^{\sqrt[6]{2n}\cdot(18\sqrt{2n}+18)} \\ &< 2^{\sqrt[6]{2n}\cdot(18\sqrt{2n}+2\sqrt{2n})} \\ &= 2^{\sqrt[6]{2n}\cdot 20\sqrt{2n}} \\ &= 2^{20\cdot(2n)^{\frac{2}{3}}}. \end{aligned}$$

Iz prethodno dobivene nejednakosti slijedi $(2n)^{\frac{1}{3}} < 20$ pa je $n < 4\ 000$. Drugim riječima, nejednakost dobivena iz ocjene binomnog koeficijenta $\binom{2n}{n}$, uz danu pretpostavku, vrijedi samo za $n < 4\ 000$.

Nejednakost ne vrijedi za $n \geq 4\,000$ pa je dana pretpostavka netočna, odnosno postoji prosti broj p takav da je $n < p \leq 2n$.

Još je potrebno pokazati da Bertrandov postulat vrijedi i za $n < 4\,000$. Nije potrebno provjeriti svaki od 4 000 slučajeva, dovoljno je samo uvjeriti se da je u nizu brojeva

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 162,\ 317,\ 631,\ 1259,\ 2503,\ 4001$$

svaki član prosti broj te manji od dvostrukog prethodnog člana (Landauov trik). Naime, ako za neki prosti broj p postoji prosti broj q iz intervala $(n,\ 2n]$, onda se q nalazi i u svakom intervalu oblika $(m,\ 2m]$ za $m = p+1, \ldots, q-1$. Prema tome, svaki interval oblika $(n,\ 2n]$ za $n \leq 4000$ sadrži jedan od 14 gornjih prostih brojeva. Ovime je teorem dokazan za sve prirodne brojeve n.

□

2.2 Kombinatorika

Osnovni odnos među skupovima određen je njihovim presjekom. Vrstu „zavisnosti" među njima opisuje veličina ili neka druga karakteristika njihovog međusobnog presjeka. Neka je dan konačni skup $N = \{1, 2, \ldots, n\}$. Familija $\mathcal{F}$ podskupova skupa N naziva se *presječna* (ili *presijecajuća*) *familija* ako je $A \cap B \neq \emptyset$, za svako $A, B \in \mathcal{F}$. Ako je $A \in \mathcal{F}$ onda komplement $\bar{A} \notin \mathcal{F}$ jer $A \cap \bar{A} = \emptyset$. Stoga presječna familija ima najviše polovicu od svih 2^n podskupova, odnosno $|\mathcal{F}| \leq 2^{n-1}$. Jednakost se postiže ako svaki član presječne familije $\mathcal{F}_1$ sadrži neki fiksni element 1, $|\mathcal{F}_1| = 2^{n-1}$.

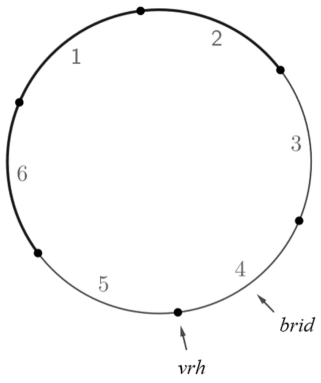
Teorem Erdös-Ko-Rado

Postavlja se pitanje kolika je najveća presječna familija skupova ako svi njezini skupovi sadrže jednak broj elemenata. Neka je njihov broj jednak k. Ako je $k > \frac{n}{2}$

onda se svaka dva k člana skupa sijeku što je trivijalan slučaj. Neka je $k \leq \frac{n}{2}$ i $\mathcal{F}_1$ presječna familija k - članih podskupova čiji svaki član sadrži fiksni element m. Svi takvi k-člani skupovi mogu se dobiti dodavanjem fiksnog m svim $(k-1)$-članim podskupovima od $N \setminus \{m\}$. Dakle, $|\mathcal{F}_1| = \binom{n-1}{k-1}$. Da ne postoji veća familija od takve, otkrili su zajednički Paul Erdös, Chao Ko i Richard Rado 1938. godine. U nastavku je dan dokaz Gyule Katona (vidi [2], str. 152).

Teorem 3. ***(Erdös-Ko-Rado).*** *Ako je $n \geq 2k$ onda svaka presječna familija $\mathcal{F}$ k-članih podskupova od n-članog skupa ima najviše $\binom{n-1}{k-1}$ članova.*

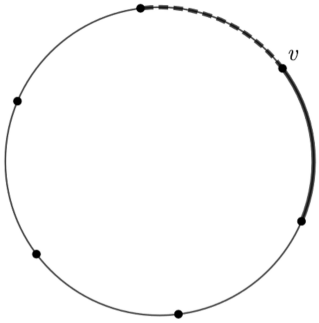
Dokaz. Neka je C kružnica podijeljena na način kao na slici 2.1 koja sadrži n vrhova (istaknute točke) i n bridova (dijelovi kružnice čiji krajevi su dvije od istaknutih točaka). Ako se bridovi označe kao na slici 2.1 brojevima od 1 do n, onda luk duljine k sadrži $k+1$ uzastopnih vrhova i k bridova. Od svih lukova duljine k kružnice C promatraju se oni lukovi koji imaju zajednički brid (oni koji se preklapaju).



Slika 2.1: Kružnica C s $n = 6$ vrhova i 6 bridova s označenim lukom duljine $k = 3$

Kako bi se dokazao teorem, potrebna je sljedeća lema.

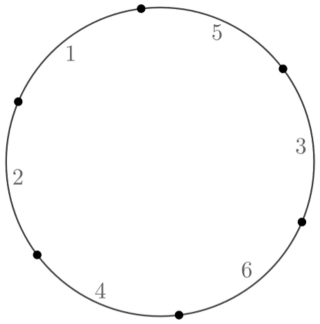
Lema 6. *Ako postoji t različitih lukova duljine $k \leq \frac{n}{2}$ takvih da bilo koja dva luka imaju zajednički brid, tada $t \leq k$.*



Slika 2.2: Lukovi A_i i A_j ne mogu imati zajednički krajnji vrh

Neka su A_i, $i = 1, 2, \ldots, t$, međusobno različiti lukovi duljine $k \leq \frac{n}{2}$ kružnice C takvi da bilo koja dva luka imaju zajednički brid. Bilo koji od vrhova kružnice C može biti krajnji vrh najviše jednog luka A_i. U suprotnom, ako međusobno različiti lukovi A_i, A_j imaju zajednički krajnji vrh v trebali bi se nadovezat jedan na drugi (vidi sliku 2.2) što bi značilo da ne mogu imati zajedničke bridove jer $2k \leq \frac{n}{2}$. Dakle, svi krajnji vrhovi danih lukova su međusobno različiti (jer da nisu, lukovi bi se ili potpuno preklapali ili bi se nadovezivali). Kako po pretpostavci leme jedan od krajnjih vrhova svakog luka A_i, $A_i \neq A_1$, mora biti sadržan u fiksnom A_1, ukupan broj takvih lukova jednak je najviše $k-1$ (jer A_1 sadrži ukupno $k-1$ unutarnjih vrhova). Nakon što se tome pribroji luk A_1, dobiva se da je ukupan broj lukova duljine k jednak najviše k. Time je lema dokazana. □

Neka je $\mathcal{F}$ presječna familija k-članih podskupova skupa $N = \{1, 2, \ldots, n\}$. Neka vrhovi kružnice C predstavljaju elemente skupa N, a lukovi duljine k (koji imaju zajednički brid) predstavljaju k-člane podskupove presječne familije $\mathcal{F}$. Tada je, prema prethodnoj lemi, broj podskupova duljine k koji sadrže uzastopne brojeve jednak najviše k. Broj svih preostalih k-članih podskupova dobiva se permutacijom oznaka bridova kružnice C uz fiksiranu oznaku 1 jednog od bridova.



Slika 2.3: Prikaz kružnice C s permutiranim oznakama bridova

Neka je $\pi(1, 2, \ldots, n)$ bilo koja od tih cikličkih permutacija[2]. Jedna od takvih prikazana je na slici 2.3. Kako je broj vrhova kružnice jednak n, uz fiksirani brid, ukupno je $(n-1)!$ tih permutacija. Dakle, broj lukova duljine k svake permutacije jednak je najviše k, a permutacija je ukupno $(n-1)!$ pa je broj lukova najviše jednak $k(n-1)!$. Među takvim lukovima nalaze se i oni jednakih oznaka, samo u drugačijem redoslijedu i na različitim mjestima kružnice C. Shvati li se lukove kao podskupove presječne familije, zaključuje se da su cikličkim permutiranjem svi podskupovi prebrojani više puta. Potrebno je odrediti koliko se puta neki fiksirani podskup $A \in \mathcal{F}$ pojavio u svakoj cikličkoj permutaciji. Podskup A pojavljuje se u pojedinoj cikličkoj permutaciji ako se k elemenata od A uzastopno pojavljuje u nekom redoslijedu. Stoga postoji $k!$ takvih mogućnosti da se A napiše uzastopno te $(n-k)!$ načina da se rasporede preostali elementi. Prema tome fiksirani skup A pojavljuje u točno $k!(n-k)!$ cikličkih permutacija.

Dakle,

$$|\mathcal{F}| \leq \frac{k!(n-1)!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \binom{n-1}{k-1}.$$

[2] Neka je X konačni skup. Permutacija na X je bijekcija s X u X. Permutacija π je *ciklička permutacija* ako vrijedi $x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n \mapsto x_1$, gdje su $x_1, x_2, \ldots, x_n$ elementi od X u nekom redoslijedu. Ciklička permutacija zapisuje se $(x_1 x_2 \ldots x_n)$.

□

2.3 Teorija grafova

Definicija 1. *Graf G je uređeni par $(V(G), E(G))$ gdje je $V(G)$ neprazni skup vrhova, a $E(G) \subseteq \{\{v_i, v_j\} : v_i, v_j \in V(G)\}$ skup bridova.*

Sam naziv *graf* proizlazi iz mogućnosti njegovog grafičkog prikaza koji olakšava razumijevanje njegovih svojstava. Svaki vrh je grafički prikazan točkom, a svaki brid spojnicom njemu dvaju pridruženih vrhova.

Napomena 1. Graf se skraćeno označava $G = (V, E)$ ili samo G. Dva vrha v_i i v_j pridružena bridu e nazivaju se *krajevi* brida.
Takvi vrhovi zovu se i *susjedni* vrhovi. Brid $\{v_i,\ v_j\}$ kojemu su krajevi vrhovi v_i i v_j kraće se označava s $e = v_i v_j$.

Definicija 2. *Broj bridova grafa G koji sadrže vrh v naziva se* ***stupanj (valencija) vrha*** *v.*

Definicija 3. *Graf $G_1 = (V_1,\ E_1)$ je* ***podgraf*** *grafa $G = (V,\ E)$ ako je $V_1 \subseteq V$ i $E_1 \subseteq \{\{v_i,\ v_j\} \in E : v_i,\ v_j \in V_1\}$.*
Ako je $E_1 = \{\{v_i,\ v_j\} \in E : v_i,\ v_j \in V_1\}$, graf G_1 naziva se ***inducirani podgraf****.*

Definicija 4. *Graf u kojemu je svaki par vrhova brid naziva se* ***potpuni graf****. Oznaka za potpuni graf s n vrhova je K_n.*

Definicija 5. *Grafovi $G_1 = (V_1, E_1)$ i $G_2 = (V_2, E_2)$ su* ***izomorfni*** *ukoliko postoje bijekcije θ: $V_1 \to V_2$ i ϕ: $E_1 \to E_2$ takve da je v incidentan s bridom e u G_1 akko je $\theta(v)$ incidentan s bridom $\phi(e)$ u G_2.*
Dakle, izomorfizam čuva incidenciju i susjednost.

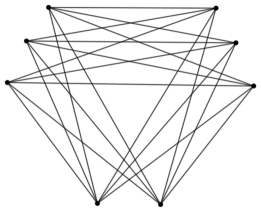
Definicija 6. *Podgraf koji je izomorfan grafu K_r zove se* ***r-klika*** *u grafu.*

Definicija 7. *Šetnja u grafu G je niz $W := v_0e_1v_1e_2 \dots e_kv_k$ čiji članovi su naizmjence vrhovi v_i i bridovi e_i, tako da su krajevi od e_i vrhovi v_{i-1} i v_i, $1 \leq i \leq k$. Šetnja W je zatvorena ako je $v_0 = v_k$.* ***Ciklus*** *je zatvorena šetnja čiji su svi bridovi međusobno različiti i čiji su svi vrhovi, osim krajeva, međusobno različiti.*

Turánov teorem

Matematičar Paul Turán 1941. godine postavio je pitanje kojim je započet razvoj novog matematičkog razmišljanja: *Ako je G jednostavan graf koji ne sadrži p-kliku, koji je najveći broj bridova koje G sadržava?* Potaknuti tim pitanjem, matematičari su počeli proučavati maksimalne ili minimalne grafove koji zadovoljavaju određeno svojstvo, što se naposljetku razvilo u teoriju nazvanu ekstremalna teorija grafova. Teorem koji odgovara na Turánovo pitanje naziva se Turánov teorem. Specijalni slučaj tog teorema, za najveći broj bridova jednostavnog grafa bez 3-klike dokazao je matematičar Willem Mantel ranije. U radu su navedena dva dokaza Turánovog teorema, oba pomoću matematičke indukcije, koja su zajednički otkrili Erdös i Turán.

Primjeri grafova koji ne sadrže p-klike mogu se dobiti dijeljenjem V na $p-1$ disjunktnih podskupova V_i, spajajući pritom dva vrha akko se oni nalaze u međusobno različitim skupovima V_i, V_j. Ako je $|V_i| = n_i$, $i = 1, \dots, p-1$, na taj način dobiveni graf $K_{n_1,\dots,n_{p-1}}$ ima $\sum_{i<j} n_in_j$ bridova (vidi sliku 2.4).
Takvim odabirom grafova, oni s maksimalnim brojem bridova dobivaju se ako se brojevi n_i podijele što ravnomjernije, odnosno ako vrijedi $|n_i - n_j| \leq 1$ za sve i, j. Drugim riječima, brojevi elemenata skupova V_i, $i = 1, \dots, p-1$ trebaju se međusobno razlikovati za najviše vrijednost 1. U suprotnom, ako postoje n_1 i n_2, $n_1 > n_2$ za koje vrijedi $n_1 - n_2 \geq 2$, pomicanjem jednog vrha iz V_1 u V_2 grafa $K_{n_1,\dots,n_{p-1}}$ dobiva se



Slika 2.4: Graf $K_{2,3,3}$

graf $K_{n_1-1,n_2+1,\ldots,n_{p-1}}$ koji sadrži barem jedan brid više nego graf $K_{n_1,\ldots,n_{p-1}}$. Naime, broj bridova čiji su krajevi iz V_1 i V_2 promijenio se s n_1n_2 na $(n_1-1)(n_2+1)$ pa iz $(n_1-1)(n_2+1)-n_1n_2 = n_1-n_2-1 \geq 1$ slijedi da dobiveni graf ima barem jedan brid više nego početni. Dakle, graf $K_{n_1,\ldots,n_{p-1}}$ ima maksimalan broj bridova ako vrijedi $|n_i - n_j| \leq 1$ za svaki i, j. Takvi grafovi nazivaju se *Turanovi grafovi*.

Posebno, ako je $|V| = n$ djeljiv s $p-1$, svi n_i mogu biti jednaki $n_i = \frac{n}{p-1}$ (najravnomjernija podjela) pa je broj bridova jednak

$$\binom{p-1}{2}\left(\frac{n}{p-1}\right)^2 = \frac{(p-2)(p-1)}{2}\cdot\frac{n^2}{(p-1)^2} = \frac{n^2(p-2)}{2(p-1)} = \left(1-\frac{1}{p-1}\right)\frac{n^2}{2}.$$

Prema Turánovom teoremu taj je broj gornja granica za broj bridova bilo kojeg grafa s n vrhova koji ne sadrži p-kliku.

Teorem 4. ***(Turánov teorem).*** *Ako graf $G = (V,\ E)$ s n vrhova ne sadrži p-kliku, $p \geq 2$, tada*

$$|E| \leq \left(1-\frac{1}{p-1}\right)\frac{n^2}{2}.$$

Dokaz. **Prvi dokaz.**

Dokaz se provodi matematičkom indukcijom po n. Ako je $n < p$, maksimalan broj bridova grafa $G = (V, E)$ jednak je $\binom{n}{2}$ kada su svake dvije točke spojene bridom. Dakle, vrijedi $|E| \leq \binom{n}{2}$. Treba pokazati da vrijedi $\binom{n}{2} \leq \left(1-\frac{1}{p-1}\right)\frac{n^2}{2}$ jer tada

vrijedi i $|E| \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}$. To slijedi iz nejednakosti koje su međusobno ekvivalente pa iz istinitosti posljednje slijedi istinitost prve.

$$\binom{n}{2} \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}$$

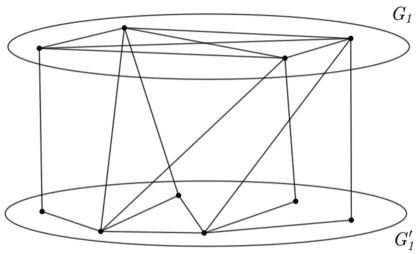
$$\frac{(n-1)n}{2} \leq \frac{n^2}{2} - \frac{n^2}{2(p-1)}$$

$$\frac{n}{2} \geq \frac{n^2}{2(p-1)}$$

$$p - 1 \geq n$$

Dakle, tvrdnja teorema vrijedi za $n < p$. Neka je dana pretpostavka da tvrdnja vrijedi za sve brojeve $n \geq p$ manje od nekog prirodnog broja k. Treba provjeriti vrijedi li tvrdnja teorema i za $n = k$, odnosno za graf s k vrhova.

Neka graf $G = (V, E)$, takav da ne sadrži p-kliku, ima $k > p$ vrhova i maksimalan broj bridova. Tada G sigurno sadrži $(p-1)$-kliku. U suprotnome bi se bridovi mogli dodati bez da se dobije p-klika, a to nije moguće jer je graf G takav da već ima maksimalan broj bridova. Neka je G_1 oznaka za $(p-1)$-kliku i G_1' oznaka za njen komplement. Za ocjenu broja bridova grafa G s k vrhova dovoljno je ocijeniti broj bridova grafova G_1 i G_1' te svih preostalih bridova, odnosno broj bridova „između" tih dvaju grafova (vidi sliku 2.5).



Slika 2.5: Graf G

Budući da su u podgrafu G_1 svaka dva vrha spojena bridom, on sadrži $\binom{p-1}{2}$ bridova. S obzirom na to da je G_1' njegov komplement, zbroj vrhova obaju grafova mora biti jednak k pa je broj vrhova komplementa jednak $k-(p-1)$. Vrijedi nejednakost $k-(p-1) \leq k$ pa je broj bridova komplementa po pretpostavci indukcije najviše jednak $\left(1-\frac{1}{p-1}\right)\frac{(k-(p-1))^2}{2}$. Broj bridova između tih dvaju grafova najviše je jednak $(p-2)(k-(p-1))$ jer svaki od $(k-(p-1))$ vrhova može imati najviše $(p-2)$ susjeda. Uz te tri ocjene, broj bridova grafa G je

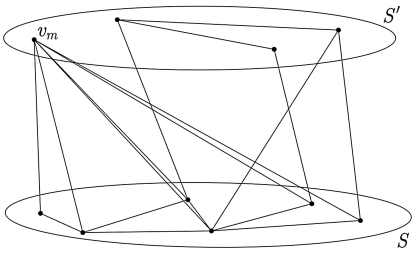
$$\begin{aligned}
|E| \leq & \binom{p-1}{2} + \left(1-\frac{1}{p-1}\right)\frac{(k-(p-1))^2}{2} + (p-2)(k-(p-1)) \\
&= \frac{(p-2)(p-1)}{2} + \frac{p-2}{p-1}\cdot\frac{(k-p+1)^2}{2} + (p-2)(k-p+1) \\
&= \frac{(p-2)(p-1)^2}{2(p-1)} + \frac{p-2}{p-1}\cdot\frac{(k-p+1)^2}{2} + \frac{2(p-1)(p-2)(k-p+1)}{2(p-1)} \\
&= \frac{p-2}{2(p-1)}\cdot((p-1)^2 + (k-p+1)^2 + 2(p-1)(k-p+1)) \\
&= \frac{p-2}{2(p-1)}\cdot((p-1)+(k-p+1))^2 \\
&= \frac{p-2}{2(p-1)}\cdot k^2 \\
&= \left(1-\frac{1}{p-1}\right)\frac{k^2}{2}.
\end{aligned}$$

Dakle, tvrdnja teorema vrijedi i za sljedbenika k pa po principu matematičke indukcije tvrdnja teorema vrijedi za sve n. □

Dokaz. **Drugi dokaz.**

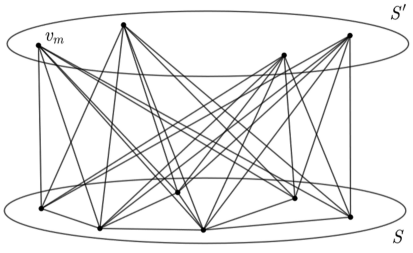
Dokaz se provodi matematičkom indukcijom po n. Ako je $n < p$, tvrdnja teorema vrijedi (vidi prvi dokaz). Neka tvrdnja teorema vrijedi za sve prirodne brojeve $n \geq p$ manje od nekog prirodnog broja k. Treba pokazati da tvrdnja vrijedi i za k. Neka

je $G = (V, E)$ graf s $k > p$ vrhova i maksimalnim brojem bridova takav da ne sadrži p-kliku. Vrh $v_m \in V$ najvećeg je stupnja $d_m = \max\limits_{1 \leq j \leq n} d_j$. Ako je S skup svih vrhova susjednih v_m, tada je broj elemenata tog skupa jednak $|S| = d_m$. Neka je S' komplement skupa S (vidi sliku 2.6).



Slika 2.6: Graf G

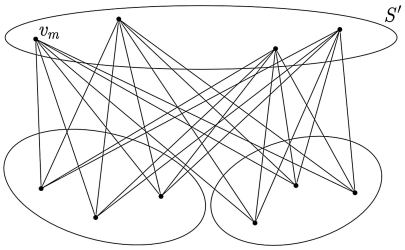
Svaki element skupa S susjedan je v_m i graf G je takav da ne sadrži p-kliku pa skup S ne sadrži $p-1$ elemenata takvih da su svaka dva povezana bridom. U suprotnom bi ti elementi s v_m i pripadajućim im bridovima činili p-kliku.
Neka je H graf s k vrhova takav da sadrži podskup S i sve bridove čiji su krajevi sadržani u S kao što je i u grafu G. Neka sadrži i njegov komplement S' čiji nijedan par vrhova nije spojen bridom. Osim toga, neka takav graf H sadrži sve bridove čiji je jedan kraj iz S, a drugi iz S' (vidi sliku 2.7).



Slika 2.7: Graf H

Takav graf H ne sadrži podskup p-kliku. Neka je d'_j stupanj vrha v_j. Ako se v_j nalazi

u S, tada vrijedi $d'_j \geq d_j$ prema konstrukciji grafa H. Ako se v_j nalazi u S', tada vrijedi $d'_j = |S| = d_m \geq d_j$ prema izboru v_m. Dakle, za stupanj vrha v_j iz H vrijedi $d'_j \geq d_j$ neovisno o tome u kojem se skupu nalazi. Stupanj vrha v_j iz H barem je jednak stupnju vrha v_j iz G za svaki j pa vrijedi $|E(H)| \geq |E(G)|$. Dakle, među svim grafovima s maksimalnim brojem bridova postoji graf H koji ima više bridova nego graf G. Ako se skup S podijeli na particiju skupova tako da nijedan par elementa bilo kojeg od tih skupova nije susjedan (na prethodno opisani način), iz grafa H dobiva se Turanov graf $K_{n_1,\ldots,n_{p-1}}$, gdje je $n_{p-1} = |S'|$ (vidi sliku 2.8).



Slika 2.8: Turanov graf

Broj vrhova skupa S jednak je $d_m < k$ pa pretpostavka indukcije vrijedi za podgraf s vrhovima iz S i bridovima između njih. Dakle, broj bridova takvog podgrafa je barem $\left(1 - \frac{1}{p-1}\right) \frac{d_m^2}{2}$ pa je broj bridova Turanovog grafa $K_{n_1,\ldots,n_{p-2}}$ veći ili jednak tome. Uz $|E(K_{n_1,\ldots,n_{p-2}})| \leq |E(K_{n_1,\ldots,n_{p-1}})|$ slijedi

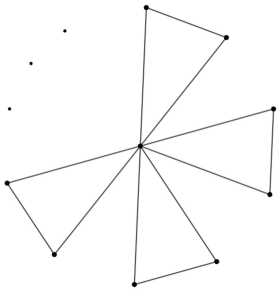
$$|E(G)| \leq |E(H)| \leq |E(K_{n_1,\ldots,n_{p-1}}| \leq \left(1 - \frac{1}{p-1}\right) \frac{k^2}{2}.$$

Dakle, tvrdnja teorema vrijedi i za k, pa po principu matematičke indukcije tvrdnja teorema vrijedi za sve n.

□

Teorem o prijateljstvu

Teorem o prijateljstvu reformulacija je jednog matematičkog problema nepoznatog podrijetla: *U nekom društvu od barem troje ljudi svake dvije osobe imaju točno jednog zajedničkog prijatelja. U tom društvu tada postoji osoba („političar") koja je svakome iz tog društva prijatelj.* U terminima teorije grafova problem se može prikazati grafom $G = (V, E)$, $|V| = n \geq 3$, u kojem vrhovi skupa V predstavljaju članove tog društva, a bridovi predstavljaju prijateljstvo odgovarajućih članova tog društva. Podrazumijeva se da je prijateljstvo obostrano i da nitko nije sam sebi prijatelj. Takvi grafovi u kojemu svaka dva vrha imaju točno jedan zajednički susjedni vrh („zajednički prijatelj") oblika su vjetrenjače (vidi sliku 2.9). To je prvi dokazao Paul Erdös u suradnji s Alfredom Rényiem i Verom Sós. Teorem je među matematičarima poznat kao *teorem o prijateljstvu*.



Slika 2.9: Vjetrenjača graf

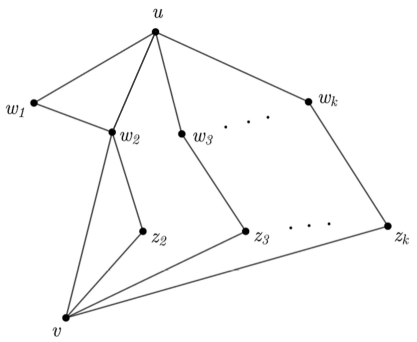
Teorem 5. *Neka je G jednostavni graf s $n \geq 3$ vrhova u kojem svaka dva vrha imaju točno jedan zajednički susjedan vrh. Tada postoji vrh susjedan svim vrhovima grafa G.*

Dokaz. Neka je zadan jednostavni graf $G = (V, E)$ s $n \geq 3$ vrhova čija svaka dva vrha imaju točno jedan zajednički susjedni vrh. Neka za takav graf vrijedi suprotno

tvrdnji teorema, odnosno neka ne postoji vrh susjedan svim preostalim vrhovima grafa. Graf G ne sadrži ciklus C_4 jer bi u suprotnom vrhovi u i v imali najmanje dva zajednička susjeda (kao suprotni vrhovi kvadrata). U nastavku će se dokazati da za takav graf G vrijedi $d(u) = d(v)$, za svako $u, v \in V$.

Neka su prvo neka dva vrha u i v takva da nisu susjedna i neka je s k označena vrijednost stupnja vrha u, $d(u) = k$, $2 \leq k \leq n-1$. To znači da postoji k bridova čiji je jedan kraj u. Neka su $w_1, \ldots, w_k$ preostali krajevi odgovarajućeg brida susjedni s u. Kako po pretpostavci teorema vrhovi u i v moraju imati točno jedan susjedni vrh, jedan od vrhova w_i susjedan je s v. Neka je to vrh w_2. Iz istog razloga vrhovi w_2 i u moraju imati točno jedan susjedni vrh pa je w_2 susjedan s točno jednim od preostalih w_i, recimo s w_1. Vrh v ima s w_1 zajedničkog susjeda w_2, a s w_i, $i \geq 2$, zajedničkog susjeda z_i, $i \geq 2$ (vidi sliku 2.10). Graf ne sadrži ciklus C_4 pa svi z_i moraju biti međusobno različiti. U suprotnom bi, za npr. $z_2 = z_3$, graf sadržavao ciklus $uw_2z_2w_3$. Stoga vrijedi $d(v) \geq k = d(u)$ pa iz simetrije slijedi $d(u) = d(v)$ za bilo koje nesusjedne vrhove u i v.

Kako graf ne sadrži ciklus C_4, bilo koji vrh $w_i \neq w_2$ susjedan je s najviše jednim od u i v i stoga $d(w_i) = d(u) = d(v)$, gdje $w_i \neq w_2$. Konačno, w_2 nije susjedan svim vrhovima pa i za w_2 vrijedi $d(w_2) = d(u) = d(v)$.



Slika 2.10: Vrhovi u i v nisu susjedni vrhovi

Ako su u i v susjedni vrhovi, bilo koji od vrhova $w_i \neq w_2$ nije susjedan s u i taj se slučaj svodi na prethodni.

Dakle, stupanj svakog vrha grafa G jednak je k, $2 \leq k \leq n-1$.

Ukupan broj vrhova može se izračunati sada kada se zna da je stupanj svakog vrha jednak k. Kako po pretpostavci teorema svaki vrh ima točno jednog zajedničkog susjeda s u, dovoljno je zbrajati stupnjeve vrha v i njegovih susjeda. Zbog toga se jedino u broji više puta. Zbroj stupnjeva svakog vrha w_i susjednog vrhu u jednak je k^2 čime se u brojao ukupno k puta pa je tom zbroju potrebno oduzeti $k-1$. Time se dobiva da je broj vrhova grafa G jednak

$$n = k^2 - k + 1.$$

U drugom dijelu dokaza koriste se neki standardni rezultati iz linearne algebre. Ako se definira *matrica susjedstva* grafa G kao $n \times n$ matrica $A = A(G) = [\,\alpha_{ij}]$, gdje je α_{ij} = broj bridova koji spajaju v_i i v_j, onda se jednostavni graf može prikazati matricom koja se sastoji od samo nula i jedinica (jer su dva vrha spojena najviše jednim bridom) koja na glavnoj dijagonali sadrži samo nule. Kako je za graf G dokazano da vrijedi $d(v) = k$, $\forall v$, slijedi da svaki redak iz A ima točno k jedinica, a iz uvjeta teorema da za svaka dva retka postoji točno jedan stupac gdje oni imaju obje jedinice. Neka je $A^2 = [\,\alpha_{ij}^2]$ kvadrat matrice A. Tada je

$$\alpha_{ii}^2 = \sum_{r=1}^{n} \alpha_{ir}\alpha_{ri} \overset{A \text{ simetrična}}{=} \sum_{r=1}^{n} \alpha_{ir}^2 = k$$

jer u svakom retku od A se nalazi točno k jedinica. Ako je $i \neq j$, onda je

$$\alpha_{ij}^2 = \sum_{r=1}^{n} \alpha_{ir}\alpha_{rj} = \sum_{r=1}^{n} \alpha_{ir}\alpha_{jr} = 1,$$

zbog toga što za svaka dva retka postoji točno jedan stupac na kojem su obje jedinice.

Dakle,

$$A^2 = \begin{bmatrix} k & 1 & \dots & 1 \\ 1 & k & & 1 \\ \vdots & & \ddots & 1 \\ 1 & \dots & 1 & k \end{bmatrix} = (k-1)I + J,$$

gdje je I jedinična matrica, a J se sastoji od samih jedinica. Lako je provjeriti da J ima svojstvene vrijednosti n (višestrukosti 1) i 0 (višestrukosti $n-1$). Stoga A^2 ima svojstvene vrijednosti $k-1+n = k^2$ (višestrukosti 1) i $k-1$ (višestrukosti $n-1$). Kako je A simetrična i zato se može dijagonalizirati, A ima svojstvene vrijednosti $\pm k$ (višestrukosti 1) i $\pm\sqrt{k-1}$. Kako je višestrukost $\pm k$ jednaka 1, A ima ili svojstvenu vrijednost k ili svojstvenu vrijednost $-k$. Neka je to k, a za $-k$ je zaključivanje analogno.

Neka je r svojstvenih vrijednosti jednako $\sqrt{k-1}$, a s svojstvenih vrijednosti jednako $-\sqrt{k-1}$, pri čemu je $r+s = n-1$. Suma svih svojstvenih vrijednosti od A je jednaka tragu $TrA = 0$ pa je

$$k + r\sqrt{k-1} - s\sqrt{k-1} = 0,$$

pa je posebno $r \neq s$ i

$$\sqrt{k-1} = \frac{k}{s-r}.$$

Lema 7. *Za $a, m \in \mathbb{N}$ je $\sqrt[n]{a}$ ili cijeli ili iracionalni broj.*

$\sqrt[n]{a}$ je rješenje jednadžbe $x^n - a = 0$. Neka vrijedi pretpostavka $\sqrt[n]{a} \in \mathbb{Q}$. Tada postoje relativno prosti brojevi $p \in \mathbb{Z}$, $q \in \mathbb{N}$ takvi da je $\sqrt[n]{a} = \frac{p}{q}$ rješenje navedene jednadžbe. Kako je $\frac{p}{q}$ rješenje jednadžbe $x^n - a = 0$ mora vrijediti $\left(\frac{p}{q}\right)^n - a = 0$ što je ekvivalentno s $aq^n = 1 \cdot p^n$. Kako su p i q relativno prosti slijedi da p i q nisu međusobno djeljivi pa ni p^n i q^n nisu međusobno djeljivi. Stoga q mora biti djelitelj

od $1 \cdot p$ što povlači da je g djelitelj broja 1. Iz $q = 1$ i $\sqrt[n]{a} = \frac{p}{q}$ slijedi $\sqrt[n]{a} = p$ pa $\sqrt[n]{a} \in \mathbb{Z}$. Dakle, $\sqrt[n]{a} \in \mathbb{Z}$ ili $\sqrt[n]{a} \notin \mathbb{Q}$. □

Iz leme 7 slijedi da je $\sqrt{k-1}$ cijeli broj. Neka $\sqrt{k-1} = t$, $t \in \mathbb{Z}$. Slijedi

$$t(s - r) = k = t^2 + 1$$

pa t dijeli $t^2 + 1$. Budući da t dijeli t^2 slijedi da t dijeli dva uzastopna broja pa mora vrijediti $t = 1$. Stoga je $k = 2$.

Dakle, za graf vrijede jednakosti $n = k^2 - k + 1$ i $k = 2$ iz kojih slijedi kontradikcija s pretpostavkom. Naime, uvrštavanjem druge jednakosti u prvu dobiva se $n = 3$, odnosno graf G sadrži $n = 3$ vrha. Kako prema pretpostavci teorema svaka dva vrha imaju točno jedan zajednički susjedni vrh, a vrhova je ukupno 3, graf je potpun (svaki par vrhova je brid). To znači da svaki je vrh susjedan preostalim vrhovima grafa što je u kontradikciji s time da takav vrh ne postoji. Dakle, tvrdnja da ne postoji vrh susjedan preostalima netočna je pa graf koji zadovoljava pretpostavku teorema mora sadržavati vrh susjedan preostalim vrhovima.

□

Teorem o prijateljstvu ne vrijedi za beskonačne grafove. Doista, za induktivnu konstrukciju protuprimjera može se, na primjer, započeti s 5-ciklusom, i uzastopno dodavati zajedničke susjede svim parovima vrhova koji ih još nemaju. To vodi do (prebrojivo) beskonačnog grafa prijateljstva bez političara (vidi [2], str. 223).

Bibliografija

[1] https://www.theoremoftheday.org/CombinatorialTheory/EKR/TotDEKR.pdf, posjećena 30.1.2019.

[2] Martin Aigner i Günter M Ziegler, *Proofs from The Book. Including illustrations by Karl H. Hofmann*, 2004.

[3] Laszlo Babai, Carl Pomerance i Peter Vertesi, *The Mathematics of Paul Erdős*, (1998).

[4] László Babai i Joel Spencer, *Uncle Paul*, NOTICES OF THE AMS **45** (1998), br. 1.

[5] John Adrian Bondy, Uppaluri Siva Ramachandra Murty et al., *Graph theory with applications*, sv. 290, Citeseer, 1976.

[6] Ivana Bubić, *Život i djelo Paula Erdősa*, 2012, http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/BUB03.pdf.

[7] Zvonimir Bujanović i Boris Muha, *Elementarna matematika 1*, 2018, https://web.math.pmf.unizg.hr/nastava/em/EM1/materijali/em1-skripta.pdf.

[8] Andrijana Ćurković, Borka Jadrijević i Marina Simić, *Bertrandov postulat*, Osječki matematički list **17** (2017), br. 2, 139–150.

[9] Paul Erdős i János Surányi, *Topics in the Theory of Numbers*, Springer, 2003.

[10] Jacob Fox, *Lecture 20: Friends and politicians*, http://math.mit.edu/~fox/MAT307-lecture20.pdf.

[11] David Galvin, *Erdos's proof of Bertrand's postulate*, 2006.

[12] Paul Hoffman, *The man who only loved numbers: the story of Paul Erdös and the search for mathematical truth*, [sn], 1998.

[13] Ivica Nakić, *Diskretna matematika*, 2011/2012, https://web.math.pmf.unizg.hr/nastava/komb/predavanja/predavanja.pdf.

[14] Darko Veljan, *Kombinatorna i diskretna matematika*, Algoritam, 2001.

[15] Elizabeth Walker, *The Friendship Theorem*, 2016, https://math.mit.edu/~apost/courses/18.204-2016/18.204_Elizabeth_Walker_final_paper.pdf.

Sažetak

U prvom poglavlju ovog diplomskog rada prikazan je život mađarskog matematičara iz 20. stoljeća, Paula Erdösa. U drugom poglavlju rada nalaze se odabrani dokazi iz triju matematičkih područja, teorije brojeve, kombinatorike i teorije grafova.
U *Teoriji brojeva* iznijet je dokaz tvrdnje da je skup prostih brojeva beskonačan i dokaz Bertrandovog postulata. U *Kombinatorici* je prikazan dokaz Teorema Erdös-Ko-Rado, a u *Teoriji grafova* dokaz Turánovog teorema i Teorema o prijateljstvu.

Summary

In the first chapter of this graduate thesis is presented the life of Hungarian mathematician from the 20th century, Paul Erdös. In the second chapter there are selected proofs from three mathematical areas, number theory, combinatorics and graph theory. Section *Number theory* gives proof of the infinity of primes and proof of Bertrand's postulate. *Combinatorics* gives proof of Erdös-Ko-Rado theorem and *Graph theory* gives the proof of Turán's theorem and Friendship Theorem.

Životopis

Rođena sam 17.8.1991. u Žepču. Osnovnoškolsko obrazovanje završila sam u Osnovnoj školi Sveta Nedelja, a srednjoškolsko u XI. gimnaziji u Zagrebu. Preddiplomski studij nastavničkog smjera matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta upisala sam 2010/2011, a završila 2013/2014. godine. Diplomski studij nastavničkog smjera Matematike upisala sam 2014/2015. godine.