UNIVERZITET U NOVOM SADU
PRIRODNO - MATEMATIČKI
FAKULTET
DEPARTMAN ZA MATEMATIKU I
INFORMATIKU

Nikolina Miholjčić

Kombinatorni „Nullstellensatz”

Master rad

Mentor:
dr Bojan Bašić

Novi Sad, 2023

Sadržaj

Predgovor

Kombinatorni „Nullstellensatz" predstavlja vrlo moćnu algebarsku tehniku koju je razvio Noga Alon[1] 1999. godine [3]. Riječ je o metodi koja počiva na polinomima, premda se oni koriste za donošenje određenih kombinatornih zaključaka. Moć pomenute algebarske tehnike se ogleda u njenoj šarenolikoj i bogatoj primjeni u raznoraznim oblastima matematike, među kojima izdvajamo kombinatoriku, aditivnu teoriju brojeva, teoriju grafova, linearnu algebru, višedimenzionalnu kombinatornu geometriju, kao i mnoge druge. Implementacija same metode je iznimno jednostavna, pri čemu sva težina problema leži u pametnom odabiru polinoma koji će nas dovesti do željenog epiloga.

U ovom radu ćemo se baviti Alonovom algebarskom tehnikom, pri čemu će akcenat biti stavljen na najrazličitije primjene. Napomenimo da je osnovna ideja rada da ubijedi čitaoca u moć pomenute tehnike, te ćemo stoga za mnogobrojne rezultate u radu navesti po dva dokaza. Pri tome će prvi dokaz biti klasičan i nerijetko zahtijevati više usputnih lema i tvrđenja, dok će drugi dokaz pomoću Kombinatornog „Nullstellensatza" biti znatno jednostavniji i kraći.

U uvodnom dijelu ćemo uvesti glavni alat ovog rada, ali i istaći njegovu povezanost sa Hilbertovim[2] „Nullstellensatzom", rezultatom na kojem počiva čitava jedna oblast pod nazivom algebarska geometrija.

Potom ćemo u sljedećoj glavi dati dvije glavne teoreme koje jednim imenom nazivamo Kombinatorni „Nullstellensatz" i njihove detaljne dokaze.

Centrani dio rada biće posvećen svakojakim primjenama. Za početak, izdvojićemo dvije klasične primjene, kako ih je sam Alon nazvao, a to su Chevalley[3]–Warningova teorema o zajedničkim nulama skupa polinoma, kao i Cauchy[4]–Davenportova[5] teorema o donjoj granici kardinalnog broja sume dva neprazna podskupa grupe $\mathbb{Z}_p$. Za oba rezultata daćemo originalne dokaze,

[1]Noga Alon (1956–), izraelski matematičar
[2]David Hilbert (1862–1943), njemački matematičar
[3]Claude Chevalley (1909–1984), francuski matematičar
[4]Augustin–Louis Cauchy (1789–1857), francuski matematičar
[5]Harold Davenport (1907–1969), engleski matematičar

a potom dokaze pomoću našeg glavnog alata.

U nastavku ćemo navesti jedan rezultat o restrikovanim sumama, koji ćemo takođe dokazati na dva načina. Zatim ćemo pokazati kako se Cauchy–Davenportova teorema, kao i Erdős[6]–Heilbronnova[7] teorema mogu dokazati koristeći pomenuti rezultat.

Sljedeći odjeljak rada biće posvećen poznatoj EGZ teoremi, njenim dokazima i primjenama. Daćemo čak pet dokaza, pri čemu će prvi koristiti Cauchy–Daveportovu teoremu, drugi Chevalley–Warningovu teoremu, treći će biti čisto kombinatorni dokaz, a za četvrti ćemo formulisati i dokazati Olsonovu teoremu, kao i jednu njenu posljedicu koje će nam biti potrebne kasnije u radu.

Zatim ćemo preći na jedan rezultat iz linearne algebre, a to je lema o permanentama, koju ćemo ponovo dokazati na dva načina. Pomoću nje ćemo dati peti dokaz EGZ teoreme, a potom i neke njene primjene u rješavanju još nekih problema kao što su Harborthov[8] problem, Jaegerova[9] hipoteza, jedan problem sa aditivnim bazama, kao i primjena na problem sa orijentisanim grafovima.

Sljedeća cjelina rada će biti posvećena grafovima. Tu ćemo dati kratak uvod u sve potrebne definicije, a potom ćemo preći na jedan rezultat koji se može posmatrati kao uopštenje Berge[10]–Sauerove[11] hipoteze. Taj rezultat ćemo dokazati na dva načina. Daćemo još jedan problem iz teorije grafova koji je dokazan pomoću Kombinatornog „Nullstellensatza".

Dalje ćemo preći na priču o problemima bojenja grafova, gdje ćemo nakon svih potrebnih definicija dati kriterijum bojenja koji su uveli Alon i Tarsi[12]. Riječ je o kriterijumu koji se bazira na svim mogućim orijentacijama grafa. Ponovo ćemo dokazati taj rezultat na dva načina i dati nekoliko njegovih primjena, a to su problem o konturi i trouglovima, rezultat o odabirnom broju planarnog bipartitnog grafa i o odabirnom broju linijskog grafa.

Uslijediće i nekoliko rezultata koji tvrde da graf ima određeno svojstvo ako pripada nekom idealu.

Zatim ćemo definisati hipergraf i njegovo bojenje, nakon čega ćemo dati dva rezultata koji tvrde da je hipergraf sa određenim osobinama obojiv sa određenim brojem boja ako dati polinomi pripadaju nekom idealu. Oba rezultata ćemo dokazati pomoću našeg glavnog alata.

---

[6]Pál Erdős (1913–1996), mađarski matematičar

[7]Hans Heilbronn (1908–1975), njemački matematičar

[8]Heiko Harborth (1938–), njemački matematičar

[9]François Jaeger (1947–1997), francuski matematičar

[10]Claude Jacques Berge (1926–2002), francuski matematičar

[11]Nobert Sauer, kanadski matematičar

[12]Michael Tarsi, izraelski matematičar

Nakon toga ćemo dati teoremu koja daje potreban i dovoljan uslov da sudoku bude rješiv i dokazaćemo je koristeći Kombinatorni „Nullstellensatz".

Naposletku, dajemo jedan rezultat o pokrivanju tjemena hiperkocke hiperravnima, kao i jedan rezultat koji uključuje Hopf–Stiefelov uslov, čime ćemo završiti ovaj rad.

* * *

Veliku zahvalnost dugujem svom mentoru, dr Bojanu Bašiću, koji je svojim savjetima i sugestijama dosta doprinio pisanju ovog rada. Zahvaljujem se za ukazano povjerenje i nesebičnu pomoć oko izbora teme, kao i za preneseno znanje tokom studija.

Zahvaljujem se i dr Petru Markoviću i dr Rozaliji Madaras-Silađi što su prihvatili da budu članovi komisije, pokazali predusretljivost i svojim sugestijama značajno unaprijedili ovaj rad.

Takođe, želim da se zahvalim i svim ostalim profesorima i asistentima, od kojih sam mnogo naučila za vrijeme svog studiranja.

Hvala i svim mojim prijateljima, što su uvijek vjerovali u mene.

Naposletku, najveću zahvalnost dugujem mojoj porodici, mami i bratu, koji su mi najveća podrška na svakom koraku ovog puta koji zovemo život. Zahvalna sam što vas imam.

Ovaj rad posvećujem pokojnom ocu Milanu.

Novi Sad, septembar 2023.

Nikolina Miholjčić

Glava 1

Uvod

U uvodnom dijelu dajemo kratak pregled veze između fundamentalne teoreme algebarske geometrije, Hilbertovog „Nullstellensatza" i teoreme na kojoj se temelji ovaj rad, Kombinatornog „Nullstellensatza".

1.1 Hilbertov „Nullstellensatz"

Algebarska geometrija je matematička disciplina koja se bavi proučavanjem geometrijskih objekata, ali koristeći algebarske alate i to najčešće iz komutativne algebre. Konkretno, bavi se proučavanjem nula polinoma po više promjenljivih. Dakle, algebarska struktura je prsten polinoma, a geometrijski objekat je skup nula tog polinoma i njega nazivamo algebarskim varijetetom.

Jedna od fundamentalnih teorema na kojoj počiva čitava oblast algebarske geometrije jeste teorema pod nazivom Hilbertov „Nullstellensatz", što u slobodnom prijevodu znači „teorema o lokacijama nula". Riječ je o rezultatu koji je formulisao i dokazao David Hilbert 1893. godine u radu [35].

Prije nego što formulišemo samu teoremu, dajemo nekoliko potrebnih definicija iz teorije prstena i polja.

Definicija 1.1. Neka je $(R, +, \cdot)$ proizvoljan prsten. Definišemo $R[x_1, ..., x_n] = (\{f(x_1, ..., x_n)$: f je polinom po n promjenljivih sa koeficijentima iz R$\}$,+,$\cdot)$. Sabiranje i množenje su standardne operacije sabiranja i množenja polinoma.

Definicija 1.2. Neka su K i F polja i $F \leq K$ (F je potpolje od K). Tada kažemo da je K proširenje polja F. Takođe, K možemo posmatrati kao vektorski prostor nad F, gdje sa $[K : F]$ označavamo dimenziju tog vektorskog prostora i tu vrijednost zovemo stepenom proširenja K nad F.

Definicija 1.3. Neka je $a = (a_1, ..., a_n) \in K$, gdje je K proširenje polja F. Kažemo da je a algebarski nad F ako postoji $f \in F[x_1, ..., x_n]$ tako da je $f(a_1, ..., a_n) = 0$.

Definicija 1.4. Neka je K proširenje polja F. Kažemo da je K algebarsko proširenje ako za svaki element $a \in K$ važi da je a algebarski nad F.

Definicija 1.5. Polje F je algebarski zatvoreno ako nema pravih algebarskih proširenja.

Sada imamo sav potreban alat za formulaciju Hilbertove teoreme.

Teorema 1.1. *(Hilbertov „Nullstellensatz") Neka je F algebarski zatvoreno polje i neka su $f, g_1, ..., g_m$ polinomi koji pripadaju prstenu polinoma $F[x_1, ..., x_n]$. Ako je f polinom koji se anulira nad svim zajedničkim nulama polinoma $g_1, ..., g_m$, onda postoji prirodan broj k i polinomi $h_1, ..., h_m \in F[x_1, ..., x_n]$ tako da je*

$$f^k = \sum_{i=1}^{n} h_i g_i.$$

Napomena 1.2. Gore navedena teorema može se ispričati i jezikom algebarske geometrije, koristeći varijatete i druge pojmove iz te oblasti, ali nama je ovaj oblik sasvim odgovarajući jer se u nastavku rada nećemo baviti algebarskom geometrijom.

Više od jednog vijeka kasnije (1999), Noga Alon je formulisao teoremu koja se može doživjeti kao kombinatorna verzija Hilbertovog „Nullstellensatza", koju je Alon onda zgodno nazvao Kombinatorni „Nullstellensatz". Riječ je o jednoj polinomnoj metodi, na kojoj je godinama radio sa nekoliko saradnika, a konačan rezultat je prvi put formulisao u radu [3].

Kombinatorni „Nullstellensatz" se zapravo sastoji od dvije teoreme. Prva teorema, koju ćemo nazvati Kombinatorni „Nullstellensatz" 1, je pojačanje Hilbertovog „Nullstellensatza" koje se dobija u specijalnom slučaju kada u teoremi 1.1 stavimo da je $m = n$ i da je $g_i = \prod_{s \in S_i}(x_i - s)$ za $i = 1, ..., m$. Ovaj rezultat ima veliku primjenu u teoriji grafova i u radu ga koristimo za teoreme koje tvrde da grafovi ili hipergrafovi imaju neko svojstvo ako određeni polinom pripada datom idealu.

Kombinatorni „Nullstellensatz" 2 je zapravo jednostavna posljedica Kombinatornog „Nullstellensatza" 1. To je teorema koja tvrdi da, za svako polje F i svaki polinom $f \in F[x_1, ..., x_n]$ koji zadovoljava određene uslove, postoji n-torka $(x_1, ..., x_n) \in F^n$ tako da je $f(x_1, ..., x_n) \neq 0$. Za razliku od Kombinatornog „Nullstellensatza" 1, ova teorema je lako primjenljiva u najrazličitijim

oblastima matematike i nju koristimo u većini rezultata koji su navedeni u radu.

U sljedećoj glavi formulišemo pomenute centralne teoreme i dajemo njihove detaljne dokaze.

Glava 2

Centralne teoreme sa dokazima

U ovoj glavi izložićemo dvije glavne teoreme, koje jednim imenom nazivamo Kombinatorni „Nullstellensatz" i na kojima se temelji ovaj rad. Iako one predstavljaju moćan alat koji se koristi u najrazličitijim oblastima matematike, njihov dokaz je prilično jednostavan i tehnički.

Za dokaz prve teoreme biće nam potrebna jedna pomoćna lema, koja je poznat rezultat od ranije [4], dok se druga teorema može dokazati kao posljedica prve.

2.1 Pomoćna lema

Lema 2.1. *Neka je F proizvoljno polje i neka $f \in F[x_1, ..., x_n]$. Pretpostavimo da je t_i najveći stepen x_i u polinomu f, za $1 \leq i \leq n$ i neka je $S_i \subset F$ podskup koji sadrži bar $t_i + 1$ različitih elemenata polja F. Ako je $f(x_1, ..., x_n) = 0$ za sve n-torke $(x_1, ..., x_n) \in S_1 \times S_2 \times ... \times S_n$, onda je $f \equiv 0$.*

Dokaz. Dokaz dajemo indukcijom po n. Za $n = 1$, imamo polinom po jednoj promjenljivoj x_1 i to stepena t_1. Kako znamo da polinom stepena t_1 može imati najviše t_1 nula, a mi imamo da je $f(x_1) = 0$, za bar $t_1 + 1$ elemenata, mora biti $f \equiv 0$.

Sada pretpostavimo da tvrđenje važi za $n - 1$ i pokažimo za n $(n \geq 2)$. Neka je $f = f(x_1, ..., x_n)$ i neka je $S_i \subset F$, takav da $|S_i| \geq t_i + 1$, za $1 \leq i \leq n$. Primijetimo da polinom f uvijek možemo posmatrati kao polinom po x_n čiji su koeficijenti iz $F[x_1, ..., x_{n-1}]$, na sljedeći način:

$$f = \sum_{i=0}^{t_n} f_i(x_1, ...x_{n-1}) x_n^i. \tag{2.1}$$

U polinomu f_i najveći stepen x_j je t_j. Neka je sada $(s_1, ..., s_{n-1}) \in S_1 \times S_2 \times ... \times S_{n-1}$ jedna fiksirana $(n-1)$-torka. Tada je $f(s_1, ..., s_{n-1}, x_n)$ polinom po 1

promjenljivoj, pa imamo istu situaciju kao u bazi. Znamo da je $f(s_1, ..., s_n) = 0$, za svako $s_n \in S_n$, a S_n ima bar $t_n + 1$ elemenata.

Ponovo, kako je $\deg(f) = t_n$, dobijemo da je pomenuti polinom po jednoj promjenljivoj identički jednak nuli. Odnosno $f_i(x_1, ..., x_{n-1}) = 0$ za sve $(x_1, ..., x_{n-1}) \in S_1 \times ... \times S_{n-1}$. Sada je na osnovnu indukcijske hipoteze $f_i \equiv 0$, za $1 \leq i \leq t_n$, odakle konačno slijedi da je $f \equiv 0$, što je i trebalo dokazati. □

2.2 Kombinatorni „Nullstellensatz"

Sada prelazimo na dvije glavne teoreme, njihove formulacije i dokaze, koji su prvi put predstavljeni u [3].

Teorema 2.2. *(Kombinatorni „Nullstellensatz" 1) Neka je F proizvoljno polje i neka $f \in F[x_1, ..., x_n]$. Neka su $\emptyset \neq S_i \subset F$ i definišimo*

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s),$$

za $1 \leq i \leq n$. Ako je $f(s_1, ..., s_n) = 0$ za sve $s_i \in S_i$, onda postoje polinomi $h_1, h_2, ..., h_n \in F[x_1, ..., x_n]$ takvi da je $deg(h_i) \leq deg(f) - deg(g_i)$ i

$$f = \sum_{i=1}^{n} h_i g_i.$$

Štaviše, ako $f, g_1, ..., g_n \in R[x_1, ..., x_n]$, gdje je R neki potprsten od F, onda i $h_i \in R[x_1, ..., x_n]$, za $1 \leq i \leq n$.

Dokaz. Definišimo $t_i := |S_i| - 1$, za $1 \leq i \leq n$. Tada je za sve i ispunjeno

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s) = x_i^{|S_i|} - \sum_{j=0}^{|S_i|-1} q_{i,j} x_i^j = x_i^{t_i+1} - \sum_{j=0}^{t_i} q_{i,j} x_i^j, \tag{2.2}$$

gdje su $q_{i,j}$ odgovarajući koeficijenti. Primijetimo da je za $x_i \in S_i$ zadovoljeno $g_i(x_i) = 0$, stoga za te x_i važi

$$x_i^{t_i+1} = \sum_{j=0}^{t_i} q_{i,j} x_i^j. \tag{2.3}$$

Definišimo sada polinom $\tilde{f}$ koji se dobija od polinoma f tako što svako pojavljivanje $x_i^{f_i}$ gdje je $f_i > t_i$ zamijenimo zbirom monoma manjeg stepena,

na gore opisan način (2.3). Ideja je da dobijemo polinom na koji ćemo primijeniti lemu 2.1, pa stoga vršimo možda pomalo neočekivane transformacije našeg polinoma f. Demonstriraćemo opisani postupak na primjeru.

Ako je $f_i = t_i + 1$, primijenićemo (2.2):

$$x_i^{t_i+1} = g_i(x_i) + \sum_{j=0}^{t_i} q_{i,j} x_i^j, \tag{2.4}$$

pri čemu se g_i anulira za $x_i \in S_i$.
Ako je $f_i = t_i + 2$, prvo pomnožimo jednačinu (2.4) sa x_i :

$$\begin{aligned}
x_i^{t_i+2} &= g_i(x_i)x_i + \sum_{j=0}^{t_i} q_{i,j} x_i^{j+1} \\
&= g_i(x_i)x_i + q_{i,t_i} x_i^{t_i+1} + \sum_{j=0}^{t_i-1} q_{i,j} x_i^{j+1} \\
&= g_i(x_i)x_i + q_{i,t_i} g_i(x_i) + q_{i,t_i} \sum_{j=0}^{t_i} q_{i,j} x_i^j + \sum_{j=1}^{t_i} q_{i,j-1} x_i^j \qquad (2.5) \\
&= g_i(x_i)(x_i + q_{i,t_i}) + \sum_{j=0}^{t_i} (q_{i,t_i} q_{i,j} + h_{i,j}) x_i^j \\
&= g_i(x_i)h_i + \sum_{j=0}^{t_i} m_{i,j} x_i^j \qquad (2.6)
\end{aligned}$$

U (2.5) smo definisali $h_{i,0} = 0$ i za sve $j > 0$ je $h_{i,j} = q_{i,j-1}$. U (2.6) smo definisali $m_{i,j} = q_{i,t_i} q_{i,j} + h_{i,j}$. Postupak se može uopštiti za $f_i \geq t_i + 3$. Rezultujući polinom $\tilde{f}$ je stepena t_i po promjenljivoj x_i, a to nam je i bio cilj.

Primijetimo da je polinom $\tilde{f}$ dobijen od polinoma f oduzimajući proizvode oblika $h_i g_i$, gdje $h_i \in F[x_1, ..., x_n]$, odnosno

$$f = \tilde{f} + \sum_{i=0}^{n} h_i g_i. \tag{2.7}$$

Kako je $g_i(x_i) = 0$ za sve $x_i \in S_i$, gdje $i = 1, ..., n$, važi

$$f(x_1, ..., x_n) = \tilde{f}(x_1, ..., x_n),$$

za sve n-torke $(x_1, ..., x_n) \in S_1 \times S_2 \times ... \times S_n$. Po pretpostavci teoreme je $f(s_1, ...s_n) = 0$ za sve $s_i \in S_i$, pa to važi i za polinom $\tilde{f}$.

Dakle, znamo da je polinom $\tilde{f}$ stepena t_i po promjenljivoj x_i i dodatno $|S_i| = t_i + 1$, te možemo primijeniti lemu 2.1. Ona nam daje da je $\tilde{f} \equiv 0$, pa iz 2.7 dobijamo:

$$f = \sum_{i=0}^{n} h_i g_i. \tag{2.8}$$

Dodatno, primijetimo da je za svako i, $(1 \leq i \leq n)$ $\deg(f) \geq \deg(h_i g_i) = \deg(h_i) + \deg(g_i)$. Odavdje dobijamo da stepen polinoma h_i zaista zadovoljava uslove teoreme, čime je dokaz završen. □

Teorema 2.3. *(Kombinatorni „Nullstellensatz" 2) Neka je F proizvoljno polje i neka $f \in F[x_1, ..., x_n]$. Neka je $deg(f) = \sum_{i=1}^{n} t_i$, gdje je t_i nenegativan cijeli broj za sve $1 \leq i \leq n$. Pretpostavimo da je koeficijent uz $\prod_{i=1}^{n} x_i^{t_i}$ u f različit od nule. Tada, ako su $S_i \subset F$ takvi da je za sve i, $|S_i| > t_i$, onda postoje $s_1 \in S_1, s_2 \in S_2, ..., s_n \in S_n$ takvi da je $f(s_1, ..., s_n) \neq 0$.*

Dokaz. Možemo pretpostaviti da je $|S_i| = t_i + 1$, za sve $1 \leq i \leq n$, jer ako su ti skupovi još veće kardinalnosti, tvrđenje će svakako važiti.

Sada pretpostavimo suprotno, da je za sve n-torke $(s_1, ..., s_n) \in S_1 \times S_2 \times ... \times S_n$ ispunjeno $f(s_1, ..., s_n) = 0$. Definišimo ponovo

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

Sada su ispunjeni uslovi teoreme 2.2, pa postoje polinomi $h_1, ..., h_n \in F[x_1, ..., x_n]$, takvi da je $\deg(h_i) \leq \deg(f) - \deg(g_i)$ i da je $f = \sum_{i=1}^{n} h_i g_i$. Po pretpostavci teoreme je koeficijent uz monom $\prod_{i=1}^{n} x_i^{t_i}$ (u polinomu f) različit od nule, pa to mora da važi i za desnu stranu nejednakosti.

Takođe, primijetimo da je $\deg(h_i g_i) = \deg(h_i) + \deg(g_i) \leq \deg(f)$. To znači da ako sa desne strane postoji monom čiji je stepen baš $\deg(f)$, on mora biti oblika $m x_i^{t_i+1}$, gdje je m monom najvećeg stepena u polinomu h_i.

Dakle, svaki term stepena $\deg(f)$ mora biti djeljiv sa $x_i^{t_i+1}$, za neko i. Ali sa lijeve strane imamo monom $\prod_{i=1}^{n} x_i^{t_i}$, čiji je stepen baš $\deg(f)$, a koeficijent uz njega je različit od nule po pretpostavci. Zato on nije djeljiv sa $x_i^{t_i+1}$, za bilo koje i, što je u kontradikciji sa prethodno zaključenim. Time je dokaz teoreme završen. □

Glava 3

Primjene

U nastavku će biti riječi o nekim od mnogobrojnih implementacija ove zanimljive algebarske tehnike. Ona je pronašla svoju primjenu u raznim oblastima, među kojima su teorija grafova, kombinatorna teorija brojeva, kombinatorika, ali i mnoge druge.

Ova glava je posvećena tome da ubijedi znatiželjnog čitaoca u istinsku moć pomenute teoreme, koju možda ne uviđa na prvo čitanje. U tu svrhu pokazaćemo na konkretnim primjerima poznatih rezultata, čiji dokazi su odavno viđeni, kako ti dokazi mogu da se skrate i pojednostave upotrebom našeg glavnog alata, a to je naravno Kombinatorni „Nullstellensatz".

Prvo ćemo predstaviti dvije klasične primjene, kako ih je nazvao sam Alon. To su Chevalley–Warning teorema i Cauchy–Davenport teorema.

3.1 Chevalley–Warning teorema

Chevalley–Warning teoremu je dokazao Ewald Warning (1935), a malo slabiji rezultat poznat kao Chevalley teorema je dokazao Chevalley (1935), dok je postavku teoreme (bez dokaza) dao Artin[1] (1934). Vidjećemo da je Chevalley teorema direktna posljedica Chevalley–Warningove teoreme.

Warning je formulisao i dokazao još jednu teoremu (eng. Warning's Second Theorem) koju ćemo spomenuti na kraju.

Kao što smo već naglasili, prvo ćemo predstaviti klasične dokaze, a potom dokaz pomoću Kombinatornog „Nullstellensatza".

[1]Emil Artin (1898–1962), austrijski matematičar

Za klasičan dokaz su nam potrebne dvije pomoćne leme koje navodimo u nastavku. Naglasimo još da ćemo se zbog jednostavnosti ograničiti na slučaj konačnih polja, mada se priča jednostavno može uopštiti na proizvoljna polja.

Lema 3.1. *([56]) Neka je u cijeli broj takav da je $0 \leq u < p-1$. Tada je*

$$\sum_{x \in \mathbb{Z}_p} x^u = 0.$$

Dokaz. Ako je $u = 0$, onda je $\sum_{x \in Z_p} x^0 = p \cdot 1 = 0$ (jer smo u $\mathbb{Z}_p$). Ako je $0 < u < p-1$, označimo sa a generator ciklične grupe $\mathbb{Z}_p$. Kako je red generatora $p-1$, slijedi da je $a^u \neq 1$. Ali kako x prolazi kroz $\mathbb{Z}_p$ i ax će proći kroz sve elemente, pa je zato

$$\sum_{x \in \mathbb{Z}_p} x^u = \sum_{x \in \mathbb{Z}_p} (ax)^u = a^u \sum_{x \in \mathbb{Z}_p} x^u \tag{3.1}$$

Kako je $a^u \neq 1$, mora biti $\sum_{x \in \mathbb{Z}_p} x^u = 0$. Time je dokaz završen. □

Lema 3.2. *([56]) Neka je $f = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$ i neka je $deg(f) = d < n(p-1)$. Tada je*

$$\sum_{(x_1,...,x_n) \in \mathbb{Z}_p^n} f(x_1, ..., x_n) = 0. \tag{3.2}$$

Dokaz. Zbog linearnosti, možemo posmatrati slučaj $f(x_1, ..., x_n) = x_1^{u_1} \cdot ... \cdot x_n^{u_n}$. Tada je

$$\sum_{(x_1,...,x_n) \in \mathbb{Z}_p^n} f(x_1, ..., x_n) = \prod_{i=1}^{n} \sum_{x_i \in \mathbb{Z}_p} x_i^{u_i}. \tag{3.3}$$

Međutim, kako je $\deg(f) = u_1 + ... + u_n = d < n(p-1)$, slijedi da postoji neko j, $1 \leq j \leq n$, tako da je $u_j < p-1$. Za taj indeks j je po lemi 3.1 ispunjeno

$$\sum_{x_j \in \mathbb{Z}_p} x_j^{u_j} = 0,$$

što nam zajedno sa (3.3) daje

$$\sum_{(x_1,...,x_n) \in \mathbb{Z}_p^n} f(x_1, ..., x_n) = 0,$$

što je i trebalo pokazati. □

Sada imamo sav potreban alat za dokaz Chevalley–Warningove teoreme, koju ponegdje zovu i Warningova prva teorema.

Teorema 3.3. *([56])(Chevalley–Warning teorema) Neka je p prost broj i neka su $P_1 = P_1(x_1, ..., x_n), ..., P_m = P_m(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$. Ako je $n > \sum_{i=1}^{m} deg(P_i) = d$, tada broj N zajedničkih nula polinoma $P_1, ..., P_m$ zadovoljava: $N \equiv 0$ (mod p).*

Dokaz. Definišimo polinom

$$g = g(x_1, ..., x_n) = \prod_{i=1}^{m} \left(1 - P_i(x_1, .., x_n)^{p-1}\right). \tag{3.4}$$

Primijetimo da je tada $\deg(g) = d(p-1) < n(p-1)$, odakle na osnovu leme 3.2 slijedi da je

$$\sum_{(x_1,...,x_n)\in\mathbb{Z}_p^n} g(x_1, ..., g_n) = 0. \tag{3.5}$$

Sa druge strane, za svako $(x_1, ..., x_n) \in \mathbb{Z}_p^n$ je $P_i(x_1, ..., x_n)^{p-1} = 1$, osim ako je $P_i(x_1, ..., x_n) = 0$. Dakle, ako je $(x_1, ..., x_n)$ zajednička nula polinoma $P_1, ..., P_m$, onda je za tu tačku $g(x_1, ..., x_n) = 1$, a inače je $g(x_1, ..., x_n) = 0$. Odatle slijedi da je

$$N = \sum_{(x_1,...,x_n)\in\mathbb{Z}_p^n} g(x_1, ..., g_n) = 0, \tag{3.6}$$

što dalje implicira da je $N \equiv 0 \pmod{p}$, što je i trebalo pokazati. □

Dokazaćemo potom i teoremu Chevalleyja.

Teorema 3.4. *([56])(Chevalley (1935)) Neka je p prost broj i neka je $f = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$ polinom koji nema slobodan član i $deg(f) = d < n$. Tada polinom f ima bar jednu netrivijalnu nulu u $\mathbb{Z}_p^n$.*

Dokaz. Kako f nema slobodan član, jedna nula mu je svakako $(0, ..., 0)$.

Ako sa N označimo broj nula polinoma f, onda je $N \geq 1$. Ali kako je $d < n$, možemo primijeniti teoremu 3.3 koja nam daje da je N djeljivo sa p, odnosno važi $N \geq p$. Tako dobijamo da je broj netrivijalnih nula polinoma f

$$N - 1 \geq p - 1 \geq 1, \tag{3.7}$$

odakle slijedi da je $N \geq 2$, pa f ima bar jednu netrivijalnu nulu, što je i trebalo pokazati. □

Zbog kompletnosti u nastavku navodimo i drugu Warningovu teoremu, kao i jedno pojačanje Chevalley–Warningove teoreme čije dokaze izostavljamo, a znatiželjni čitalac ih može pronaći u [56].

Teorema 3.5. *(Warning (1935)) Pretpostavimo da važe isti uslovi kao u teoremi 3.3 i neka je dodatno $N > 0$. Tada je*

$$N \geq p^{n-d}.$$

Teorema 3.6. *(J. Ax (1964)) Pretpostavimo da važe isti uslovi kao u teoremi 3.3 i neka je dodatno b cijeli broj i $b < n/d$. Tada je*

$$N \equiv 0 \ (mod\, p^b).$$

Konačno, predstavićemo verziju Chavelley–Warning teoreme koju je Alon izložio u svom radu i dokazao koristeći Kombinatorni „Nullstellensatz" tj. teoremu 2.3.

Teorema 3.7. *([3])(Chevalley–Warning teorema) Neka je p prost broj i neka su $P_1 = P_1(x_1, ..., x_n), ..., P_m = P_m(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$. Ako je $n > \sum_{i=1}^{m} deg(P_i)$ i polinomi P_i imaju zajedničku nulu $(c_1, ..., c_n)$, onda imaju bar još jednu zajedničku nulu.*

Dokaz. Pretpostavimo suprotno i definišimo:

$$f = f(x_1, ..., x_n) = \prod_{i=1}^{m} \big(1 - P_i(x_1, ..., x_n)^{p-1}\big) - \delta \prod_{j=1}^{n} \prod_{c \in \mathbb{Z}_p, c \neq c_j} (x_j - c), \quad (3.8)$$

gdje je δ izabrano tako da je $f(c_1, ..., c_n) = 0$. Time je δ određeno i primijetimo da je sigurno različito od nule, jer za $\delta = 0$ važi $f(c_1, ..., c_n) = 1$. Uočimo i da je $f(s_1, ..., s_n) = 0$ za sve $s_i \in \mathbb{Z}_p$. Ovo je svakako ispunjeno za $(s_1, ..., s_n) = (c_1, ..., c_n)$. Za druge vrijednosti $(s_1, ..., s_n)$ postoji neko i, $1 \leq i \leq m$, tako da se P_i ne anulira u toj tački, jer smo pretpostavili da naši polinomi imaju samo jednu zajedničku nulu $(c_1, ..., c_n)$. To dalje implicira da je za to i ispunjeno

$$1 - P_i(s_1, ..., s_n)^{p-1} = 0.$$

Dalje, kako je za bar jedan indeks i ispunjeno $s_i \neq c_i$, imamo da je i $\prod_{c \in \mathbb{Z}_p, c \neq c_i} (s_i - c) = 0$, što sve zajedno daje da je i $f(s_1, ..., s_n) = 0$.

Definišimo sada $t_i = p - 1$ za sve i, gdje $i = 1, ..., n$ i primijetimo da je koeficijent uz $\prod_{i=1}^{n} x_i^{t_i}$ u f baš $-\delta \neq 0$, jer je

$$\deg\Big(\prod_{i=1}^{m} \big(1 - P_i(x_1, ..., x_n)^{p-1}\big)\Big) = (p-1) \sum_{i=1}^{m} \deg(P_i) < n(p-1). \quad (3.9)$$

Uzmimo sada da je $S_i = \mathbb{Z}_p$, za sve $i = 1, ..., n$. Tada na osnovu teoreme 2.3 postoje $s_1, ..., s_n \in \mathbb{Z}_p$ za koje je $f(s_1, ..., s_n) \neq 0$, što je u kontradikciji sa gore zaključenim. Dakle, pretpostavka je bila pogrešna i navedeni polinomi imaju bar još jednu zajedničku nulu. □

3.2 Cauchy–Davenport teorema

Klasična Cauchy–Davenport teorema je jedna od prvih teorema u oblasti teorije aditivnih grupa. Nosi naziv po dva poznata matematičara, Cauchyju, koji ju je prvi dokazao 1813. godine i Davenportu, koji je ponovo došao do istog rezultata 1935. i dao svoj dokaz [23]. Oba dokaza se temelje na istoj kombinatornoj ideji i primjeni indukcije. Danas ova teorema ima mnogobrojne primjene u aditivnoj teoriji brojeva.

Teorema nam daje donju granicu za $|A + B|$, gdje su A i B neprazni podskupovi od $\mathbb{Z}_p$, za p prost broj. Ponovo ćemo predstaviti dva dokaza, klasični i dokaz pomoću teoreme 2.3, redom.

Definicija 3.1. Za proizvoljna dva skupa A i B, $A + B$ definišemo sa:

$$A + B = \{a + b \mid a \in A,\ b \in B\}. \tag{3.10}$$

Teorema 3.8. *([23])(Cauchy–Davenport) Neka je p proizvoljan prost broj, a A i B dva neprazna podskupa od $\mathbb{Z}_p$. Tada je*

$$|A + B| \geq min\{p, |A| + |B| - 1\}. \tag{3.11}$$

Dokaz. ([1],[42]) Dokaz dajemo indukcijom po $|B|$. Ako je $|B| = 1$, onda je

$$|A + B| = |A| = |A| + |B| - 1 \geq \min\{p, |A| + |B| - 1\}, \tag{3.12}$$

čime je baza završena. Sada pretpostavimo da je $|B| = n > 1$ i da tvrđenje važi kada god je skup B manje kardinalnosti od n i pokažimo baš za n.

Primijetimo da kada je $|A| = p$ ili $|B| = p$ tvrđenje trivijalno važi, pa možemo pretpostaviti da je

$$|A| \neq p \ \text{ i } \ |B| \neq p. \tag{3.13}$$

Dalje, uvijek važi $|A+B| \geq |A|$. Prvo pretpostavimo da važi baš jednakost i pretpostavimo da $0 \in B$, jer ako ne pripada, uvijek možemo uzeti najmanji element iz B i oduzeti ga od svih. Tako ćemo dobiti nulu, a kardinalnost skupa B ostaće nepromijenjena. Kako je $0 \in B$, imamo da je $A \subseteq A + B$, jer za svako $a \in A$ važi da $a \in A + B$ (uzmemo $a + 0$).

Onda, kako je $A \subseteq A + B$ i $|A| = |A + B|$, slijedi da je $A = A + B$. To znači da je $b + A = A$, za sve $b \in B$. Sada definišemo skup

$$H = \{h \in \mathbb{Z}_p \mid h + A = A\}.$$

Rutinski se provjerava da je H grupa i da je podgrupa od $\mathbb{Z}_p$. Očigledno je $B \subseteq H$. Kako je $|B| = n \geq 2$, dobijamo da je H netrivijalna grupa.

Sada se pitamo da li može $H = \mathbb{Z}_p$. Pretpostavimo da je tako. Tada bi važilo $h+A = A$ za sve $h \in \mathbb{Z}_p$, pa bi slijedilo $A = H$ i bili bi iste kardinalnosti, odnosno $|A| = p$, što je u kontradikciji sa pretpostavkom (3.13).

Konačno, jedina mogućnost koja preostaje, jeste da je H prava podgrupa od $\mathbb{Z}_p$, ali kako je p prost broj, znamo da takve podgrupe ne postoje.

Dakle, možemo pretpostaviti da je $|A + B| > |A|$. Onda $A + B \not\subseteq A$, pa postoji $a_1 \in A$ tako da $a_1 + B \not\subseteq A$. Definišimo sada skup

$$B_1 = \{b \in B \mid a_1 + b \notin A\}.$$

Tada znamo da je $|B_1| \geq 1$. Definišimo nove skupove

$$\tilde{A} = A \cup (a_1 + B_1) \text{ i } \tilde{B} = B \backslash B_1. \tag{3.14}$$

Pokažimo sada da je $(a_1 + B_1) \cap A = \emptyset$. Pretpostavimo suprotno, postoji neko $x \in A$ tako da $x \in a_1 + B_1$. Onda postoji neko $b_1 \in B_1$ tako da je $x = a_1 + b_1$, ali tada po definiciji skupa B_1 slijedi da $x \notin A$, kontradikcija.

Dakle, zaista dati skupovi imaju neprazan presjek, što zajedno sa (3.14) daje:

$$|\tilde{A}| = |A| + |a_1 + B_1| = |A| + |B_1| \text{ i } |\tilde{B}| = |B| - |B_1|. \tag{3.15}$$

Konačno, pokažimo da je

$$\tilde{A} + \tilde{B} \subseteq A + B. \tag{3.16}$$

Zbog definicije skupa $\tilde{A}$ dovoljno je pokazati da je

$$(a_1 + B_1) + (B \backslash B_1) \subseteq A + B. \tag{3.17}$$

Uzmimo $b_2 \in B_1$ i neko $b_3 \in B \backslash B_1$. Treba pokazati da

$$a_1 + b_2 + b_3 \in A + B.$$

Kako $b_3 \notin B_1$, onda postoji neko $a_2 \in A$ tako da je $a_1 + b_3 = a_2$ (zbog definicije skupa B_1). Tada je

$$a_1 + b_2 + b_3 = a_2 + b_2 \in A + B,$$

čime smo pokazali da važi (3.16). Na osnovu toga sada imamo da je

$$\begin{aligned} |A + B| \geq |\tilde{A} + \tilde{B}| &\geq \min\{p, |\tilde{A}| + |\tilde{B}| - 1\} && (3.18)\\ &= \min\{p, |A| + |B_1| + |B| - |B_1| - 1\} && (3.19)\\ &= \min\{p, |A| + |B| - 1\}, \end{aligned}$$

gdje smo u (3.18) primijenili induktivnu hipotezu, a u (3.19) smo iskoristili (3.15). Time je dokaz završen. □

U nastavku dajemo drugi dokaz teoreme 3.8.

Dokaz. ([3]) Posmatrajmo $|A| + |B|$. Razdvajamo na 2 slučaja:

1. $|A| + |B| > p$:

   Primijetimo da je u ovom slučaju $A \cap B \neq \emptyset$. Neka je c neki proizvoljan element iz $\mathbb{Z}_p$. Tada je $|c - B| = |B|$, pa i skupovi A i $c - B$ imaju neprazan presjek. To znači da postoji element $a \in A$ i postoji $b \in B$ tako da je $a = c - b$. Odatle slijedi da je $c = a + b$, odnosno $c \in A + B$. Kako je c bio neki proizvoljan element, to važi za sve elemente iz skupa $\mathbb{Z}_p$, pa je $\mathbb{Z}_p \subseteq A + B$, a kako obratna inkluzija svakako važi, imamo jednakost. Dakle, dobili smo da je

   $$|A + B| = p \geq \min\{p, |A| + |B| - 1\},$$

   što svakako važi u ovom slučaju, jer nam je pretpostavka da je $|A| + |B| > p$.

2. $|A| + |B| \leq p$:

   Pretpostavimo da tvrđenje nije tačno, odnosno da je

   $$|A + B| < \min\{p, |A| + |B| - 1\}.$$

   Tada kako je

   $$|A| + |B| \leq p < p + 1 \implies |A| + |B| - 1 < p,$$

   te je stoga

   $$\min\{p, |A| + |B| - 1\} = |A| + |B| - 1.$$

   Kada to iskoristimo, imamo da je

   $$|A + B| < |A| + |B| - 1 \implies |A + B| \leq |A| + |B| - 2.$$

   Uzmimo sada skup C koji je podskup $\mathbb{Z}_p$ takav da je $A + B \subseteq C$ i $|C| = |A| + |B| - 2$. Definišimo polinom $f = f(x, y) \in \mathbb{Z}_p[x, y]$ na sljedeći način:

   $$f(x, y) = \prod_{c \in C} (x + y - c). \tag{3.20}$$

   Primijetimo da je

   $$f(a, b) = 0 \tag{3.21}$$

   za sve $a \in A$ i $b \in B$, jer za svaki izbor a i b postoji neko $\tilde{c} \in C$ tako da je $a + b = \tilde{c}$ i baš za to $\tilde{c}$ će vrijednost (3.20) biti jednaka nuli.

Neka su $t_1 = |A| - 1$ i $t_2 = |B| - 1$. Primijetimo da je koeficijent uz $x^{t_1}y^{t_2}$ po binomnoj formuli baš

$$\binom{|A| + |B| - 2}{|A| - 1}.$$

Međutim, kako je $|A| + |B| - 2 < p$, onda p ne dijeli ovaj binomni koeficijent, pa je on u $\mathbb{Z}_p$ različit od nule. Ako izaberemo da je $S_1 = A$ i $S_2 = B$, onda su ispunjeni svi uslovi teoreme 2.3. Iz nje onda slijedi da postoje neki $a_1 \in A$ i $b_1 \in B$ tako da je $f(a_1, b_1) \neq 0$, što je u kontradikciji sa (3.21). Time je dokaz završen.

□

3.3 Restrikovane sume

U ovom odjeljku ćemo nešto reći o restrikovanim sumama i u glavnoj ulozi ćemo imati teoremu koju je Alon dokazao u radu [6], zajedno sa Nathansonom[2] i Ruzsom[3]. Prvo ćemo dati originalni dokaz, a potom ćemo pokazati da je to zapravo samo jedna posljedica naše glavne teoreme 2.3. Predstavićemo još neke rezultate koji su usko vezani za ovu temu, a za više detalja pogledati [6].

Definicija 3.2. Neka je p prost broj. Neka $h = h(x_0, ..., x_k) \in \mathbb{Z}_p[x_0, ..., x_k]$. Za podskupove $A_i \subseteq \mathbb{Z}_p$, $0 \leq i \leq k$, definišemo njihovu restrikovanu sumu u odnosu na polinom h sa:

$$\bigoplus_h \sum_{i=0}^{k} A_i = \{a_0 + a_1 + ... + a_k : a_i \in A_i,\ h(a_0, ..., a_k) \neq 0\}.$$

Ako je $h(x_0, ..., x_k)$ polinom koji za svako $(x_0, ..., x_k)$ ima konstantnu vrijednost, odnosno $h(x_0, ..., x_k) = c$ gdje je c proizvoljna konstanta različita od nule, onda je restrikovana suma zapravo samo $A_0 + ... + A_k$. Takođe lako zaključujemo da je $\left|\bigoplus_h \sum_{i=0}^{k} A_i\right| > 0$ ako i samo ako postoje $a_0 \in A_0, ..., a_k \in A_k$ takvi da je $h(a_0, ..., a_k) \neq 0$.

Sada ćemo formulisati pomenutu teoremu. Zanimljivo je što se u njenom dokazu koristi pomoćna lema 2.1 iz prethodne glave, koja je tada bila već poznat i dokazan rezultat.

[2]Melvyn Bernard Nathanson (1944–), američki matematičar
[3]Imre Z. Ruzsa (1953–), mađarski matematičar

Teorema 3.9. *([6]) Neka je p prost broj. Neka* $h = h(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$ *i neka su* $\emptyset \neq A_i \subseteq \mathbb{Z}_p$, $0 \leq i \leq k$, *gdje je* $|A_i| = c_i + 1$. *Definišimo:*

$$m = \sum_{i=0}^{k} c_i - deg(h).$$

Ako je koeficijent uz monom $\prod_{i=0}^{k} x_i^{c_i}$ *u polinomu* $(x_0 + ... + x_k)^m h(x_1, ..., x_k)$ *različit od nule (u* $\mathbb{Z}_p$*), onda je*

$$\left| \bigoplus_h \sum_{i=0}^{k} A_i \right| \geq m + 1.$$

Dokaz. ([6]) Pretpostavimo da tvrđenje ne važi. Neka je $E \subset \mathbb{Z}_p$ koji ima m ne nužno različitih elemenata i $\bigoplus_h \sum_{i=0}^{k} A_i \subset E$. Definišimo polinom $Q = Q(x_0, ..., x_k)$ na sljedeći način:

$$Q(x_0, ..., x_k) = h(x_0, ..., x_k) \cdot \prod_{e \in E} (x_0 + x_1 + ... + x_k - e).$$

Primijetimo da smo polinom Q zgodno definisali tako da zadovoljava

$$Q(a_0, ..., a_k) = 0 \tag{3.22}$$

za sve

$$(a_0, ..., a_k) \in A_0 \times ... \times A_k.$$

Objasnimo zašto je tako. Naime, ili je $(a_0, ..., a_k)$ baš nula polinoma h pa je $h(a_0, ..., a_k) = 0$, ili je baš tačka u kojoj je h različito od nule. U tom slučaju po definiciji 3.2 imamo $a_0 + ... + a_k \in \bigoplus_h \sum_{i=0}^{k} A_i$. Međutim znamo da je to podskup skupa E, pa postoji neko $e_1 \in E$ tako da je $a_0 + ... + a_k = e_1$. Baš za to e_1 će gornji proizvod, pa samim tim i vrijednost polinoma Q, biti jednaka nuli.

Dalje, primijetimo da je

$$\deg(Q) = \deg(h) + |E| = \deg(h) + m = \sum_{i=0}^{k} c_i.$$

Takođe, lako je uočljivo da polinomi Q i $(x_0 + ... + x_k)^m h(x_0, ..., x_k)$ imaju isti koeficijent uz monom $\prod_{i=0}^{k} x_i^{c_i}$, a taj koeficijent je po pretpostavci teoreme različit od nule. Sada za svako i, $0 \leq i \leq k$, definišimo:

$$g_i(x_i) = \prod_{a \in A_i} (x_i - a) = x_i^{c_i+1} - \sum_{j=0}^{c_i} b_{ij} x_i^j,$$

gdje su b_{ij} odgovarajući koeficijenti. Definišimo sada polinom $\tilde{Q} = \tilde{Q}(x_0, ..., x_k)$ koji se dobija od polinoma Q, tako što se svako javljanje $x_i^{c_i+1}$, zamijeni sa $\sum_{j=0}^{c_i} b_{ij} x_i^j$. Primijetimo da je za sve $x_i \in A_i$, $g(x_i) = 0$, odnosno važi jednakost:

$$x_i^{c_i+1} = \sum_{j=0}^{c_i} b_{ij} x_i^j.$$

To znači da je za sve $(x_0, ..., x_k) \in A_0 \times ... \times A_k$, ispunjeno

$$\tilde{Q}(x_0, ..., x_k) = Q(x_0, ..., x_k),$$

što znači da (3.22) važi i za $\tilde{Q}$. Zbog načina na koji smo definisali polinom $\tilde{Q}$, najveći stepen x_i u $\tilde{Q}$ je c_i. Sada su ispunjeni uslovi leme 2.1, i kada je primijenimo, dobijemo da je $\tilde{Q} \equiv 0$.

Da bismo došli do kontradikcije sa ovom činjenicom, pokazaćemo da polinom $\tilde{Q}$ ima koeficijent različit od nule i to baš onaj koji stoji uz monom $\prod_{i=0}^{k} x_i^{c_i}$. Razlog je taj što zapravo Q i $\tilde{Q}$ imaju isti koeficijent uz taj monom, jer opisani proces dobijanja polinoma $\tilde{Q}$ ne utiče na koeficijent pomenutog monoma. Takođe, ovaj monom se ne može javiti uz neki novi koeficijent u procesu dobijanja $\tilde{Q}$, zato što sam proces smanjuje stepen polinoma, a stepen polaznog polinoma Q je bio $\sum_{i=0}^{k} c_i$.

Time smo dobili da je $\tilde{Q} \neq 0$, čime smo došli u kontradikciju sa gore zaključenim i završili dokaz.

□

Pažljivi čitalac je možda već primijetio da se u dokazu ove teoreme javljaju neke ideje koje se koriste i u dokazu Kombinatornog „Nullstellensatza", odnosno teoreme 2.2. To je sigurno jedan od razloga zašto se ova teorema može dobiti kao direktna posljedica teoreme 2.2. Postavke dokaza su iste, ali se do zaključka dolazi na jednostavniji način.

Dokaz. ([3]) Pretpostavimo da tvrđenje ne važi. Neka je $E \subset \mathbb{Z}_p$ koji ima m ne nužno različitih elemenata i $\bigoplus_h \sum_{i=0}^{k} A_i \subset E$. Definišimo polinom $Q = Q(x_0, ..., x_k)$ kao i u teoremi 3.9:

$$Q(x_0, ..., x_k) = h(x_0, ..., x_k) \cdot \prod_{e \in E} (x_0 + x_1 + ... + x_k - e).$$

Ponovo važi

$$Q(a_0, ..., a_k) = 0 \tag{3.23}$$

za sve

$$(a_0, ..., a_k) \in A_0 \times ... \times A_k,$$

iz istih razloga koji su već obrazloženi.

Ponovo, primijetimo da je $\deg(Q) = m + \deg(h) = \sum_{i=0}^{k} c_i$ i da je koeficijent uz monom $\prod_{i=0}^{k} x_i^{c_i}$ u polinomu Q isti kao u polinomu

$$(x_0 + ... + x_k)^m h(x_0, ..., x_k),$$

a on je po pretpostavci različit od nule.

Sada direktno iz teoreme 2.3 slijedi da postoje $x_0 \in A_0, ..., x_k \in A_k$ takvi da je $Q(x_0, ..., x_k) \neq 0$, što je u kontradikciji sa (3.23). Time je dokaz završen. □

Teorema 3.9 je vrlo značajan rezultat, jer iz nje slijede mnogobrojne teoreme i posljedice. Ovdje ćemo navesti samo neke od njih. Za početak pokazaćemo kako se teorema Cauchy–Davenport 3.8 dobija kao neposredna posljedica teoreme 3.9.

Dokaz. Kao u jednom od prethodnih dokaza ove teoreme, razdvojićemo prvo na dva slučaja:

1. $|A| + |B| \leq p + 1$:
   Pretpostavimo da je polinom $h \equiv 1$ i neka su skupovi $A_0 = A$ i $A_1 = B$, gdje $|A| = c_0 + 1$ i $|B| = c_1 + 1$. Tada m iz teoreme 3.9 ima sljedeću vrijednost:

   $$m = \sum_{i=0}^{1} c_i - \deg(h) = |A| - 1 + |B| - 1 + 0 = |A| + |B| - 2.$$

   Dalje, primijetimo da je koeficijent uz monom $\prod_{i=0}^{1} x_i^{c_i}$ u polinomu $(x_0 + x_1)^m \cdot 1$ zapravo

   $$\binom{m}{c_0} \neq 0 \quad (\text{u } \mathbb{Z}_p),$$

   jer je $m < p$ pa p ne dijeli pomenuti koeficijent.

   Zapazimo još da je restrikovana suma u ovom slučaju samo $A + B$, jer je h konstantan polinom. Sada možemo jednostavno da primijenimo teoremu 3.9:

   $$\left| \bigoplus_{h} \sum_{i=0}^{1} A_i \right| = |A + B| \geq m + 1 = |A| + |B| - 1.$$

2. $|A| + |B| > p + 1$:
   Posmatrajmo $B' \subset B$, koji je takav da $|B'| = p + 1 - |A|$. Opet, neka je $h \equiv 1$, $|A| = c_0 + 1$ i $p + 1 - |A| = |B'| = c_1 + 1$, odakle slijedi da je $c_1 = p - |A|$. Tada m iz teoreme 3.9 ima vrijednost:

$$m = \sum_{i=0}^{1} c_i - \deg(h) = c_0 + c_1 = |A| - 1 + p - |A| = p - 1.$$

   Sada je jasno da je

$$\binom{m}{c_0} = \binom{p-1}{c_0} \neq 0,$$

   pa ponovo možemo primijeniti teoremu 3.9 sada na A i B':

$$|A + B| \geq |A + B'| \geq m + 1 = p - 1 + 1 = p.$$

   Koristili smo da je $B' \subset B$ i običnu sumu skupova, jer je polinom h konstantan.

□

Jedna od primjena teoreme 3.9 je i sljedeća propozicija, koju ovdje navodimo bez dokaza. Svi detalji dokaza se mogu pronaći u [6].

Propozicija 3.10. *Neka je p prost broj i neka su $\emptyset \neq A_i \subset \mathbb{Z}_p$, za sve $0 \leq i \leq k$. Ako su svi podskupovi različite kardinalnosti i*

$$\sum_{i=0}^{k} |A_i| \leq p + \binom{k+2}{2} - 1,$$

onda je

$$|\{a_0 + ... + a_k : a_i \in A_i, a_i \neq a_j, i \neq j\}| \geq \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

Ova propozicija je zanimljiva zato što u jednom specijalnom slučaju dokazuje teoremu koja je usko vezana za Cauchy–Davenport teoremu.

Naime, sedamdesetih godina prošlog vijeka, Erdős i Heilbronn postavili su hipotezu koja tvrdi da, ako se u Cauchy–Davenport teoremi dodatno ograničimo na sume međusobno različitih elemenata, donja granica će se malo promijeniti. Erdős je prvi iznio ovu hipotezu, dok je držao konferenciju u Koloradu 1963, a kasnije se spominje u njegovim radovima tek 1971. [28] i u knjizi „Erdős and Graham" [29] iz 1980.

Teorema 3.11. *(Erdős–Heilbronn) Neka je p prost broj i neka su $\emptyset \neq A, B \subset \mathbb{Z}_p$. Tada je*

$$|\{a+b : a \in A, b \in B, a \neq b\}| \geq \min\{p, |A| + |B| - 3\}.$$

Prvi dokaz ove teoreme su dali Dias Da Silva[4] i Hamidoune[5] [25] (1994), koji se temelji na linearnoj algebri i teoriji reprezentacije simetričnih grupa i to za specijalan slučaj kada je $A = B$. Mi ćemo ovdje dati skicu dokaza koji slijedi direktno is propozicije 3.10.

Pretpostavimo da je $k = 1$ i neka su $A_0 = A$ i $A_1 = A\backslash\{a\}$, za neki proizvoljni element $a \in A$. Ako je $A \subset \mathbb{Z}_p$ takav da je $2|A| - 1 \leq p + 2$, onda direktno iz propozicije 3.10 dobijamo da je

$$|\{a + a' : a, a' \in A, a \neq a'\}| \geq 2|A| - 3.$$

Time smo za odgovarajući izbor skupova dobili dokaz teoreme 3.11 direktno iz propozicije 3.10, ali ponovo za specijalni slučaj $A = B$.

Sljedeća propozicija je još jedna jednostavna posljedica teoreme 3.9. To je rezultat koji je formulisao i dokazao Alon sa koautorima prvi put u [7], gdje se može pronaći i detaljan dokaz.

Propozicija 3.12. *Neka je p prost broj i neka su $\emptyset \neq A, B \subset \mathbb{Z}_p$. Tada je*

$$|\{a+b : a \in A, b \in B, ab \neq 1\}| \geq \min\{p, |A| + |B| - 3\}.$$

Dokaz dobijamo primjenom teoreme 3.9 na $k = 1$, $A_0 = A$, $A_1 = B$ i $m = |A| + |B| - 4$. Polinom koji će riješiti problem je $h = x_0x_1 - 1$.

3.4 EGZ teorema

Teorija nula-suma (eng. Zero-sum theory) je relativno nova disciplina, koja se smatra granom kombinatorike, a kombinuje alate iz raznih oblasti, kao što su teorija brojeva, teorija grafova, algebra i linearna algebra, diskretna analiza i druge.

Ova oblast se bavi proučavanjem sljedećeg tipa problema, koji opravdava naziv nula-sume. Neka je data neka algebarska struktura (najčešće Abelova

[4]J. A. Dias Da Silva, portugalski matematičar

[5]Yahya Ould Hamidoune (1947–2011), afrički matematičar

grupa) i pozitivan cijeli broj n. Traži se najmanja vrijednost k takva da svaki niz od tačno k elemenata date strukture sadrži n elemenata koji u zbiru daju nulu.

Klasičan rezultat iz ove oblasti je EGZ teorema, koja nosi naziv po tri naučnika koja su je dokazala, a to su Erdős, Ginzburg[6] i Ziv[7]. Prvi put ju je formulisao Erdős 1956. u svom radu [30], a do dokaza [31] je došao zajedno sa navedenim autorima 1961.

Danas je poznato više dokaza ove teoreme, a u radu [8] se može pronaći čak pet različitih. U tim dokazima se koriste neki od alata koje smo pomenuli u ovom radu, a to su teorema Cauchy–Davenport 3.8 i Chevalley–Warning teorema 3.3, ali i neki dobro poznati rezultati poput Male Fermaove teoreme.

Teorema 3.13. *(EGZ teorema) Neka je $a_1, a_2, ..., a_{2n-1}$ niz elemenata ciklične grupe $\mathbb{Z}_n$, koji nisu nužno međusobno različiti. Tada postoji indeksni skup $I \subset \{1, 2, ..., 2n-1\}$, $|I| = n$, tako da je*

$$\sum_{i \in I} a_i = 0 \ (\ u\ \mathbb{Z}_n).$$

Mi ćemo zapravo dati dokaz prividno malo slabijeg rezultata, tj. dokazaćemo gornju teoremu za $n = p$, gdje je p neki prost broj.

Propozicija 3.14. *Neka je p prost broj i neka je $a_1, a_2, ..., a_{2p-1}$ niz elemenata ciklične grupe $\mathbb{Z}_p$, koji nisu nužno međusobno različiti. Tada postoji indeksni skup $I \subset \{1, 2, ..., 2p-1\}$, $|I| = p$, tako da je*

$$\sum_{i \in I} a_i = 0 \ (\ u\ \mathbb{Z}_p).$$

Dokažimo prvo da je ovo tvrđenje dovoljno, tj. da iz njega slijedi dokaz teoreme 3.13.

Propozicija 3.15. *Ako EGZ teorema važi za svaki prost broj p, onda važi i za svako $n \in \mathbb{N}$.*

Dokaz. Pretpostavimo da EGZ teorema važi za svaki prost p, odnosno pretpostavimo da je tvrđenje 3.14 tačno. Dokažimo da onda važi i za proizvoljno n. Dokaz dajemo indukcijom po n.

[6] Abraham Ginzburg (1926–2020), izraelski matematičar
[7] Abraham Ziv (1940–2013), izraelski matematičar

Za $n = 1$ tvrđenje trivijalno važi, pa zato pretpostavimo da je $n > 1$ i da tvrđenje važi za sve prirodne brojeve manje od n. Pokažimo za n.

Neka je $n = kp$, gdje je p prost, i posmatramo niz $a_1, ..., a_{2n-1}$. Tada na osnovu propozicije 3.14 znamo da, kada god imamo niz od $2p-1$ elemenata, možemo da odaberemo p tako da im je suma 0 (u $\mathbb{Z}_p$). Zato možemo da izaberemo disjunktne skupove $I_1, ..., I_{2k-1} \subset \{1, 2, ..., 2n-1\}$ koji svi imaju po p elemenata i $\sum_{i \in Ij} a_i = 0$ (u $\mathbb{Z}_p$). Znamo da možemo naći $2k-1$ takvih indeksnih skupova, jer ako smo ih našli $r < 2k-1$, onda nam ostaje niz dužine

$$2kp - 1 - rp \geq 2kp - 1 - (2k-2)p = 2p - 1,$$

pa među tih preostalih $2p-1$ članova niza možemo opet pronaći još jedan indeksni skup sa p elemenata koji ispunjava gore opisano.

Definišimo sada niz $b_1, ..., b_{2k-1}$ na sljedeći način:

$$b_i = \sum_{j \in I_i} a_j/p.$$

Kako je $k < n$, možemo primijeniti indukcijsku hipotezu. Dakle, postoji neki podskup od k elemenata, čija suma je 0 (u $\mathbb{Z}_k$). Tada unija odgovarajućih k indeksnih skupova I_i, jeste skup koji ima $kp = n$ elemenata, a suma n elemenata sa tim odgovarajućim indeksima će biti 0 (u $\mathbb{Z}_n$). Time je dokaz završen.

□

Dakle, dovoljno je dokazati propoziciju 3.14, jer kao što smo upravo vidjeli, iz nje slijedi EGZ teorema. Stoga, u nastavku dajemo razne dokaze pomenute propozicije.

3.4.1 Prvi dokaz

Prvo ćemo predstaviti originalni dokaz, u kome glavnu ulogu igra Cauchy–Davenport teorema 3.8.

Dokaz. ([31]) Neka je dat niz $a_1, ..., a_{2p-1}$ elemenata ciklične grupe $\mathbb{Z}_p$. Prvo preimenujmo elemente niza da budu u neopadajućem redoslijedu tj. tako da je $a_1 \leq a_2 \leq ... \leq a_{2p-1}$. Tada, ako za neko i, gdje $1 \leq i \leq p-1$, važi $a_i = a_{i+p-1}$, onda je

$$a_i + a_{i+1} + ... + a_{i+p-1} = pa_i = 0 \ \ (\text{u } \mathbb{Z}_p).$$

Zato pretpostavimo da je $a_i \neq a_{i+p-1}$, za sve i, gdje $1 \leq i \leq p-1$. Definišimo skupove $A_i = \{a_i, a_{i+p-1}\}$ za $1 \leq i \leq p-1$.

Pokažimo da važi jednakost

$$|A_1 + A_2 + ... + A_{p-1}| = p.$$

Dokaz dajemo indukcijom po p. Za $p = 2$ imamo $|A_1| = 2$, pa važi. Pretpostavimo da tvrđenje važi za $p-1$ i dokažimo za p. Kada Cauchy–Davenport teoremu primijenimo na skupove $A_1+A_2+...+A_{p-2}$ i A_{p-1}, dobijemo sljedeće:

$$|A_1 + A_2 + ... + A_{p-1}| \geq \min\{p, |A_1 + A_2 + ... + A_{p-2}| + |A_{p-1}| - 1\}. \quad (3.24)$$

Kako je po indukcijskoj pretpostavci $|A_1 + A_2 + ... + A_{p-2}| = p - 1$, imamo da je

$$|A_1 + A_2 + ... + A_{p-2}| + |A_{p-1}| - 1 = p - 1 + 2 - 1 = p.$$

Odatle dobijamo da je $|A_1 + A_2 + ... + A_{p-1}| \geq p$, a kako su $A_i \subset \mathbb{Z}_p$, važi i obratna nejednakost, odnosno imamo da je

$$|A_1 + A_2 + ... + A_{p-1}| = p \implies A_1 + A_2 + ... + A_{p-1} = \mathbb{Z}_p.$$

Time smo dobili da se svaki element iz $\mathbb{Z}_p$ može predstaviti kao zbir $p - 1$ elemenata našeg niza, ali tačno među prva $2p-2$ člana našeg niza (iz svakog skupa A_i uzmemo po jednog).

Dalje, kako je $-a_{2p-1} \in \mathbb{Z}_p$, i on se može predstaviti na taj način, tj. kao zbir nekih $p - 1$ elemenata našeg niza. Kada ga prebacimo sa druge strane, dobićemo p elemenata niza dužine $2p - 1$ čiji zbir je nula (u $\mathbb{Z}_p$). Time je dokaz završen. □

3.4.2 Drugi dokaz

U sljedećem dokazu propozicije 3.14 koristićemo Chevalley–Warning teoremu 3.3. Koristićemo i Malu Fermaovu teoremu, koje ćemo se prvo podsjetiti u nastavku.

Teorema 3.16. *(Mala Fermaova teorema) Neka je p prost broj i $a \in \mathbb{Z}$ takav da a nije djeljivo sa p. Tada je*

$$a^{p-1} \equiv 1 \,(mod\, p).$$

Dakle, za sve cijele brojeve a je $a^p \equiv a \,(mod\, p)$.

Sada smo spremni za dokaz propozicije.

Dokaz. ([8]) Neka je dat niz $a_1, ..., a_{2p-1}$ elemenata ciklične grupe $\mathbb{Z}_p$. Definišimo polinome $f, g \in \mathbb{Z}_p[x_1, ..., x_{2p-1}]$ na sljedeći način:

$$f(x_1, ..., x_{2p-1}) = a_1 x_1^{p-1} + a_2 x_2^{p-1} + ... + a_{2p-1} x_{2p-1}^{p-1},$$

$$g(x_1, ..., x_{2p-1}) = x_1^{p-1} + x_2^{p-1} + ... + x_{2p-1}^{p-1}.$$

Posmatrajmo sistem

$$f(x_1, ..., x_{2p-1}) = 0,$$

$$g(x_1, ..., x_{2p-1}) = 0.$$

Tada je $\deg(f) = p - 1$ i $\deg(g) = p - 1$.

Dakle, kako je $\deg(f) + \deg(g) = 2p - 2 < 2p - 1$ i sistem ima trivijalno rješenje $x_1 = x_2 = ... = x_{2p-1} = 0$, tada na osnovu teoreme 3.7 slijedi da sistem ima još jedno rješenje. Označimo ga sa $(x_1', ..., x_{2p-1}')$. Kako to rješenje nije trivijalno, postoji bar jedno $i, 1 \leq i \leq 2p - 1$, tako da je $x_i' \neq 0$.

Sada kada primijenimo teoremu 3.16 u $\mathbb{Z}_p$, imamo da je $(x_i')^{p-1} = 1$, osim ako je $x_i' = 0$ (tada trivijalno $0^{p-1} = 0$). Označimo sa $I = \{i : x_i' \neq 0\}$. Tada, kako je $(x_1', ..., x_{2p-1}')$ nula polinoma g, slijedi da je

$$(x_1')^{p-1} + (x_2')^{p-1} + ... + (x_{2p-1}')^{p-1} = 0 \quad (\text{u } \mathbb{Z}_p).$$

Sada, kako imamo ukupno $2p - 1$ sabiraka sa lijeve strane i svaki od njih je 0 ili 1, a bar jedan je jednak 1, slijedi da mora biti tačno p sabiraka jednakih 1, da bismo sa desne strane dobili 0 u $\mathbb{Z}_p$. Stoga je $|I| = p$ i $\sum_{i \in I} a_i = 0$ (gdje su a_i odgovarajući koeficijenti polinoma f). Time je dokaz završen. □

3.4.3 Treći dokaz

Sljedeći dokaz propozicije 3.14 je pronašlo više naučnika nezavisno jedni od drugih (pogledati [52], [16], [63]).

Dokaz. ([8]) Neka je dat niz $a_1, ..., a_{2p-1}$ elemenata ciklične grupe $\mathbb{Z}_p$. Posmatrajmo sljedeću sumu:

$$S = \sum_{I \subset J, |I| = p} \left(\sum_{i \in I} a_i \right)^{p-1},$$

gdje je $J = \{1, 2, ..., 2p-1\}$. Primijetimo da sumu S možemo posmatrati kao polinom po $a_1, ..., a_{2p-1}$, sa koeficijentima iz $\mathbb{Z}$. Taj polinom je suma monoma oblika

$$c \prod_{i \in I} a_i^{k_i},$$

gdje mora važiti $\sum_{i\in I} k_i = p-1$, a c je odgovarajući koeficijent.

U svakom opisanom monomu bar jedan od k_i mora biti različit od nule, pa je broj pozitivnih k_i neka vrijednost j, tako da $1 \leq j \leq p-1$. Hajde da prebrojimo koliko skupova I doprinosi vrijednosti tog koeficijenta c.

Dakle, skup I ima p elemenata, a njih j je već određeno. Pitamo se na koliko načina možemo izabrati preostalih $p-j$. Odgovor je

$$\binom{2p-1-j}{p-j}.$$

Kako je $2p-1-j \geq 2p-1-(p-1) = p$, slijedi da p dijeli ovaj binomni koeficijent, odnosno

$$\binom{2p-1-j}{p-j} \equiv 0 \pmod{p}.$$

Kako svaki takav skup I doprinosi jednako koeficijentu c (za svako opisano I u c će se dodati 1), dobijamo da je i $S \equiv 0 \pmod{p}$.

Pokažimo sada da je za neki indeksni skup $I \subset J$, $|I| = p$, ispunjeno

$$\sum_{i\in I} a_i = 0.$$

Pretpostavimo suprotno, tj. da je za svako I ova suma različita od nule. Tada je na osnovu Male Fermaove teoreme važi $\left(\sum_{i\in I} a_i\right)^{p-1} = 1$ za svaki $I \subset \mathbb{Z}_p$, $|I| = p$.

Tada, kako takvih podskupova I ima tačno $\binom{2p-1}{p}$, važi da je

$$S \equiv \binom{2p-1}{p} \cdot 1 \equiv 1 \pmod{p}.$$

Time smo došli u kontradikciju sa $S \equiv 0 \pmod{p}$ i zaključujemo da nam pretpostavka nije bila dobra. Odnosno, mora da postoji p-podskup skupa J tako da je zbir njegovih elemenata 0 u $\mathbb{Z}_p$. Time je dokaz završen.

□

Napomena 3.17. Na kraju prethodnog dokaza korišćena je poznata kongruencija

$$\binom{2p-1}{p} \equiv 1 \pmod{p}$$

koja se može pokazati pomoću sljedeće teoreme.

Teorema 3.18. *(Lucas[8] (1878)) Za nenegativne brojeve m i n i prost broj p važi*

$$\binom{m}{n} = \prod_{i=0}^{k} \binom{m_i}{n_i},$$

gdje je

$$m = m_k p_k + m_{k-1} p^{k-1} + ... + m_0 p^0$$

i

$$n = n_k p^k + n_{k-1} p^{k-1} + ... + n_0 p^0.$$

3.4.4 Četvrti dokaz

U nastavku ćemo izložiti i četvrti dokaz, ali prije toga definišemo potrebne pojmove. Prvo uvodimo pojam Davenportove konstante, koju je prvi put definisao Davenport ([24]) 1966, mada je i ranije izučavana ([54]) 1963.

Definicija 3.3. Neka je G konačna Abelova grupa. Davenportova konstanta, u oznaci $s = s(G)$, je najmanji prirodan broj takav da za svaki niz dužine s, ne nužno različitih elemenata, postoji neki neprazan podniz čiji je zbir nula. Odnosno, za proizvoljan niz $x_1, ..., x_s$, postoji $\emptyset \neq I \subset \{1, 2, ..., s\}$, tako da je

$$\sum_{i \in I} x_i = 0.$$

Dakle, glavno pitanje je kako za proizvoljnu Abelovu grupu pronaći vrijednost Davenportove konstante. Da bismo što bolje objasnili ovaj pojam, dajemo jedan jednostavan i reprezentativan primjer.

Primjer 3.19. Odrediti Davenportovu konstantu ciklične grupe $G = \mathbb{Z}/n\mathbb{Z}$.

Prije svega, napomenimo da ova grupa jeste Abelova. Označimo sa a generator ciklične grupe i uzmimo niz koji se sastoji od $n-1$ kopije ovog generatora. Tada nijedan podniz tog niza ne daje u zbiru nulu. Zato je $s(G) \geq n$.

Pokažimo da je $s(G) = n$. U tu svrhu, uzmimo proizvoljan niz $z_1, ..., z_n$ u G. Tada posmatrajmo niz suma $\sum_{i=1}^{k} z_i$, gdje k ide od 1 do $n+1$. Tada su neka dva člana tog niza ista (jer posmatrana grupa ima n elemenata). Onda, ako napravimo razliku te dvije sume, dobićemo niz u G čiji zbir elemenata daje nulu. Time smo pokazali da je $s(G) = n$.

[8] Édouard Lucas (1842–1891), francuski matematičar

Postoji mnogo zanimljivih problema u vezi sa ovom konstantom, a neki od njih mogu se pronaći u [15], [27] itd.

Potom uvodimo pojam prstena grupe.

Definicija 3.4. Neka je R prsten i neka je $G = \{g_1, ..., g_n\}$ konačna multiplikativna grupa. Tada je prsten grupe (eng. group ring) G sa koeficijentima iz R skup svih suma oblika

$$R[G] = \{a_1g_1 + a_2g_2 + ... + a_ng_n \ : a_i \in R,\ 1 \leq i \leq n\}.$$

Može se pokazati da je $R[G]$ također prsten. Važi i sljedeća teorema.

Teorema 3.20. *Neka je G grupa i neka je R prsten. Tada je $R[G]$ komutativan prsten ako i samo ako je G Abelova grupa.*

Dokaz ovog tvrđenja, kao i mnoge druge osobine prstena grupe, ali i zanimljivi primjeri, mogu se pronaći u [64].

Sada ćemo dokazati teoremu koju je Olson[9] dokazao 1969. a čiji specijalan slučaj će dati i dokaz naše propozicije 3.14.

Definicija 3.5. Za prost broj p, grupa G je p-grupa ako za svaki njen element $g \in G$, gdje $g \neq 1$, važi da postoji $n \geq 1$ tako da je red elementa g jednak p^n.

Teorema 3.21. *([48]) Neka je G konačna Abelova p-grupa sa invarijantama $p^{e_1}, p^{e_2}, ..., p^{e_r}$, odnosno*

$$G = \mathbb{Z}_{p^{e_1}} \oplus \mathbb{Z}_{p^{e_2}} \oplus ... \oplus \mathbb{Z}_{p^{e_r}}.$$

Tada je Davenportova konstanta grupe G data sa

$$s(G) = 1 + \sum_{i=1}^{r} (p^{e_i} - 1).$$

Dokaz. Prvo ćemo pokazati da je

$$s(G) \geq 1 + \sum_{i=1}^{r} (p^{e_i} - 1).$$

Dovoljno je da nađemo niz dužine $\sum_{i=1}^{r}(p^{e_i} - 1)$ koji nema podniz čija suma elemenata daje nulu. Neka $x_1, x_2, ..., x_r$ čine bazu grupe G, i neka je red elementa x_i baš p^{e_i}. Posmatrajmo sada niz u kome se x_1 javlja $p^{e_1} - 1$ puta,

[9] John E. Olson, američki matematičar

x_2 se javlja $p^{e_2} - 1$ puta i tako redom. Taj niz će biti dužine $\sum_{i=1}^{r}(p^{e_i} - 1)$, a nema podniz čija je suma nula. Time smo dokazali što je i trebalo.

Sada treba pokazati i obratnu nejednakost. Označimo sa R prsten grupe G nad $\mathbb{Z}_p$, pri čemu ćemo koristiti multiplikativnu notaciju za grupu G. Neka je sada $g_1, ..., g_s$ neki proizvoljan niz u G. Tvrdimo da je u R

$$(1 - g_1)(1 - g_2) \cdot ... \cdot (1 - g_s) = 0. \tag{3.25}$$

Neka je g_i neki proizvoljni element grupe G. Tada ga možemo predstaviti kao proizvod baznih, odnosno x_i. Primijetimo da važi jednostavan identitet $1 - uv = (1 - u) + u(1 - v)$. Primijenimo sada taj identitet na naše g_i koje smo zapisali kao proizvod baznih i dobićemo da se $1 - g_i$ može napisati kao linearna kombinacija elemenata $1 - x_i$, sa koeficijentima iz R.

Takođe, na osnovu teoreme 3.20 imamo da je R komutativan prsten, jer je grupa G Abelova. Tako da kada u (3.25) umjesto $1 - g_i$ ubacimo gore opisano, dobićemo sa lijeve strane linearnu kombinaciju terma oblika

$$\prod_{i=1}^{r}(1 - x_i)^{s_i},$$

gdje je $\sum_{i=1}^{r} s_i = s > \sum_{i=1}^{r}(p^{e_i} - 1)$. To znači da je za bar jedno i, $1 \leq i \leq r$, ispunjeno $s_i \geq p^{e_i}$. Kako je u R ispunjeno $(1 - x_i)^{p^{e_i}} = 1 - x_i^{p^{e_i}} = 0$, iz čega slijedi da važi (3.25).

Sada jednakost (3.25) možemo da interpretiramo tako da mora da postoji podniz niza $g_1, ..., g_s$ čiji je proizvod 1. Međutim, baš to je i trebalo da pokažemo s obzirom na to da smo rekli da u G imamo multiplikativnu operaciju, pa onda Davenportovu konstantu interpretiramo kao najmanji prirodan broj s takav da svaki niz dužine s ima podniz čiji je proizvod 1. □

Sada smo spremni za dokaz propozicije 3.14.

Dokaz. Primijenimo prethodnu teoremu na $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Dobijemo da je

$$s(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 1 + 2(p - 1) = 2p - 1.$$

To znači da svaki niz dužine $2p - 1$ grupe G ima neki neprazan podniz čija suma elemenata daje nulu.

Neka su $a_1, a_2, ..., a_{2p-1} \in \mathbb{Z}_p$. Tada posmatrajući sljedeći niz u G :

$$(a_1, 1),\ (a_2, 1), ..., (a_{2p-1}, 1),$$

dolazimo do željenog rješenja. □

U nastavku ćemo preformulisati teoremu 3.21 u ekvivalentno tvrđenje, ali izraženo na malo drugačiji način, jer će nam u jednom od narednih odjeljaka biti potrebno baš u tom obliku.

Teorema 3.22. *([9]) Neka je p prost i pretpostavimo da je $d_1 \geq d_2 \geq ... \geq d_n \geq 0$. Neka je $a^{(i)} = (a_1^{(i)}, a_2^{(i)}, ..., a_n^{(i)})$ vektor čije koordinate su iz $\mathbb{Z}$, za $1 \leq i \leq m$. Ako je*

$$m > \sum_{j=1}^{n} (p^{d_j} - 1),$$

onda postoji neki neprazan indeksni skup $I \subset \{1, 2, ..., m\}$ takav da je

$$\sum_{i \in I} a_j^{(i)} \equiv 0 \, (mod \, p^{d_j}), \; za \; j = 1, 2, ..., n.$$

Zanimljivo je što u specijalnom slučaju $d_1 = d_2 = ... = d_n = 1$, ovo tvrđenje slijedi direktno iz Chevalley–Warningove teoreme 3.3. Pokažimo to u nekoliko redova.

Posmatrajmo sljedeći sistem jednačina u $\mathbb{Z}_p$:

$$\sum_{i=1}^{m} a_j^{(i)} x_i^{p-1} = 0, \;\; j = 1, 2, ..., n.$$

Nula vektor je jedno rješenje ovog sistema. Dalje, kako je stepen svakog polinoma $p-1$, a ukupno ih ima n, slijedi da je zbir svih $n(p-1) < m$, po uslovu zadatka. Sada su zadovoljeni uslovi Chevalley–Warning teoreme 3.3, iz koje onda slijedi da ovaj sistem ima i netrivijalno rješenje $x = (x_1, ..., x_m)$. Kako je netrivijalno, bar jedno $x_i \neq 0$, a kako smo u $\mathbb{Z}_p$, iz male Fermaove teoreme 3.16 je onda $x_i^{p-1} = 1$ (u $\mathbb{Z}_p$). Označimo sa $I \subset \{1, 2, ..., m\}$ indeksni skup u kome su svi indeksi za koje je $x_i \neq 0$. Za taj indeksni skup su zadovoljeni uslovi teoreme.

Navešćemo i jednu posljedicu ove teoreme, koja će nam kasnije zatrebati.

Posljedica 3.23. *([9]) Pretpostavimo da je $d_1 \geq d_2 \geq ... \geq d_n \geq 1$ i neka su p i vektor $a^{(i)}$ kao u 3.22. Ako je*

$$\sum_{j=1}^{n} a_j^{(i)} \equiv 0 \, (mod \, p) \;\; za \; i = 1, ..., m$$

i ako je

$$m > p^{d_n-1} - 1 + \sum_{j=1}^{n-1}(p^{d_j} - 1),$$

onda važi teorema 3.22.

Dokaz. Definišimo vektor $b^{(i)} = (b_1^{(i)}, ..., b_n^{(i)})$ na sljedeći način:

$$b_j^{(i)} = a_j^{(i)}, \text{ za } j = 1, ..., n-1 \text{ i } b_n^{(i)} = \frac{1}{p}\sum_{j=1}^{n} a_j^{(i)}, \text{ za } i = 1, ..., m.$$

Tada, ako teoremu 3.22 primijenimo na prethodno definisan vektor $b^{(i)}$, slijedi da postoji $\emptyset \neq I \subset \{1, ..., m\}$ tako da je

$$\sum_{i\in I} a_j^{(i)} = \sum_{i\in I} b_j^{(i)} \equiv 0 \pmod{p^{d_j}} \text{ za } 1 \leq j \leq n-1, \text{ i}$$

$$\frac{1}{p}\sum_{i\in I}\left(\sum_{j=1}^{n} a_j^{(i)}\right) = \sum_{i\in I} b_n^{(i)} \equiv 0 \pmod{p^{d_n-1}}.$$

Odatle slijedi da je

$$\sum_{i\in I}\left(\sum_{j=1}^{n} a_j^{(i)}\right) \equiv 0 \pmod{p^{d_n}},$$

a kako je $d_1 \geq d_2 \geq ... \geq d_n$ slijedi da je

$$\sum_{i\in I} a_j^{(i)} \equiv 0 \pmod{p^{d_j}} \text{ za } j = 1, ..., n.$$

□

Za peti dokaz EGZ teoreme nam je potrebna tzv. lema o permanentama, o kojoj će biti riječi u nastavku.

3.5 Lema o permanentama

U ovom odjeljku ćemo predstaviti jedan vrlo moćan rezultat iz linearne algebre, koji je našao široku primjenu u teoriji grafova, kao i aditivnoj teoriji brojeva. Riječ je o jednoj lemi, koju je Alon nazvao lema o permanentama.

Permanenta matrice je pojam iz linearne algebre, sličan pojmu determinante, a u nastavku ćemo vidjeti i zašto. Radi što lakšeg uviđanja sličnosti ova dva pojma, podsjetićemo se prvo definicije determinante.

Definicija 3.6. Neka je $A = (a_{ij})$ kvadratna matrica dimenzija $n \times n$. Tada je determinanta matrice A definisana sa

$$\mathrm{Det}(A) = \sum_{\sigma \in S_n} \left(\mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \right),$$

gdje suma ide po svim elementima simetrične grupe S_n, odnosno po svim permutacijama elemenata $1, 2, ...n$. Sa $\mathrm{sgn}(\sigma)$ označavamo parnost date permutacije.

Definicija 3.7. Neka je $A = (a_{ij})$ kvadratna matrica dimenzija $n \times n$. Tada je permanenta matrice A definisana sa

$$\mathrm{Per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)},$$

gdje suma ide po svim elementima simetrične grupe S_n, odnosno po svim permutacijama elemenata $1, 2, ...n$.

Jednostavnije rečeno, jedina razlika je u tome što pri računanju permanente zanemarujemo parnost permutacije i u sumi uvijek imamo znak „+".

Još jednu ekvivalentnu definiciju permanente matrice uveo je Vardi[10] 1991. godine [60].

Definicija 3.8. Neka je $A = (a_{ij})$ kvadratna matrica dimenzija $n \times n$. Tada je permanenta matrice A koeficijent monoma $x_1 \cdot ... \cdot x_n$ u polinomu

$$\prod_{i=1}^{n} (a_{i1}x_1 + a_{i2}x_2 + ... + a_{in}x_n).$$

Da bismo što bolje objasnili ovaj pojam, daćemo nekoliko primjera.

Primjer 3.24. Izračunati permanentu sljedeće matrice.

$$\mathrm{Per} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh + ceg + bdi + afh.$$

Primjer 3.25. Neka je A kvadratna matrica dimenzija $n \times n$ čiji su svi elementi jednaki 1. Izračunati njenu permanentu.

[10] Ilan Vardi (1957–), kanadski matematičar

Koristimo definiciju:

$$\mathrm{Per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Kako su svi elementi date matrice A jednaki 1, važi sljedeća jednakost:

$$\mathrm{Per}(A) = \sum_{\sigma \in S_n} 1.$$

Dakle, permanenta je jednaka broju permutacija na skupu od n elemenata, a to je $n!$. Stoga je

$$\mathrm{Per}(A) = n!\ .$$

Lema o permanentama se u potpunosti uklapa u okvir naše priče, jer osim toga što ćemo pomoću nje doći do još jednog dokaza propozicije 3.14, odnosno teoreme EGZ, ova lema je još jedan primjer široke primjene Kombinatornog „Nullstellensatza".

Stoga ćemo kao i do sada prvo dati originalni dokaz leme o permanentama, a potom dokaz pomoću našeg glavnog alata tj. teoreme 2.3. Prvi dokaz i više o samoj lemi može se pronaći u [10] i [5].

Prvo navodimo i dokazujemo lemu iz koje slijedi lema o permanentama.

Lema 3.26. *([9]) Neka je P multilinearni polinom (linearan po svim promjenljivim) nad nekim komutativnim prstenom R, gdje je*

$$P = P(x_1, x_2, ..., x_m) = \sum_{J \subset \{1,2,...,m\}} b_J \cdot \prod_{i \in J} x_i.$$

Ako je

$$P(x_1, x_2, ..., x_m) = 0,\ za\ sve\ (x_1, x_2, ..., x_m) \in \{0,1\}^m,$$

onda je $P \equiv 0$, tj. $b_J = 0$ za sve $J \subset \{1, 2, ..., m\}$.

Dokaz. Dokaz dajemo indukcijom po broju promjenljivih m.

Za $m = 1$, imamo linearni polinom $P(x_1)$ po jednoj promjenljivoj i neka je $P(0) = P(1) = 0$. Kako linearni polinom može imati najviše jednu nulu, slijedi da je $P \equiv 0$.

Sada pretpostavimo da tvrđenje važi za $m - 1$ i dokažimo za m. Primijetimo da polinom P uvijek možemo posmatrati kao polinom po x_m čiji su koeficijenti iz $R[x_1, ..., x_m]$, na sljedeći način:

$$P(x_1, ..., x_m) = \sum_{i=0}^{1} P_i(x_1, ..., x_{m-1}) x_m^i,$$

gdje i ide od 0 do 1, jer je P linearan po x_m. Neka je

$$P(x_1, ..., x_m) = 0, \text{ za sve } (x_1, x_2, ..., x_m) \in \{0,1\}^m.$$

Tada mora biti

$$P_i(x_1, ..., x_{m-1}) = 0, \text{ za sve } (x_1, x_2, ..., x_{m-1}) \in \{0,1\}^{m-1},$$

za $i \in \{0,1\}$. Sada za svako P_i možemo iskoristiti indukcijsku hipotezu, odakle dobijamo da je $P_0 \equiv 0$ i $P_1 \equiv 0$, pa je i $P \equiv 0$, što je i trebalo dobiti. □

Primijetimo da prethodna lema može jednostavno da se dobije i kao posljedica pomoćne leme 2.1.

Dokaz. Kako je dati polinom P linearan po svakoj promjenljivoj, najveći stepen x_i je 1 za sve i, gdje $1 \leq i \leq m$. Ako definišemo $S_i = \{0,1\}$ za sve $i = 1, ..., m$, biće ispunjeni uslovi leme 2.1 iz koje onda slijedi da je $P \equiv 0$. Time je dokaz završen. □

Sada prelazimo na glavnu lemu.

Lema 3.27. *(Lema o permanentama) Neka je $A = (a_{ij})$ kvadratna matrica dimenzija $n \times n$ nad $\mathbb{Z}_p$ i pretpostavimo da je $Per(A) \neq 0$ ($u\ \mathbb{Z}_p$). Tada za sve $b_1, ..., b_n \in \mathbb{Z}_p$, postoje neki $\eta_1, ..., \eta_n \in \{0,1\}$ tako da je*

$$\sum_{j=1}^{n} \eta_j a_{ij} \neq b_i \text{ za sve } 1 \leq i \leq n.$$

Dokaz. ([8]) Pretpostavimo suprotno, da opisani $\eta_1, ..., \eta_n$ ne postoje. Posmatrajmo sljedeći polinom

$$P = P(x_1, ..., x_n) = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j - b_i \right).$$

Tada primijetimo da za proizvoljno izabrane $(x_1, ..., x_n) \in \{0,1\}^n$, mora biti

$$\sum_{j=1}^{n} a_{ij} x_j = b_i,$$

za bar jedno i, $1 \leq i \leq n$, jer bismo u suprotnom došli u kontradikciju sa polaznom pretpostavkom. Zato je $P(x_1, ..., x_n) = 0$ za sve $(x_1, ..., x_n) \in \{0,1\}^n$.

Definišimo sada polinom $\tilde{P}$, koji se od našeg polinoma P dobija sljedećom vrstom linearizacije. Naime, prvo polinom P napišimo kao sumu monoma oblika $a_J \prod_{i \in J} x_i^{s_i}$. Potom, kada god je $s_i > 1$, zamijenimo javljanje datog monoma sa monomom $a_J \prod_{i \in J} x_i$. Na taj način dobićemo polinom koji ima iste nule kao polinom P, a dodatno je linearan po svim promjenljivim.

Sada su zadovoljeni uslovi leme 3.26 za polinom $\tilde{P}$, odakle sijedi da je $\tilde{P} \equiv 0$. Ali sa druge strane, kako je koeficijent uz monom $x_1 x_2 \cdot ... \cdot x_n$ baš $\mathrm{Per}(A) \neq 0$, slijedi da postoji koeficijent različit od nule, odnosno dati polinom ne može biti identički jednak nuli. To nas dovodi do kontradikcije sa gore dokazanim, čime je dokaz završen. □

Lema koju ćemo sada predstaviti je neka vrsta uopštenja leme o permanentama 3.27, koju je Alon formulisao na ovaj način da bi njen dokaz slijedio direktno iz Kombinatornog „Nullstellensatza", odnosno teoreme 2.3.

Lema 3.28. *Neka je $A = (a_{ij})$ kvadratna matrica dimenzija $n \times n$ nad nekim poljem F i pretpostavimo da je $Per(A) \neq 0$. Tada za svaki vektor $b = (b_1, ..., b_n) \in F^n$ i za svaku familiju skupova $S_i \subset F, |S_i| = 2, za\, 1 \leq i \leq n$, postoji vektor $x = (x_1, ..., x_n) \in S_1 \times S_2 \times ... \times S_n$ tako da je i-ta koordinata vektora Ax različita od b_i, za svako $1 \leq i \leq n$.*

Dokaz. Kao i do sada, najteži zadatak je smisliti odgovarajući polinom koji će dovesti do rješenja. U tu svrhu posmatrajmo već viđen polinom

$$P(x_1, x_2, ..., x_n) = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j - b_j \right).$$

Tada je koeficijent monoma $x_1 x_2 \cdot ... \cdot x_n$ u polinomu P zapravo baš permanenta matrice A, koja je po pretpostavci različita od nule. Sada su zadovoljeni uslovi teoreme 2.3, pa postoji vektor $s = (s_1, ..., s_n) \in S_1 \times S_s \times ... \times S_n$, tako da je

$$P(s_1, ..., s_n) \neq 0.$$

Odnosno, za svako i je

$$\sum_{j=1}^{n} a_{ij} s_j \neq b_i.$$

Kada to prevedemo na jezik matrica, dobili smo da je $(As)_i \neq b_i$, za svako $1 \leq i \leq n$, a to je i trebalo pokazati. □

Primijetimo da u specijalnom slučaju ove leme, kada je $S_i = \{0, 1\}$ za sve i, dobijamo baš lemu o permanentama 3.27.

Sada ćemo navesti neke od primjena leme o permanentama.

3.5.1 Peti dokaz EGZ teoreme

Prva od njih je svakako još jedan dokaz propozicije 3.14, koji je dat u nastavku.

Dokaz. ([8]) Neka je dat niz $a_1, ..., a_{2p-1}$ elemenata ciklične grupe $\mathbb{Z}_p$. Prvo preimenujmo elemente niza da budu u neopadajućem redoslijedu tj. tako da je $a_1 \leq a_2 \leq ... \leq a_{2p-1}$. Tada, kao u prvom dokazu propozicije 3.14, u kome smo koristili Cauchy–Davenport teoremu, ako za neko i, gdje $1 \leq i \leq p-1$, važi $a_i = a_{i+p-1}$, onda je

$$a_i + a_{i+1} + ... + a_{i+p-1} = pa_i = 0,$$

u $\mathbb{Z}_p$. Zato pretpostavimo da je $a_i \neq a_{i+p-1}$, za sve i, $1 \leq i \leq p-1$.

Neka je $-a_{2p-1}$ jedan element grupe $\mathbb{Z}_p$, a preostalih $p-1$ označimo sa $b_1, ..., b_{p-1}$.

Definišimo kvadratnu matricu A dimenzija $(p-1) \times (p-1)$ čiji su svi elementi jedinice i definišimo skupove $S_i = \{a_i, a_{i+p-1}\}$, za sve $1 \leq i \leq p-1$. Permanenta tako definisane matrice je na osnovu primjera 3.25 jednaka

$$\mathrm{Per}(A) = (p-1)!,$$

što je sigurno različito od nule ($p \geq 2$). Sada možemo upotrebiti lemu 3.28. Dobijamo da postoji vektor $(x_1, ..., x_{p-1}) \in S_1 \times ... \times S_{p-1}$ tako da je

$$\sum_{j=1}^{p-1} x_j \neq b_i, \text{ za sve } 1 \leq i \leq p-1.$$

Kako je suma elemenata iz $\mathbb{Z}_p$ ponovo u $\mathbb{Z}_p$, slijedi da ta suma mora biti jednaka jedinom preostalom elementu, a to je $-a_{2p-1}$. Zato je

$$\sum_{j=1}^{p-1} x_j + a_{2p-1} = 0.$$

Time smo dobili da postoji podniz nekih p elemenata iz $\mathbb{Z}_p$ koji u zbiru daju nulu (u $\mathbb{Z}_p$), a to je upravo i trebalo dokazati. □

3.5.2 Harborthov problem

Sljedeća primjena leme o permanentama 3.27 koju ćemo navesti je ponovo usko vezana za problem sličan EGZ teoremi.

Naime, riječ je o problemu koji je prvi put diskutovao Harborth ([34]) 1973. Označimo sa $f(n,d)$ najmanji mogući broj f takav da svaki skup od f tačaka rešetke d-dimenzionalnog euklidskog prostora sadrži neki podskup od tačno n elemenata čije je težište ponovo tačka rešetke. Ovaj problem se može prevesti na priču o nizovima elemenata grupe $\mathbb{Z}_n^d$ i u tom smislu $f(n,d)$ onda označava najmanju vrijednost f takvu da svaki niz dužine f u $\mathbb{Z}_n^d$, ima podniz dužine n čija je suma elemenata u posmatranoj grupi jednaka 0.

Osnovni zadatak je odrediti ili procijeniti funkciju $f(n,d)$ za različite dimenzije prostora.

Na primjer, EGZ teorema rješava jednodimenzionalni slučaj, i ako se ispriča jezikom ovog problema, imamo da je $f(n,1) = 2n-1$ za sve $n \in \mathbb{N}$.

Za dvodimenzionalni slučaj postoji poznata hipoteza Kemnitza ([40]), koju navodimo u nastavku.

Hipoteza 3.29. *Neka je dat niz $a_1, a_2, ..., a_{4n-3}$ ne nužno različitih elemenata grupe $\mathbb{Z}_n \oplus \mathbb{Z}_n$. Tada postoji indeksni skup $I \subset \{1,2,...,4n-3\}$, takav da je $|I| = n$ i $\sum_{i\in I} a_i = 0$ (u datoj grupi).*

Kao u jednodimenzionalnom slučaju dovoljno je pokazati ovu hipotezu za proste brojeve, odnosno za $n = p$, gdje p prost. Kemnitz je pokazao svoju hipotezu za neke vrijednosti prostih brojeva tj. za $p = 2, 3, 5$ i 7.

Sljedeći značajan pomak u dvodimenzionalnom slučaju je teorema koju su dokazali Alon i Dubiner[11] [8]. Riječ je o malo slabijem rezultatu nego što je gore navedena hipoteza.

Teorema 3.30. *Neka je dat niz $a_1, a_2, ..., a_{6n-5}$ ne nužno različitih elemenata grupe $\mathbb{Z}_n \oplus \mathbb{Z}_n$. Tada postoji indeksni skup $I \subset \{1,2,...,6n-5\}$, takav da je $|I| = n$ i $\sum_{i\in I} a_i = 0$ (u datoj grupi).*

Glavni alat u dokazu ovog rezultata je baš lema o permanentama 3.27, a kako dokaz nije baš direktan i zahtjeva više usputnih rezultata i dokazivanja, za više detalja pogledati [8].

Kemnitzova hipoteza je dokazana u jesen 2003. godine, zahvaljujući Reiheru[12]. Za detaljan dokaz pogledati [53].

U opštem slučaju određivanje vrijednosti $f(n,d)$ je nimalo trivijalan problem. Neke od poznatih granica ove funkcije su date sa

$$(n-1)2^d + 1 \leq f(n,d) \leq (n-1)n^d + 1,$$

[11]Moshe Dubiner (1957–), izraelski matematičar

[12]Christian Reiher (1984–), njemački matematičar

$$f(n_1 n_2 d) \leq f(n_1, d) + n_1(f(n_2, d) - 1).$$

Ostavljamo čitaocu da se uvjeri da je zaista tako, a dokaz se može se pronaći u [34].

3.5.3 Jaegerova hipoteza

Još jedna primjena leme o permanentama je u dokazu specijalnog slučaja hipoteze koju je postavio Jaeger. Prije nego što navedemo samu hipotezu, podsjetićemo se pojma regularne matrice.

Definicija 3.9. Za kvadratnu matricu A dimenzija $n \times n$ kažemo da je regularna (nesingularna, invertibilna), ako postoji matrica B istih dimenzija tako da je

$$AB = BA = I_n,$$

gdje je I_n jedinična matrica $n \times n$.

Hipoteza 3.31. *([36])(Jaeger) Neka je A nesingularna kvadratna matrica dimenzija $n \times n$ nad proizvoljnim poljem koje ima bar četiri elementa. Tada postoji vektor x takav da x i Ax imaju sve koordinate različite od nule.*

Daćemo dokaz ove hipoteze koristeći lemu o permanentama u specijalnom slučaju kada je posmatrano polje karakteristike 2. Tada se determinanta i permanenta matrice A poklapaju, jer je u polju karakteristike 2 svaki element sam svoj inverz, odnosno $x = -x$, pa nam nije važno da li obraćamo pažnju na znak permutacije.

Primijetimo kako je data matrica nesingularna, tj. regularna, njena determinanta, pa samim tim i permanenta je različita od nule. Dalje, uzmimo da je b nula vektor i svaki S_i podskup datog polja takav da sadrži neka 2 elementa polja i nijedan ne sadrži nulu.

Tada su ispunjeni svi uslovi leme 3.28 iz koje onda slijedi da postoji neki vektor $x = (x_1, x_2, ..., x_n) \in S_1 \times S_2 \times ... \times S_n$ tako da je i-ta koordinata vektora Ax različita od i-te koordinate vektora b, za svako i, $1 \leq i \leq n$. Odnosno, svaka koordinata vektora Ax je različita od nule, a isto važi i za vektor x, jer nijedan skup S_i ne sadrži nulu, za $1 \leq i \leq n$.

Time je dokaz završen.

Dokaz ove hipoteze za polje koje ima pet elemenata je i danas otvoren problem. Alon i Tarsi su pokazali sljedeću teoremu koja je formulisana u nastavku, a dokazana u [5].

Teorema 3.32. *Neka je A nesingularna kvadratna matrica dimenzija $n \times n$ nad proizvoljnim poljem koje ima $q \geq 4$ elemenata. Tada ako q nije prost broj, odnosno $q = p^k$, gdje je $k \geq 2$ i p prost, postoji vektor x takav da x i Ax imaju sve koordinate različite od nule.*

3.5.4 Aditivne baze

Sljedeća primjena leme 3.27 je izložena u nastavku. Prvo definišemo pojam aditivne baze.

Definicija 3.10. ([10]) Neka je $\mathbb{Z}_p^n$ n-dimenzionalni vektorski prostor. Aditivna baza prostora $\mathbb{Z}_p^n$ je neka kolekcija C vektora iz $\mathbb{Z}_p^n$ koji nisu nužno različiti, a koja je takva da se svaki vektor $x \in \mathbb{Z}_p^n$ može predstaviti kao suma nekih elemenata date kolekcije.

Označimo sa $f(p, n) = c$ najmanji broj c takav da kada god imamo baš c linearnih baza $B_1, ..., B_c$, njihova unija sadrži aditivnu bazu tj. postoji gore opisana kolekcija C tako da je

$$C \subset \bigcup_{i=1}^{c} B_i.$$

Prvo ćemo dati neke jednostavne procjene vrijednosti ove funkcije. Važi da je

$$f(p, n) \geq p - 1.$$

Da bismo to vidjeli dovoljno je da uzmemo $p - 2$ kopije iste baze i uočimo da njihova unija ne sadrži aditivnu bazu. Međutim ova granica se može lako popraviti za $p \geq 3$ i $n \geq 2$, na

$$f(p, n) \geq p.$$

Dokažimo ovu tvrdnju za $n = 2$. Označimo sa $\{x, y\}$ neku bazu prostora $\mathbb{Z}_p^2$. Potom posmatrajmo $p-2$ kopije te baze i dodajmo jednu bazu $\{x+y, x-y\}$. Primijetimo da sumom bilo kojih elemenata datih baza ne možemo dobiti elemenat $-y$.

Dakle, našli smo primjer $p - 1$ baze koje su takve da njihova unija ne sadrži aditivnu bazu, pa je stoga $f(p, 2)$ bar p.

U radu [37] je postavljena sljedeća hipoteza.

Hipoteza 3.33. *Za svaki prost broj p postoji konstanta $c(p)$ tako da unija bilo kojih $c(p)$ linearnih baza prostora $\mathbb{Z}_p^n$ sadrži aditivnu bazu.*

Dokaz ove tvrdnje je još uvijek otvoren problem. Neki od značajnih rezultata u vezi sa ovim pitanjem mogu se naći u radu [10]. Između ostalog tu su data dva dokaza sljedeće teoreme.

Teorema 3.34.

$$f(p,n) \leq c(p)\log n.$$

Tačnije, pokazana su sljedeća dva rezultata:

$$f(p,n) \leq 1 + \frac{p^2}{2}\log 2pn \quad \text{i}$$

$$f(p,n) \leq (p-1)\log n + p - 2.$$

U drugom rezultatu se do date granice, koja je nešto bolja od prve, dolazi baš koristeći lemu o permanentama 3.27. Ključni korak u dokazu tog tvrđenja je baš posljedica pomenute leme, koju ćemo dokazati u nastavku.

Prije nego što formulišemo samu posljedicu, prvo ćemo objasniti notaciju u njoj.

Definicija 3.11. Neka su x i y dva vektora dimenzije n i m redom. Tada je njihov tenzorski proizvod $x \oplus y$ matrica dimenzija $n \times m$, čiji elementi su dati sa $(x \oplus y)_{ij} = x_i y_j$. Odnosno $x \oplus y = xy^T$.

Neka je dat neki vektor $v = (v_1, ..., v_n) \in \mathbb{Z}_p^n$. Sa v^* ćemo označiti tenzorski proizvod vektora v sa vektorom koji ima $p-1$ jedinica. Tako ćemo dobiti vektor koji pripada prostoru $\mathbb{Z}_p^{(p-1)n}$, koji je nastao nadovezivanjem $p-1$ kopije vektora v.

Posljedica 3.35. *Neka je $v_1, ..., v_{(p-1)n}$ niz od $(p-1)n$ vektora u prostoru $\mathbb{Z}_p^n$. Neka je A kvadratna matrica dimenzija $(p-1)n \times (p-1)n$ čije kolone čine vektori $v_1^*, v_2^*, ..., v_{(p-1)n}^*$. Ako je $Per(A) \neq 0$, onda dati polazni niz čini aditivnu bazu prostora $\mathbb{Z}_p^n$.*

Dokaz. Treba da pokažemo da se svaki element prostora $\mathbb{Z}_p^n$ može predstaviti kao suma nekih elemenata niza $v_1, ..., v_{(p-1)n}$. Neka je $a = (a_1, ..., a_n) \in \mathbb{Z}_p^n$ neki proizvoljan element.

Označimo sa a^* vektor koji se dobija konkatenacijom sljedećih vektora

$$a + i, a + 2i, ..., a + (p-1)i,$$

gdje je $i = (1, 1, ..., 1)$ vektor dimenzije n. Dakle, imamo da je

$$a^* = (a_1 + 1, ..., a_n + 1, a_1 + 2, ..., a_n + 2, ..., a_1 + (p-1), ..., a_n + (p-1))$$

vektor dimenzije $(p-1)n$. Definišimo skupove $S_i = \{0, 1\}$, za $1 \leq i \leq (p-1)n$. Tada, kako su ispunjeni uslovi leme 3.28, slijedi da postoji neki vektor $x = (x_1, ..., x_{(p-1)n}) \in S_1 \times ... \times S_{(p-1)n}$ takav da se i-ta koordinata vektora Ax razlikuje od i-te koordinate vektora a^*. Kako je svaka koordinata vektora x ili 0 ili 1, slijedi da vektor Ax možemo napisati kao

$$\sum_{i \in I} v_i^*$$

gdje je $I \subset \{1, 2, ..., (p-1)n\}$ indeksni skup svih indeksa i za koje je $x_i = 1$. Dakle, dobili smo $p-1$ vrijednosti za svaku koordinatu $\sum_{i \in I} v_i$ koje ne dolaze u obzir. Tako da ostaje samo jedna opcija, tj. da je

$$\sum_{i \in I} v_i = a.$$

Tako smo vektor a predstavili kao sumu vektora iz datog niza i time dovršili dokaz. □

Dajemo još jednu hipotezu iz rada [10] koja nije dokazana, ali ako bi se ispostavilo da je tačna, iz nje bi slijedilo da unija bilo kojih p linearnih baza prostora $\mathbb{Z}_p^n$ jeste aditivna baza, odnosno $f(p, n) \leq p$.

Hipoteza 3.36. *Neka su date regularne matrice $A_1, A_2, ..., A_p$ nad $\mathbb{Z}_p$ dimenzija $n \times n$. Tada postoji matrica C dimenzija $n \times pn$ tako da matrica $pn \times pn$*

$$\begin{bmatrix} A_1 & A_2 & ... & A_{p-1} & A_p \\ A_1 & A_2 & ... & A_{p-1} & A_p \\ . & . & . & . & . \\ . & . & . & . & . \\ A_1 & A_2 & ... & A_{p-1} & A_p \\ & & C & & \end{bmatrix} \tag{3.26}$$

ima permanentu različitu od nule (u $\mathbb{Z}_p$).

3.5.5 Permanenta $(0, 1)$-matrice

Posljednja primjena leme 3.27 koju ćemo ovdje pomenuti je data u nastavku. Naime, u pitanju je jedan rezultat iz teorije grafova kojim ćemo zainteresovati čitaoce za kombinaciju ove zanimljive oblasti i algebarskih tehnika koje su se pokazale vrlo korisnim u raznim dokazima. To je upravo tema kojoj će biti posvećeno naredno poglavlje ovog rada. Prvo uvodimo potrebne pojmove.

Definicija 3.12. Usmjeren graf ili digraf je graf čije ivice imaju orijentaciju. Digraf D posmatramo kao uređeni par $D = (V, E)$ gdje su

1. V skup tjemena (čvorova);

2. $E \subseteq \{(x, y) : (x, y) \in V^2\}$.

Ako $(u, v) \in E(D)$, onda je u početak te grane, a v je kraj. Odnosno kažemo da ta grana izlazi iz u u v ili da je orijentisana od u ka v. Pišemo još $u \to v$.

Definicija 3.13. Za svaki čvor v definišemo njegov izlazni skup $O_D(v)$ i ulazni skup $I_D(v)$ sa

$$O_D(v) = \{x \in V(D) : v \to x\},$$

$$I_D(v) = \{x \in V(D) : x \to v\}.$$

Izlazni stepen je kardinalnost izlaznog skupa $|O_D(v)|$, a ulazni stepen je kardinalnost ulaznog $|I_D(v)|$.

Definicija 3.14. Neka je dat digraf D. Tada je njegov podgraf H Ojlerov ako je

$$|O_D(v)| = |I_D(v)| \text{ za } \forall v \in V(H).$$

Definicija 3.15. 1-regularan podgraf digrafa je podgraf u kome svaki čvor v ima izlazni i ulazni stepen 1, odnosno $|O_D(v)| = |I_D(v)| = 1$ (to je podgraf koji je unija orijentisanih kontura).

Sada smo spremni za propoziciju.

Propozicija 3.37. *([3]) Neka je dat digraf $D = (V, E)$ koji sadrži 1-regularan podgraf. Neka je svakom čvoru digrafa D dodijeljen dvoelementni skup S_v koji sadrži neke realne elemente. Tada se za svako v može odabrati $c(v) \in S_v$ tako da je za svaki čvor u ispunjeno*

$$\sum_{v:\,(u,v)\in E} c(v) \neq 0.$$

Dokaz. Označimo sa A tzv. matricu susjedstva. Njeni elementi su definisani na sljedeći način:

1. $a_{u,v} = 1$ ako i samo ako $(u, v) \in E$,

2. i $a_{u,v} = 0$ inače.

Prema uslovima propozicije, permanenta ove matrice je strogo pozitivna. Onda traženi rezultat slijedi iz leme 3.28. □

U nastavku dajemo jedan interesantan podatak o računanju permanenti ovakvih matrica.

Permanenta $(0,1)$-matrice koja je pridružena usmjerenom grafu je jednaka broju pokrivača grafa koji čine čvorno disjunktne konture. Tako se u teoriji brojeva interpretira pojam permanente i ova činjenica se zapravo koristi u dokazu tvrđenja koje kaže da je računanje permanente matrice problem koji je # P-kompletan.

P-kompletni problemi predstavljaju jednu klasu kompleksnosti u računskoj teoriji složenosti (eng. Computational complexity theory), što je grana teorijske računarske nauke. Više o pomenutoj temi se može pronaći u [39].

Tvrdnja da je računanje permanente $(0,1)$-matrice # P-kompletan problem je poznato i kao Valiantova teorema [49].

3.6 Grafovi i podgrafovi

U ovom odjeljku ćemo predstaviti neke interesantne rezultate iz teorije grafova, čiji dokazi mogu da se ispričaju pomoću alata koje smo uveli u ovom radu, sa Kombinatornim „Nullstellensatzom" u glavnoj ulozi. Prvo ćemo se podsjetiti nekih osnovnih pojmova.

Definicija 3.16. Neka je $G = (V, E)$ graf i v neki njegov čvor. Tada je $\deg(v)$ stepen čvora v i predstavlja broj susjeda datog čvora. Za dva čvora kažemo da su susjedi ako su povezani granom.

Definicija 3.17. Za graf $G = (V, E)$ kažemo da je regularan ako su mu svi čvorovi istog stepena. Dodatno, $G = (V, E)$ je k-regularan, ako je $\deg(v) = k$ za sve $v \in V$.

Definicija 3.18. Grana $e = \{v, v\}$ je petlja. Grane e_1 i e_2 su paralelne ako je $e_1 = e_2 = \{u, v\}$. Graf je prost ako nema ni petlje ni paralelne grane.

Definicija 3.19. Graf $H = (V', E')$ je pokrivajući podgraf grafa $G = (V, E)$ ako je $V' = V$ i $E' \subset E$.

Definicija 3.20. Za graf $G = (V, E)$, $|V| = n$, kažemo da je kompletan ako je $\deg(v) = n - 1$, *za sve* $v \in V$. Sa K_n označavamo kompletan graf sa n čvorova.

Definicija 3.21. Prazan graf $G = (V, E)$ je komplement kompletnog grafa. To je graf koji ima samo čvorove i nijednu granu. Ako je $|V| = n$, onda sa $\overline{K}_n$ označavamo prazan graf sa n čvorova.

Definicija 3.22. Za graf kažemo da je planaran ukoliko se može nacrtati u ravni tako da mu se grane ne sijeku.

Definicija 3.23. Za graf kažemo da je povezan ako postoji put između svaka dva njegova čvora, gdje je put vid šetnje od jednog čvora do drugog u kome ne smijemo proći kroz jedan čvor više puta. Povezan graf je k-povezan ako, kada god obrišemo manje od k čvorova, graf i dalje ostaje povezan.

Definicija 3.24. Hamiltonova kontura je kontura koja sadrži sve čvorove grafa. Za graf kažemo da je Hamiltonov ako sadrži Hamiltonovu konturu.

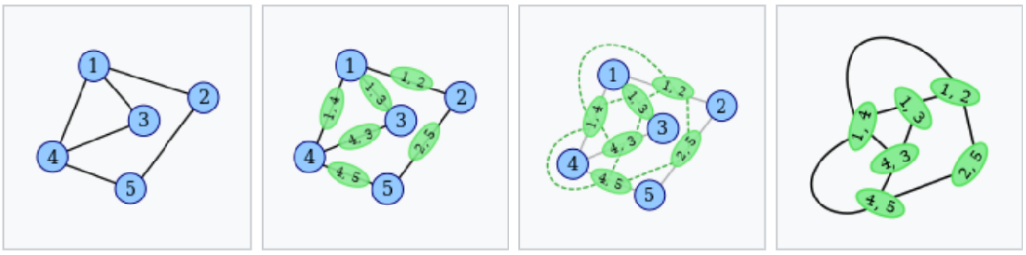
Definicija 3.25. Ojlerov put je put u grafu koji prolazi kroz svaku granu tačno jednom. Ojlerova kontura je Ojlerov put koji počinje i završava se u istom čvoru. Graf je poluojlerov ako sadrži Ojlerov put, a Ojlerov ako sadrži Ojlerovu konturu.

Definicija 3.26. Za graf $G = (V, E)$ kažemo da je bipartitan, ako se njegovi čvorovi mogu podijeliti u dva disjunktna skupa M i N tako da svaka grana datog grafa ima jedan čvor u M a jedan u N. Ako je graf dodatno i kompletan, onda je to kompletan bipartitni graf, u oznaci $K_{m,n}$, gdje je $|M| = m$ i $|N| = n$.

Važi sljedeća teorema.

Teorema 3.38. *Graf sa bar dva čvora je bipartitan ako i samo ako ne sadrži neparnu konturu (konturu neparne dužine).*

Definicija 3.27. Za svaki graf $G = (V, E)$ možemo definisati njemu odgovarajući linijski graf $L(G)$, tako što za svaku granu koja postoji u grafu G nacrtamo po jedan čvor u grafu $L(G)$, a ako su dvije grane u G imale zajednički čvor, onda će one biti povezane granom u $L(G)$.



Slika 3.1. Graf G i postepeno crtanje linijskog grafa $L(G)$

Definicija 3.28. Matrica incidencije A grafa G je matrica koja u potpunosti određuje graf. Vrste te matrice predstavljaju grane grafa, dok su kolone čvorovi. Element $a_{i,j} = 1$ ako čvor iz j-te kolone pripada grani iz i-te vrste (pri čemu posmatramo graf bez petlji), a inače je $a_{i,j} = 0$.

Definicija 3.29. Neka je dat graf $G = (V, E)$ (usmjeren ili neusmjeren) i neka su njegovi čvorovi $V = \{v_1, ..., v_n\}$. Tada tom grafu možemo pridružiti sljedeći polinom:

$$f_G(x_1, ..., x_n) = \prod_{i<j, \{v_i, v_j\} \in E(G)} (x_i - x_j),$$

i njega onda zovemo polinom grafa G.

Više o osobinama ovog polinoma se može pronaći u [55].

3.6.1 p-djeljivi podgrafovi

Prvi zanimljiv rezultat kojem ćemo posvetiti nekoliko redova je sljedeća hipoteza.

Hipoteza 3.39. *([19])(Berge–Sauer) Svaki prost, 4-regularan graf sadrži 3-regularan podgraf.*

Hipoteza je dokazana u radu ([58]).

Primijetimo da, ako oslabimo uslove i dozvolimo paralelne grane, hipoteza ne važi. Na primjer, posmatrajmo neku neparnu konturu i konstruišimo graf G tako što ćemo svaku granu konture zamijeniti sa dvije paralelne grane. Time ćemo dobiti 4-regularan graf koji nema podgraf koji je 3-regularan, pa hipoteza ne važi.

U sljedećoj teoremi ćemo pokazati šta će se desiti ako dodamo jednu granu i ne zahtijevamo da graf bude prost. Riječ je o rezultatu koji se jednostavno dobija primjenom Chevalley–Warningove teoreme 3.3.

Teorema 3.40. *([11]) Neka je dat 4-regularan graf G. Ako mu dodamo jednu granu, dobićemo graf koji sadrži 3-regularan podgraf.*

Dokaz. Neka je $G = (V, E)$ 4-regularan graf sa n čvorova kome smo dodali jednu granu, pa je $|E| = 2n + 1$. Neka je A matrica incidencije datog grafa.

Posmatrajmo sljedeći sistem jednačina u $\mathbb{Z}_3$:

$$\sum_{i=1}^{2n+1} a_{i,j} x_i^2 = 0, \text{ za sve } j \in \{1, 2, ..., n\}.$$

Kako je svaki od datih polinoma stepena 2, a ukupno ih ima n, suma njihovih stepena je $2n$ što je manje od $2n+1$. Takođe, primijetimo da je nula vektor trivijalno rješenje ovog sistema. Sada na osnovu Chevalley–Warning teoreme 3.3, ovaj sistem ima netrivijalno rješenje $x = (x_1, x_2, ..., x_{2n+1})$.

Ako sa I označimo indeksni skup svih indeksa za koje je $x_i \neq 0$, imamo da je $\emptyset \neq I \subseteq \{1, 2, ..., 2n+1\}$. Kako smo u $\mathbb{Z}_3$, za svako $x_i \neq 0$ je ispunjeno $x_i^2 = 1$ (u $\mathbb{Z}_3$). Stoga važi sljedeće zapažanje:

$$\sum_{i \in I} a_{i,j} = 0 \text{ (u } \mathbb{Z}_3) \text{ za sve } j \in \{1, 2, ..., n\}.$$

Kako je dati graf 4-regularan, u svakoj koloni matrice incidencije su tačno 4 elementa jednaka 1. Ovdje smo izdvojili indeksni skup za koji suma datih elemenata mora iznositi baš 3 i time smo našli traženi 3-regularan podgraf. □

Sada ćemo dokazati opštiju teoremu čiji je ovo specijalan slučaj. Ponovo, riječ je o teoremi koja može da se dokaže i pomoću Kombinatornog „Null-stellensatza".

Teorema 3.41. *([9]) Neka je q prost broj i neka je $G = (V, E)$ graf bez petlji čiji čvorovi imaju stepen k ili $k+1$ i bar jedan čvor ima stepen $k+1$. Ako je $k \geq 2q-2$, tada G ima q-regularan podgraf.*

U nastavku ćemo dati originalni dokaz. Prvo uvodimo nove pojmove.

Definicija 3.30. Za graf $G = (V, E)$ kažemo da je p-djeljiv ako $p \mid \deg(v)$ za sve $v \in V$.

Definicija 3.31. Neka je dat graf $G = (V, E)$ koji ima n čvorova. Sa $f(n, p)$ označavamo maksimalan broj ivica grafa G takav da nema netrivijalan p-djeljiv podgraf.

Imamo sav potreban alat da formulišemo teoremu koja će nam biti potrebna za dokaz teoreme 3.41.

Teorema 3.42. *([9]) Neka je dat graf $G = (V, E)$, $|V| = n$, p neparan prost broj i neka je $f(n, q)$ gore definisano. Tada je*

1. *$f(n, q) \leq (q-1)n$, ako je $q = p^d$,*
2. *$f(n, q) \leq (q-1)n - \frac{q}{2}$, ako je $q = 2^d$.*

Dokaz. 1. Neka je dat graf $G = (V, E)$ takav da $|V| = n$. Treba pokazati da ako dati graf ima više od $(p^d - 1)n$ grana, mora sadržati q-djeljiv podgraf. Zato pretpostavimo da je $|E| = m > (p^d - 1)n$.

Neka je $V = \{v_1, v_2, ..., v_n\}$, i za svaku granu $e \in E$ definišimo vektor $a^{(e)} = (a^{(e)}_{v_1}, a^{(e)}_{v_2}, ..., a^{(e)}_{v_n})$ na sljedeći način:

$$a^{(e)}_{v_i} = 1, \text{ ako } v_i \in e, \text{ inače } a^{(e)}_{v_i} = 0.$$

Tada, ako označimo $d_1 = d_2 = ... = d_n = d$, kako je broj vektora $a^{(e)}$ jednak broju grana $|E| = m$, i kako je po pretpostavci $m > n(p^d - 1)$, ispunjeni su uslovi Olsonove teoreme 3.22. Iz nje slijedi da postoji indeksni skup $\emptyset \neq \tilde{E} \subset E$ takav da je

$$\sum_{e \in \tilde{E}} a^{(e)}_{v_i} \equiv 0 \pmod{q} \text{ za } i = 1, ..., n.$$

Tada je graf $H = (V, \tilde{E})$ traženi q-djeljiv podgraf grafa G.

2. U ovom slučaju pretpostavimo da je $|E| = m > (2^d - 1)n - 2^{d-1}$, i koristeći iste argumente i posljedicu 3.23, dobijamo traženo.

□

Formulisaćemo i dvije pomoćne leme čije dokaze izostavljamo. Prvu je dokazao Thomassen[13] [59], a drugu Petersen za parno k [19], a Taškinov za neparno [58].

Lema 3.43. *Neka je G graf čiji svaki čvor ima stepen k ili $k+1$ i bar jedan čvor ima stepen $k+1$, i neka je $0 \leq r < k$. Tada G sadrži pokrivajući podgraf čiji su svi čvorovi stepena r ili $r+1$ i bar jedan je stepena $r+1$.*

Lema 3.44. *Neka je $k \geq r$ i $k \equiv r \pmod 2$. Tada svaki k-regularan graf sadrži r-regularan podgraf.*

Konačno imamo sve što nam je potrebno za dokaz teoreme 3.41.

Dokaz. ([9]) Kako su ispunjeni uslovi leme 3.43, slijedi da graf G ima pokrivajući podgraf $L = (V, E_1)$ čiji su svi čvorovi stepena $2q - 2$ i bar jedan čvor je stepena $2q - 1$. Tada je broj grana datog podgrafa

$$|E_1| > |V| \frac{2q - 2}{2} = |V|(q - 1).$$

[13] Carsten Thomassen (1948–), danski matematičar

Sada na osnovu teoreme 3.42, slijedi da graf L ima q-djeljiv podgraf koji ćemo označiti sa H. Kako je,

$$\deg_H(v) \leq \deg_L(v) \leq 2q-1,$$

za svaki čvor $v \in V$, jedina mogućnost je da su svi čvorovi grafa H baš stepena q. Time svo pronašli q-regularan podgraf i završili dokaz. □

Ako na dobijeni podgraf H, primijenimo lemu 3.44, dobićemo r-regularan podgraf grafa G (gdje je $q \geq r$ i $q \equiv r \pmod 2$). Time smo dokazali sljedeću teoremu.

Teorema 3.45. *([9]) Neka je q prost broj i neka je $G = (V, E)$ graf bez petlji čiji čvorovi imaju stepen k ili $k+1$ i bar jedan čvor ima stepen $k+1$. Ako je $k \geq 2q-1$ i $q \geq r$, $q \equiv r \,(mod\, 2)$, tada G ima r-regularan podgraf.*

Nakon što smo vidjeli koliko pomoćnih tvrđenja nam je bilo potrebno za dokaz teoreme 3.41, pokažimo kako dokaz iste teoreme može da se dobije prilično jednostavno i direktno koristeći Kombinatorni „Nullstellensatz" (2.3). Dokaz dajemo za $k = 2p-2$, gdje je p prost broj.

Dokaz. ([3]) Neka je $A = (a_{v,e})$ matrica incidencije grafa $G = (V, E)$ (ovdje su vrste čvorovi $v \in V$, a kolone su grane $e \in E$). Pridružimo svakoj grani e neku promjenljivu x_e. Definišimo polinom f nad nekim konačnim poljem sa p elemenata na sljedeći način:

$$f(x_e|\, e \in E) = \prod_{v \in V} \Big(1 - \Big(\sum_{e \in E} a_{v,e} x_e\Big)^{p-1}\Big) - \prod_{e \in E}(1 - x_e).$$

Prvo treba da izračunamo $\deg(f)$. Kako je

$$\deg\Big(\prod_{v \in V}\Big(1 - \Big(\sum_{e \in E} a_{v,e} x_e\Big)^{p-1}\Big)\Big) = (p-1)|V| \text{ i}$$

$$\deg\Big(\prod_{e \in E}(1 - x_e)\Big) = |E|,$$

slijedi da je $\deg(f) = \max\{(p-1)|V|, |E|\}$. Ako bi svi čvorovi bili stepena baš $(2p-2)$, onda bi slijedilo $|E| = |V|\frac{2p-2}{2}$, ali kako imamo bar jedan čvor stepena $2p-1$, slijedi da je $|E| > (p-1)|V|$ i time smo dobili da je $\deg(f) = |E|$.

Dalje, stepen monoma $\prod_{e \in E} x_e$ je $(-1)^{|E|+1}$, jer se dati monom javlja samo u $\prod_{e \in E}(1 - x_e)$, a dodajemo 1 zbog minusa koji se javlja ispred proizvoda u

f. Neka su $S_i = \{0, 1\}$ podskupovi datog polja i neka ih ima koliko i grana $|E|$.

Sada su ispunjeni uslovi teoreme 2.3, iz koje slijedi da postoje $x_e \in \{0, 1\}$, za sve $e \in E$, tako da je

$$f(x_e |\, e \in E) \neq 0.$$

Primijetimo da vektor $x = (x_e | e \in E)$ ne može biti nula vektor, jer je za nula vektor vrijednost polinoma f baš nula. Dakle, postoji bar jedno $x_e = 1$. Takođe, primijetimo da za dati vektor x važi

$$\sum_{e \in E} a_{v,e} x_e \equiv 0 \pmod{p}, \tag{3.27}$$

jer bi u suprotnom, na osnovu male Fermaove teoreme, slijedilo da je

$$\Big(\sum_{e \in E} a_{v,e} x_e \Big)^{p-1} = 1,$$

pa bi opet bilo $f = 0$.

Stoga, možemo izdvojiti podgraf grafa G tako što ćemo izabrati sve grane za koje je $x_e = 1$. Na osnovu (3.27), svi stepeni datog podgrafa su djeljivi sa p, a kako su manji od $2p$ po pretpostavci teoreme, ostaje da moraju biti tačno p. Time smo našli p-regularan podgraf i dokazali teoremu.

□

3.6.2 Erdős–Sauerov problem

Erdős i Sauer su 1975. formulisali sljedeći problem ([17]):

Neka je dat prost graf G koji ima n čvorova. Koliko maksimalno grana može da ima pomenuti graf, ali tako da ne sadrži 3-regularan podgraf?

Postavili su hipotezu da za svako $\epsilon > 0$ traženi broj grana ne prelazi $n^{1+\epsilon}$, za dovoljno veliko n. Ovu hipotezu je pokazao Pyber[14] koristeći baš teoremu koju smo mi upravo dokazali. Mi ćemo ovdje dati glavnu ideju, a dokaz se može pronaći u [50].

Naime, posmatrao je graf sa n čvorova i bar $200n \log n$ grana i pokazao da takav graf ima podgraf čiji čvorovi imaju stepen 4 ili 5 i bar jedan čvor ima stepen 5. Ako na taj podgraf primijenimo teoremu 3.41, dobićemo da dati podgraf ima podgraf koji je 3-regularan.

Dakle, na neki način je odredio gornju granicu do koje ima smisla ispitivati i tražiti maksimalan broj grana u opisanom problemu.

[14] László Pyber (1960–), mađarski matematičar

Deset godina kasnije je u radu [51] pokazano da postoje prosti grafovi sa n čvorova i bar $cn \log\log n$ ($c > 0$) grana, a koji ne sadrže 3-regularan podgraf.

3.6.3 Još jedna primjena KN u teoriji grafova

U nastavku ćemo predstaviti još jedan rezultat iz teorije grafova, koji će čitaocu pokazati šarenoliku primjenu Kombinatornog „Nullstellensatza".

Biće nam potreban jedan poznat rezultat iz kombinatorike. Riječ je o principu uključenja i isključenja, koga ćemo se podsjetiti u nastavku.

Teorema 3.46. *(PUI) Neka su $A_1, A_2, ..., A_n$ konačni skupovi. Kardinalni broj unije datih skupova ispunjava jednakost:*

$$\Big|\bigcup_{i=1}^{n} A_i\Big| = \sum_{k=1}^{n}(-1)^{k-1}\Big(\sum_{1\le i_1<i_2<...<i_k\le n} |A_{i_1}\cap A_{i_2}\cap ...\cap A_{i_k}|\Big).$$

Propozicija 3.47. *Neka je p prost broj i neka je $G = (V, E)$ graf sa $|V| > d(p-1)$ čvorova. Tada postoji skup U, $\emptyset \neq U \subseteq V$, takav da je broj kompletnih podgrafova K_d koji sijeku skup U kongruentan sa 0 po modulu p.*

Dokaz. Neka je $\emptyset \neq I \subset V$, i označimo sa $K(I)$ broj kompletnih podgrafova K_d koji sadrže I. Svakom čvoru grafa G dodijelimo promjenljivu x_v i definišimo sljedeći polinom nad $GF(p)$ (konačno polje sa p elemenata):

$$F = \prod_{v\in V}(1 - x_v) - 1 + H,$$

gdje je

$$H = \Big(\sum_{\emptyset\neq I\subset V}(-1)^{|I|+1}K(I)\prod_{i\in I}x_i\Big)^{p-1}.$$

Tada je

$$\deg(F) = \max\{\deg\Big(\prod_{v\in V}(1-x_v)\Big), \deg(H)\}.$$

Lako uočavamo da je $\deg(\prod_{v\in V}(1-x_v)) = |V|$ i $\deg(H) = (p-1)|I|$.

Primijetimo da je $K(I) = 0$, pa samim tim i polinom $H = 0$, kada god je $|I| > d$. Stoga je $\deg(H) \le d(p-1)$. Kako je po pretpostavci $|V| > d(p-1)$, slijedi da je $\deg(F) = |V|$.

Dalje, koeficijent monoma $\prod_{v\in V} x_v$ u polinomu F je $(-1)^{|V|} \neq 0$. Definišimo skupove $S_i = \{0, 1\}$, za sve $i = 1, ..., |V|$. Tada na osnovu teoreme 2.3 slijedi da postoji vektor $x = (x_1, ..., x_{|V|})$, gdje $x_i \in S_i$, takav da je

$$F(x_1, ..., x_{|V|}) \neq 0.$$

Kako je nula vektor jedna nula polinoma F, vektor x ima bar jednu koordinatu jednaku 1, odakle slijedi da je

$$\prod_{v\in V}(1 - x_v) = 0.$$

Odatle dobijamo da je $H(x_1, ..., x_{|V|}) \neq 1$.

Ako iskoristimo malu Fermaovu teoremu, dobijemo da je

$$\sum_{\emptyset\neq I\subset V} (-1)^{|I|+1} K(I) \prod_{i\in I} x_i \equiv 0 \pmod{p},$$

jer bi u suprotnom slijedilo $H(x_1, ..., x_{|V|}) = 1$.

Ako definišemo skup $U := \{v \ : \ x_v = 1\}$, primijetimo da je lijeva strana kongruencije tačno broj kopija kompletnog podgrafa K_d koji sijeku skup U, na osnovu principa uključenja i isključenja. Kako je $|U| \geq 1$, pronašli smo traženi skup i time završili dokaz.

□

3.7 Bojenje grafova

Bojenje grafova je vrlo popularna oblast u okviru teorije grafova, koja je privukla veliku pažnju i interesovanje mnogobrojnih matematičara.

Istorija razvoja ove oblasti je vrlo zanimljiva i prvi počeci se vezuju za planarne grafove, odnosno za bojenje mapa. Naime, Guthrie[15] je bojio mapu Engleske tako što je imao jedno pravilo, da svaka dva susjedna okruga budu obojena različitim bojama. Tada je primijetio da su mu bile dovoljne samo četiri boje da oboji čitavu mapu. Njegov brat je potom ovu zanimljivu činjenicu ispričao svom profesoru matematike De Morganu[16] koji je to saznanje podijelio sa Hamiltonom[17] 1852. 27 godina kasnije, Cayley[18] je formulisao ovaj problem, a rješenje je ugledalo svjetlost dana tek čitav vijek kasnije.

[15] Francis Gutrie (1831–1899), afrički matematičar
[16] Augustus De Morgan (1806–1871), engleski matematičar
[17] Sir William Rowan Hamilton (1805–1865), irski matematičar, astronom i fizičar
[18] Arthur Cayley (1821–1895), engleski matematičar

Naime, Appel[19] i Haken[20] su 1977. pokazali da su 4 boje zaista dovoljne, ali njihov intrigantni dokaz se oslanja na računar i ispitivanje mnogobrojnih slučajeva, pa ga mnogi matematičari ne prihvataju, iako još niko nije pronašao grešku u tom dugom i iscrpnom dokazu. Danas je ovaj rezultat poznat kao Teorema o 4 boje.

Prije nego što navedemo neke interesantne rezultate iz ove oblasti, koji se mogu dokazati koristeći Kombinatorni „Nullstellensatz", napravićemo mali teorijski uvod sa definicijama svih osnovnih pojmova koji će nam biti potrebni.

Definicija 3.32. Neka je $C = \{c_1, c_2, ..., c_k\}$ skup boja i neka je dat graf $G = (V, E)$. Bojenje čvorova grafa G je funkcija $f : V(G) \to C$, koja svakom čvoru dodjeljuje neku boju. Za bojenje f kažemo da je pravilno ako

$$\forall\ uv \in E(G) \implies f(u) \neq f(v).$$

Bojenje f je k-bojenje $\iff |C| = k$. Graf G je k-obojiv ako postoji l-bojenje gdje je $l \leq k$.

Definicija 3.33. Hromatski broj grafa $G = (V, E)$, u oznaci $\chi(G)$, je broj koji označava koliko je najmanje boja potrebno da se čvorovi grafa G pravilno oboje. Odnosno, važi

$$\chi(G) = \min\{k \mid G \text{ je } k\text{-obojiv}\}.$$

Definicija 3.34. Neka je $C = \{c_1, c_2, ..., c_k\}$ skup boja i neka je dat graf $G = (V, E)$. Bojenje grana grafa G je funkcija $f : E(G) \to C$, koja svakoj grani dodjeljuje neku boju. Za bojenje grana f kažemo da je pravilno ako

$$\forall\, e_1, e_2 \in E(G) \text{ koje su susjedne } \implies f(e_1) \neq f(e_2).$$

Bojenje f je k-bojenje grana $\iff |C| = k$. Graf G je granski k-obojiv ako postoji l-bojenje grana gdje je $l \leq k$.

Definicija 3.35. Hromatski indeks grafa $G = (V, E)$, u oznaci $\chi_1(G)$, je broj koji označava koliko je najmanje boja potrebno da se grane grafa G pravilno oboje. Odnosno, važi

$$\chi_1(G) = \min\{k \mid G \text{ je granski } k\text{-obojiv}\}.$$

[19]Kenneth Ira Appel (1932–2013), američki matematičar
[20]Wolfgang Haken (1928–2022), njemačko-američki matematičar

Posebno zanimljivi problemi u ovoj oblasti nastaju kada se pri bojenju čvorova grafa uvedu i neki dodatni uslovi koji sužavaju izbor mogućih boja za svaki čvor. Taj tip problema su proučavali Erdős i Vizing[21] ([62]), i Rubin[22] i Taylor[23] ([32]), nezavisno jedni od drugih i danas je ta teorija poznata pod nazivom „The choosability properties of a graph", što i nema neki zgodan prevod na srpski jezik, te ćemo ga ostaviti u pomenutom obliku.

Alon i Tarsi su u radu [4] razvili određenu algebarsku tehniku koja se pokazala vrlo uspješnom u rješavanju problema koji pripadaju gore opisanom spektru problema. Ovdje ćemo pokazati kako neki od tih rezultata mogu da se dokažu pomoću Kombinatornog „Nullstellensatza".

Prvo ćemo definisati osnovne pojmove iz ove oblasti.

Definicija 3.36. Neka je dat konačan graf $G = (V, E)$ i neka je data funkcija $f : V(G) \to \mathbb{Z}$. Graf G je f-birljiv (eng. f-choosable) ako za svaku dodjelu skupova $S(v) \subset \mathbb{Z}$ svakom čvoru $v \in V$, gdje je $|S(v)| = f(v)$ (broj mogućih opcija za čvor v), postoji pravilno bojenje čvorova grafa G tako da $c : V \to \mathbb{Z}$ i pri tome $c(v) \in S(v)$ za sve $v \in V$. Graf G je k-birljiv ako je f-birljiv za konstantnu funkciju $f(v) \equiv k$.

Definicija 3.37. Odabirni broj grafa $G = (V, E)$ (eng. the choice number), u oznaci $\mathrm{ch}(G)$ je najmanja vrijednost k tako da je G k-birljiv. Drugim riječima,

$$\mathrm{ch}(G) = \min\{k \mid G \text{ je } k\text{-birljiv}\}.$$

Jednostavnije rečeno, za svaki čvor grafa G napravimo jednu listu boja koje mu možemo dodijeliti. Zatim definišemo funkciju bojenja koja svakom čvoru dodijeli jednu boju iz njegove liste mogućih boja. Naravno, da bi to bojenje bilo pravilno, dva susjedna čvora moraju biti obojena različitim bojama. Za graf kažemo da je k-birljiv ako kada god svakom čvoru dodijelimo listu od tačno k različitih boja, postoji gore opisano pravilno bojenje.

Jasno, važi

$$\mathrm{ch}(G) \geq \chi(G).$$

Međutim postoje mnogobrojni primjeri grafova za koje je

$$\mathrm{ch}(G) > \chi(G).$$

Neke od tih primjera ćemo vidjeti u nastavku.

[21] Vadim Georgievich Vizing (1937–2017), rusko-ukrajinski matematičar
[22] Arthur L . Rubin (1956–), američki matematičar
[23] Herbert Taylor, američki matematičar

Odabirni broj linijskog grafa G ima posebnu oznaku $\mathrm{ch}'(G)$ i nekada se naziva hromatski indeks liste grafa G. Ono što odmah uočavamo jeste da važi

$$\mathrm{ch}'(G) \geq \chi_1(G).$$

Da bismo riješili čitaoca svih nedoumica koje je potencijalno imao čitajući nove pojmove, daćemo nekoliko jednostavnih primjera.

Primjer 3.48. Za bipartitni graf $G = K_{2,4}$ odrediti $\mathrm{ch}(G)$.

Označimo sa U i V dva disjunktna skupa čvorova grafa G, gdje je $U = \{u_1, u_2\}$ i $V = \{v_1, v_2, v_3, v_4\}$. Kako je G bipartitan graf, njegov hromatski broj je 2. Znamo da je $\mathrm{ch}(G) \geq \chi(G)$, pa hajde da ispitamo da li je i $\mathrm{ch}(G) = 2$.

Radi jednostavnijeg zapisa, boje obično označavamo brojevima. Neka važi $u_1 \in \{1, 2\}$, $u_2 \in \{3, 4\}$. Dalje, neka $v_1 \in \{1, 3\}$, $v_2 \in \{1, 4\}$, $v_3 \in \{2, 3\}$ *i* $v_4 \in \{2, 4\}$.

Tada, kakav god izbor napravimo za čvorove u_1 *i* u_2, bar jedan od čvorova iz skupa V će biti obojen u istu boju kao jedan od čvorova iz U, jer imamo tačno 4 dostupne boje, i tačno 4 čvora u skupu V. Time smo pokazali da je $\mathrm{ch}(G) > \chi(G) = 2$.

Tvrdimo da je $\mathrm{ch}(G) = 3$. Naime, ako imamo za svaki čvor listu od po 3 boje, uvijek možemo dva čvora iz skupa U obojiti u neke proizvoljne, a sva četiri čvora skupa V u onu jednu preostalu. Time smo pokazali da je $\mathrm{ch}(G) = 3$.

Primjer 3.49. Za bipartitni graf $G = K_{3,27}$ pokazati da je $\mathrm{ch}(G) > 3$.

Ponovo, kako je G bipartitan graf važi $\chi(G) = 2$. Takođe, znamo da je $\mathrm{ch}(G) \geq \chi(G) = 2$. Pokazaćemo da je $\mathrm{ch}(G) \geq 4$.

U tu svrhu posmatrajmo sliku 3.2, i neka je svakom čvoru pridružena lista od po 3 moguće boje baš kao na slici.

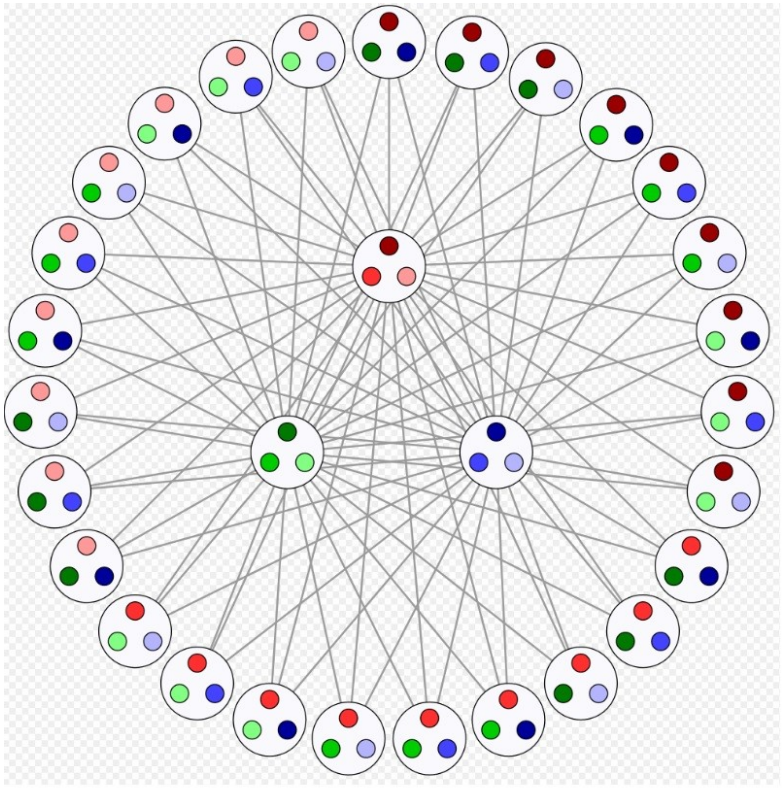
Tada možemo donijeti isti zaključak kao i u prethodnom primjeru. Naime, kako god da izaberemo boje za 3 centralna čvora, bar jedan od preostalih čvorova će biti iste te boje. Stoga je

$$\mathrm{ch}(G) \geq 4,$$

što je i trebalo dokazati.

Naime, nije teško pokazati da za svako $k \geq 2$ postoji neki bipartitni graf G za koji je $\mathrm{ch}(G) > k$.

Takođe važi i sljedeći rezultat, koji je dokazao Alon.



Slika 3.2. Graf $K_{3,27}$

Teorema 3.50. *([13]) Za svaki prirodan broj k postoji neka konačna vrijednost $c(k)$ takva da svi prosti grafovi čiji je minimalni stepen čvorova bar $c(k)$ imaju odabirni broj koji je strogo veći od k.*

Za razliku od bipartitnih grafova, kod kojih smo pronašli jednostavne primjere koji pokazuju da postoje grafovi čiji je odabirni broj strogo veći od hromatskog broja grafa, za linijski graf se čvrsto vjeruje da važi sljedeća hipoteza.

Hipoteza 3.51. *Za svaki graf G je ispunjeno* $\mathrm{ch}'(G) = \chi_1(G)$.

Hipotezu su postavili mnogi naučnici nezavisno jedni od drugih, a prvi put se javlja u radu ([18]) iz 1985. Danas je još uvijek otvoren problem, iako su dokazani neki specijalni slučajevi.

3.7.1 Kriterijum bojenja Alona i Tarsija

Sada imamo sav potreban alat za jednu važnu teoremu iz ove oblasti koju ćemo detaljno dokazati. Naime, riječ je o kriterijumu bojenja grafa G koji se bazira na svim mogućim orijentacijama tog grafa. To je rezultat do koga su došli Alon i Tarsi u radu [4]. Mi ćemo ga ovdje dokazati na dva načina, pri čemu je prvi znatno komplikovaniji i zahtijeva mnogo pomoćnih rezultata, a drugi je jednostavna posljedica Kombinatornog „Nullstellensatza".

Uvedimo oznake:

1. EE(D): broj parnih Ojlerovih podgrafova digrafa D (graf je paran ako ima paran broj grana);
2. EO(D): broj neparnih Ojlerovih podgrafova digrafa D,

a neka je prazan graf i paran i Ojlerov podgraf.

Za ovako uvedene oznake važi sljedeća teorema.

Teorema 3.52. *Neka je dat neusmjeren graf $G = (V, E)$ i neka su njegovi čvorovi $V = \{v_1, v_2, ..., v_n\}$. Označimo sa $D = (V, E)$ digraf kojim je data orijentacija grafa G i definišimo funkciju*

$$f : V \to \mathbb{Z} \ sa \ f(v_i) = d_i + 1,$$

gdje je $d_i = |O_D(v_i)|$, za sve $i = 1, ..., n$. Tada važi sljedeća implikacija:

$$EE(D) \neq EO(D) \implies D \text{ je } f\text{-birljiv.}$$

Prvi korak u dokazu ove teoreme je pomoćna lema koja će nam dati način da polinom grafa G (definicija 3.29) izrazimo pomoću orijentacije njegovih grana. Prisjetimo se, polinom grafa $G = (V, E)$ je definisan sa:

$$f_G(x_1, ..., x_n) = \prod_{i<j, \{v_i, v_j\} \in E(G)} (x_i - x_j).$$

Neka je dat graf $G = (V, E)$ i neka su $V = \{v_1, ..., v_n\}$ njegovi čvorovi. Ako je graf G neusmjeren, označimo sa D neku njegovu orijentaciju. Za svaku usmjerenu granu $e = (v_i, v_j)$, definišimo njenu težinu $w(e)$ sa:

$$w(e) = x_i \text{ ako je } i < j \text{ i } w(e) = -x_i \text{ ako je } i > j.$$

Težina digrafa D, u oznaci $w(D)$, je definisana kao $\prod_{e \in E} w(e)$, gdje proizvod ide kroz sve usmjerene grane digrafa D.

Uočimo da je tada

$$f_G = \sum w(D),$$

gdje D prolazi kroz sve moguće orijentacije grafa G, zato što svaki član proizvoda

$$f_G(x_1, ..., x_n) = \prod_{i<j, \{v_i, v_j\} \in E(G)} (x_i - x_j),$$

odgovara izboru neke orijentacije grane $\{v_i, v_j\}$, i tako za sve grane grafa G.

Dalje, za usmjerenu granu (v_i, v_j) kažemo da je opadajuća ako je $i > j$, a za orijentaciju D grafa G da je parna ako ima paran broj opadajućih grana, u suprotnom je neparna. Primijetimo da ako digraf D ima parnu orijentaciju, to znači da ima paran broj opadajućih grana, a kako je težina svake opadajuće grane $e = (v_i, v_j)$ data sa $w(e) = -x_i$, taj paran broj minusa će se poništiti i dobićemo da je $w(D)$ monom obila $\prod_i x_i$. Dakle, koeficijent uz dati monom je 1 u digrafu parne orijentacije. Slično, ako je digraf neparne orijentacije taj koeficijent će biti -1.

Neka je d_i definisano kao u teoremi 3.52 i označimo sa $DE(d_1, ..., d_n)$ i $DO(d_1, ..., d_n)$ skupove svih parnih i neparnih orijentacija grafa G. U prethodnom pasusu smo pokazali da važi sljedeća lema.

Lema 3.53.

$$f_G(x_1, ..., x_n) = \sum_{d_1, ..., d_n \geq 0} \Big(|DE(d_1, ..., d_n)| - |DO(d_1, ..., d_n)| \Big) \prod_{i=1}^{n} x_i^{d_i}.$$

U sljedećem koraku dokazujemo jednu posljedicu ove leme, koja će nam također biti potrebna.

Posljedica 3.54. *Neka je dat neusmjeren graf $G = (V, E)$ i neka su njegovi čvorovi $V = \{v_1, ..., v_n\}$. Označimo sa D neku orijentaciju grafa G i sa $d_i = |O_D(v_i)|$ za sve $v_i \in V$. Tada je apsolutna vrijednost koeficijenta koji stoji uz monom $\prod_{i=1}^{n} x_i^{d_i}$ u standardnoj reprezentaciji polinoma f_G baš $|EE(D) - EO(D)|$. Dakle, ako je $EE(D) \neq EO(D)$, onda je pomenuti koeficijent različit od nule.*

Dokaz. Neka je D_1 neka fiksna orijentacija iz $DE(d_1, ..., d_n) \cup DO(d_1, ..., d_n)$, gdje je $d_1, d_2, ..., d_n$ neki fiksiran niz nenegativnih cijelih brojeva. Za neku proizvoljnu orijentaciju D_2 iz istog skupa, definišemo $D_1 \oplus D_2$ kao podgraf grafa D_1, koji smo izdvojili tako što smo izabrali sve grane iz D_1 koje u digrafu D_2 imaju suprotnu orijentaciju. Kako svaki čvor v_i ima izlazni stepen d_i u oba digrafa D_1 i D_2, dobijamo da je definisani graf $D_1 \oplus D_2$ Ojlerov. Dalje,

$D_1 \oplus D_2$ je paran Ojlerov graf ako i samo ako su D_1 i D_2 oba parna ili oba neparna digrafa. Možemo definisati preslikavanje

$$DE(d_1, ..., d_n) \cup DO(d_1, ..., d_n) \to \text{skup Ojlerovih podgrafova grafa } D_1,$$

koje je bijekcija i u našem slučaju slika D_2 u $D_1 \oplus D_2$. Ako je D_1 paran digraf, onda ovo preslikavanje slika sve parne orijentacije u parne Ojlerove podgrafove grafa G, a neparne orijentacije u neparne podgrafove. Ako je D_1 neparan digraf, onda slika sve neparne orijentacije u parne Ojlerove podgrafove, a za parne pak u neparne podgrafove. Kakve god parnosti je fiksiran digraf D_1, možemo zaključiti da važi:

$$\big||DE(d_1, ..., d_n)| - |DO(d_1, ..., d_n)|\big| = |EE(D_1) - EO(D_1)|.$$

Sada ako iskoristimo prethodnu lemu, dobijemo da je koeficijent uz monom $\prod_{i=1}^{n} x_i^{d_i}$ zaista

$$|EE(D_1) - EO(D_1)|,$$

što je i trebalo pokazati. □

Sada imamo sav potreban alat za dokaz teoreme 3.52.

Dokaz. Neka je dat neusmjeren graf $G = (V, E)$ čiji je skup čvorova $V = \{v_1, ..., v_n\}$ i neka je D neka njegova orijentacija. Pridružimo svakom čvoru v_i listu od $d_i + 1$ različitih boja (to radimo pomoću funkije f), gdje je d_i definisano u formulaciji teoreme, i označimo tu listu sa S_i za $i = 1, ..., n$. Pretpostavimo da je $EE(D) \neq EO(D)$. Treba pokazati da postoji pravilno bojenje čvorova grafa G koje bi svakom čvoru dodijelilo neku boju sa njemu pridružene liste.

Primijetimo da, ako pretpostavimo da takvo bojenje $c : v_i \to c(v_i) \in S_i$ postoji za sve $i = 1, ..., n$, onda, ako je f_G polinom pridružen grafu G, važi

$$f(c(v_1), ..., c(v_n)) = \prod_{i<j,\, \{v_i, v_j\} \in E(G)} (c(v_i) - c(v_j)) \neq 0, \tag{3.28}$$

jer su svaka dva povezana čvora obojena različitom bojom pri pravilnom bojenju.

Pretpostavićemo da takvo bojenje ne postoji, te je stoga na osnovu (3.28) to ekvivalentno uslovu

$$f_G(x_1, ..., x_n) = 0 \text{ za sve } n\text{-torke } (x_1, ..., x_n) \in S_1 \times ... \times S_n.$$

Definišimo za svako $i = 1, ..., n$ sljedeći polinom:

$$Q_i(x_i) = \prod_{s \in S_i} (x_i - s) = x_i^{d_i+1} - \sum_{0}^{d_i} q_{ij} x_i^j.$$

Primijetimo da je $\forall x_i \in S_i,\ Q_i(x_i) = 0$, odnosno

$$x_i^{d_i+1} = \sum_0^{d_i} q_{ij} x_i^j.$$

Dakle, kada god se javi x_i^m, gdje je $m \geq d_i + 1$, možemo ga zapisati kao sumu monoma u kojima je najveći stepen x_i baš d_i. Upravo smo opisali postupak kojim se od polinoma f_G dobija polinom $\tilde{f_G}$ u kome je sada najveći stepen promjenljive x_i baš d_i za sve $i = 1, ..., n$.

Takođe, primijetimo da je

$$f_G(x_1, ..., x_n) = \tilde{f_G}(x_1, ..., x_n)$$

za sve $(x_1, ..., x_n) \in S_1 \times ... \times S_n$. Zato je i $\tilde{f_G}(x_1, ..., x_n) = 0$ za sve $(x_1, ..., x_n) \in S_1 \times ... \times S_n$. Tada je na osnovu leme 2.1 $\tilde{f_G} \equiv 0$.

Sa druge strane, kako je $EE(D) \neq EO(D)$, iz posljedice 3.54 slijedi da je koeficijent uz monom $\prod_{i=1}^n x_i^{d_i}$ u polinomu f_G različit od nule. Međutim, primijetimo da je koeficijent uz pomenuti monom isti u oba polinoma f_G i $\tilde{f_G}$, zato što se pri postupku dobijanja polinoma $\tilde{f_G}$ samo smanjuje stepen polinoma i neće nastati neki novi umnožak monoma $\prod_{i=1}^n x_i^{d_i}$. Time smo dobili da bar jedan monom u polinomu $\tilde{f_G}$ ima koeficijent različit od nule, što je u kontradikciji sa našim zaključkom da je $\tilde{f_G} \equiv 0$.

Dakle, pretpostavka je bila pogrešna i opisano bojenje postoji, što je i trebalo dokazati.

□

Pažljivi čitalac je sigurno primijetio da se u ovom dokazu koristi ista algebarska tehnika kao u dokazu samog Kombinatornog „Nullstellensatza" tj. teoreme 2.2. To je razlog zašto je dokaz koji slijedi direktan i znatno kraći.

Dokaz. Neka su date iste oznake kao u prvom dokazu. Vidjeli smo da je postojanje traženog bojenja ekvivalentno sa uslovom da postoji izbor boja $c(v_i) \in S_i$ za sve $i = 1, ..., n$, tako da je

$$f_G = (c(v_1), ..., c(v_n)) \neq 0. \tag{3.29}$$

Primijetimo da je $|S_i| = d_i + 1$ i $\deg(f_G) = \sum_{i=1}^n d_i$, a iz posljedice 3.54 slijedi da je koeficijent uz $\prod_{i=1}^n x_i^{d_i}$ različit od nule. Kako su sada ispunjeni uslovi Kombinatornog „Nullstellensatza" 2.3, dobijamo da postoje neki $c(v_i) \in S_i$, za sve $i = 1, ..., n$, za koje je isunjeno (3.29). Time je dokaz završen. □

U radu [4] se mogu pronaći tri direktne posljedice teoreme koju smo upravo dokazali. Mi ćemo ovdje predstaviti nekoliko rezultata, do čijeg dokaza se došlo zahvaljujući ovoj teoremi.

Problem o konturi i trouglovima

Prvi rezultat je poznat kao problem o konturi i trouglovima (eng. cycle plus triangles–problem). Naime, riječ je o problemu koji je formulisao Erdős na jednoj konferenciji 1990, a dokaz su dali H. Fleischner[24] i M. Stiebitz[25] 1991. u svom radu [33], upravo koristeći teoremu 3.52.

Teorema 3.55. *Neka je $n \in \mathbb{N}$ i neka je G 4-regularan graf sa $3n$ čvorova. Pretpostavimo da je skup njegovih grana disjunktna unija Hamiltonove konture i n trouglova koji su svi čvorno disjunktni. Tada je $\chi(G) = ch(G) = 3$.*

U ključnom dijelu dokaza se pokazuje da, ako pridružimo grafu G digraf D koji je dobijen tako što smo usmjerili Hamiltonovu konturu kao i svaki od trouglova ciklično, tada važi

$$EE(D) - EO(D) \equiv 2 \pmod 4.$$

Onda je $EE(D) \neq EO(D)$, pa rezultat slijedi iz teoreme 3.52.

Odabirni broj planarnog bipartitnog grafa

Sljedeći rezultat koji ćemo predstaviti je ponovo odgovor na jedan otvoren problem koj su Erdős, Rubin i Taylor formulisali u radu [32]. Naime, oni su postavili sljedeću hipotezu o planarnim grafovima.

Hipoteza 3.56. *Svaki planaran graf je 5-birljiv.*

Međutim, Alon i Tarsi su u [4] pokazali sljedeći rezultat i to pomoću teoreme 3.52.

Teorema 3.57. *Svaki planaran bipartitan G graf je 3-birljiv ($ch(G) \leq 3$).*

Daćemo nekoliko koraka kako su došli do ovog rezultata, a detalji se mogu pogledati u [4].

Za dati graf $G = (V, E)$ prvo definišemo vrijednost $L(G)$ kao

$$L(G) = \max\big(|E(H)|/|V(H)|\big),$$

[24] Herbert Fleischner (1944–), austrijski matematičar

[25] Michael Stiebitz, njemački matematičar

gdje maksimum ide po svih mogućim podgrafovima H grafa G. Jednostavnije rečeno, vrijednost $L(G)$ interpretiramo kao polovinu maksimalne vrijednosti prosječnog stepena čvorova u podgrafovima grafa G. Za uvedene oznake, važi sljedeća lema čiji dokaz se može pronaći u [57], a spominje se i u [14].

Lema 3.58. *Graf $G = (V, E)$ ima orijentaciju D u kojoj je $|O_D(v)| \leq d$ za svako $v \in V(G)$ ako i samo ako je $L(G) \leq d$.*

Važi i sljedeća teorema, u kojoj ćemo vidjeti primjenu teoreme 3.52.

Teorema 3.59. *Za svaki bipartitan graf G je $ch(G) \leq (\lceil L(G) \rceil + 1)$.*

Dokaz. Neka je dat graf $G = (V, E)$ i neka je $d = \lceil L(G) \rceil$, odnosno važi $L(G) \leq d$. Tada na osnovu leme 3.58 slijedi da postoji neka orijentacija grafa G, u oznaci D, takva da je maksimalan izlazni stepen svakog čvora baš d. Kako je G bipartitan graf, na osnovu teoreme 3.38 slijedi da G, pa ni D, nema neparne konture, te je stoga $EE(D) \neq EO(D)$. To je zato što je $EE(D) \geq 1$, jer smo rekli da je prazan graf po dogovoru i paran i Ojlerov. Sada tvrđenje slijedi iz teoreme 3.52. □

Da bismo pokazali da je teorema 3.57, posljedica upravo dokazane teoreme, potreban nam je još jedan rezultat iz teorije grafova koji slijedi iz poznate Ojlerove formule.

Teorema 3.60. *(Euler[26] (1752)) Neka je graf $G = (V, E)$ planaran sa v čvorova i e grana. Označimo sa f broj povezanih oblast na koje G dijeli ravan. Tada je*

$$f - e + v = 2.$$

Posljedica 3.61. *Neka je $G = (V, E)$ povezan, prost, planaran graf sa v čvorova ($v \geq 3$), e grana i f oblasti. Ako G nema konturu dužine 3, onda je*

$$e \leq 2v - 4.$$

Dokaz. Za svaku oblast možemo definisati njen stepen kao dužinu konture koja ograničava datu oblast. Uočimo da je zbir stepeni svih oblast jednak dvostrukom broju grana. Pri tome je svaka oblast stepena bar 4, jer nemamo konture dužine 3. Odatle dobijamo da je $2e \geq 4f$, odnosno $\frac{1}{2}e \geq f$. Ako Ojlerovu formulu zapišemo kao $f = 2 + e - v$, i iskoristimo dobijenu nejednakost, dobijamo

$$e - v + 2 \leq \frac{1}{2}e \implies e \leq 2v - 4,$$

što je i trebalo pokazati. □

[26]Leonhard Euler (1707–1783), švajcarski matematičar i fizičar

Sada imamo potreban alat za dokaz teoreme 3.57.

Dokaz. Neka je dat graf $G = (V, E)$, sa v čvorova i e grana, koji je planaran i bipartitan. Treba pokazati da je $\mathrm{ch}(G) \leq 3$.

Bez umanjena opštosti možemo pretpostaviti da je graf G povezan, jer ako nije, možemo primijeniti isti postupak za svaku komponentu povezanosti. Na osnovu posljedice 3.61 slijedi da G ima najviše $2v - 4$ grane. Odatle dobijamo da je $L(G) \leq 2$. Sada kada iskoristimo teoremu 3.59, dobijamo da je $\mathrm{ch}(G) \leq 3$, što je i trebalo pokazati. □

Odabirni broj linijskog grafa

Kao što smo vidjeli do sada, kriterijum bojenja Alona i Tarsija je vrlo moćan alat koji je riješio dosta otvorenih problema u ovoj oblasti. Zato su Jaeger i Tarsi probali pokazati hipotezu 3.51 o linijskim grafovima baš pomoću pomenutog alata.

U nastavku ćemo dati do kog rezultata su došli i skicu toga šta su sve uradili usput, a za više detalja pogledati [13] i [38].

Prvo su pokušali izraz $EE(D) - EO(D)$ napisati na neki zgodniji način. U tu svrhu su posmatrali linijski graf grafa G koji je d-regularan i takav da je $\chi_1(G) = d$. Linijski graf takvog grafa $L(G)$ je onda $(2d-2)$-regularan, jer je svaki njegov čvor zapravo neka grana grafa G, a 2 čvora su povezana ako odgovarajuće grane u G imaju zajednički čvor. Kako svaka grana u G dijeli jedan krajnji čvor sa još $d - 1$ grana, a isto tako i na drugom kraju, slijedi da svaki čvor u grafu $L(G)$ ima $2d - 2$ susjeda. Neka je D orijentacija grafa $L(G)$ tako da

$$\forall v \in V(L(G)) \text{ je } |O_{L(G)}(v)| = |I_{L(G)}(v)| = d - 1.$$

Neka je $f_D(x_1, ...)$ polinom grafa D i označimo sa $C(D)$ koeficijent koji stoji uz monom $\prod_i x_i^{d-1}$. Na osnovu posljedice 3.54 znamo da je

$$|C(D)| = |EE(D) - EO(D)|.$$

Potom su pokazali da se izraz sa desne strane može posmatrati kao suma koja ide po svim pravilnim d-bojenjima grana grafa G, gdje se pod sumom nalaze tzv. znakovi bojenja (definicija ovog pojma je tehnička i ovdje u skici dokaza je izostavljamo, a detalji se mogu vidjeti u [13]).

Koristili su i sljedeći poznat rezutat, čiji dokaz se može pronaći u [38].

Teorema 3.62. *([61]) Neka je graf $G = (V, E)$ planaran i 3-regularan i neka je njegov hromatski indeks 3. Tada sva pravilna 3-bojenja grana grafa G imaju isti znak.*

Takođe su koristili dobro poznatu činjenicu da je Teorema o četiri boje ekvivalentna sa teoremom Taita (1880) koja tvrdi da svaki 2-povezan, 3-regularan planaran graf ima hromatski indeks 3. Dokaz ove ekvivalencije se može pronaći u [66].

Kombinujući sve ove rezultate, pokazali su teoremu koja slijedi.

Teorema 3.63. *Svaki 2-povezan, 3-regularan, planaran graf ima odabirni broj 3.*

3.7.2 Ideali polinoma

U ovom odjeljku ćemo predstaviti 3 rezultata koja tvrde da graf G ima određeno svojstvo ako njemu odgovarajući polinom f_G (definicija 3.29), leži u nekom idealu. Jedan od tih rezultata ćemo i dokazati koristeći Kombinatorni „Nullstellensatz".

Prvo ćemo se podsjetiti definicije ideala.

Definicija 3.38. Neka je R proizvoljan prsten. Kažemo da je $I \subseteq R$ ideal ako je $I \leq R$ (I je potprsten od R) i ispunjen je sljedeći uslov:

$$\forall r \in R,\ s \in I \text{ važi da } r \cdot s \in I.$$

Teorema 3.64. *([43]) Graf $\overline{K}_{k+1}$ nije podgraf grafa G ako i samo ako polinom f_G leži u idealu I generisanom svim polinomima koji odgovaraju grafovima koji su unija k čvorno disjunktnih kompletnih grafova, tako da tom unijom pokrijemo sve čvorove grafa G.*

Teorema 3.65. *([44],[45]) Graf G nije k-obojiv ako i samo ako polinom f_G leži u idealu generisanom svim polinomima $f_{K_{k+1}}$ koji odgovaraju kompletnim grafovima K_{k+1}.*

Teorema 3.66. *([4]) Neka je $G = (V, E)$ graf sa n čvorova i označimo ih sa $1, 2, ..., n$. Tada G nije k-obojiv ako i samo polinom f_G leži u idealu koji je generisan polinomima*

$$p_i(x_i) = x_i^k - 1,\ \ za\ \ i = 1, ..., n.$$

Dokaz. Pretpostavimo da graf $G = (V, E)$ nije k-obojiv. Treba da pokažemo da f_G leži u opisanom idealu.

Primijetimo da su nule polinoma p_i zapravo k-ti korijeni iz jedinice. Ima ih tačno k i to su

$$e^{\frac{2s\pi i}{k}} = \cos\left(\frac{2s\pi}{k}\right) + i\sin\left(\frac{2s\pi}{k}\right) \ \text{ za } \ s = 0, ..., k-1.$$

Za nastavak dokaza nam neće biti bitan ovaj oblik, nego samo činjenica da ih ima k, pa ćemo ih označiti sa $c_1, ..., c_k$, a skup koji ih sve sadrži sa C.

Kako smo pretpostavili da G nije k-obojiv, svako bojenje $c : V(G) \to C$ će biti takvo da će neka dva susjedna čvora biti obojena istom bojom. Odnosno, biće ispunjeno

$$f_G(c(x_1), ..., c(x_n)) = 0.$$

Dakle, polinom f_G se anulira nad k-tim korijenima iz 1, odnosno baš nad zajedničkim nulama polinoma p_i. Tada na osnovu Kombinatornog „Null-stellensatza" tj. teoreme 2.2, slijedi da je f_G linearna kombinacija polinoma p_i za $i = 1, ..., n$, odnosno f_G leži u idealu koji je njima generisan, što je i trebalo pokazati.

U suprotnom smjeru, dokaz ide vrlo slično. Naime, ako pretpostavmo da f_G leži u opisanom idealu, onda su njegove nule baš k-ti korijeni iz 1. To znači da ako definišemo neko bojenje koje čvorovima grafa G dodjeljuje neki k-ti korijen, polinom grafa G će imati vrijednost nula, što znači da će neka dva susjedna čvora biti obojena istom bojom, Dakle, graf G nije k-obojiv, što je i trebalo dokazati u ovom smjeru. Time je dokaz završen.

□

Primijetimo da je ovo prvi put da smo u radu koristili Kombinatorni „Nullstellensatz" 1 tj. teoremu 2.2.

3.7.3 Propusnost grafa

U ovom odjeljku ćemo predstaviti još jedan rezultat koji tvrdi da graf ima određeno svojstvo ako dati polinom pripada nekom idealu. Samo što dati polinom nije polinom grafa, nego polinom koji je posebno definisan tako da nas dovede do željenog ishoda. Zato smo ovaj rezultat izdvojili u posebnu cjelinu.

Zamislimo da imamo problem koji od nas zahtijeva da za dati graf na optimalan način pridružimo njegovim čvorovima različite brojeve, ili skupove elemenata, tako da neki uslov bude zadovoljen. Ovo je problem označavanja grafova i jednom tipu tog problema ćemo posvetiti posebnu pažnju. Više informacija o ovakvim i sličnim problemima se može pronaći u [22].

Jedan vid označavanja grafa jeste svakako dodijeljivanje određenih boja njegovim čvorovima ili dodijeljivanje nekog broja svakom čvoru. Takav je i problem propusnosti grafa, koji dajemo u sljedećoj definiciji.

Definicija 3.39. Neka je dat graf $G = (V, E)$ sa n čvorova. Propusnost grafa G je najmanja vrijednost k takva da postoji bijekcija $f : V \to \{1, 2, ..., n\}$ tako da je

$$|f(u) - f(v)| \leq k, \ \ \forall uv \in E.$$

Označimo propusnost grafa sa $b(G)$.

Teorema koja slijedi daje potreban i dovoljan uslov da propusnost grafa G bude bar $k+1$, za neki prirodan broj k. Nastavljamo u duhu prethodnog odjeljka, jer će ponovo taj uslov biti zadovoljen ako određeni polinom pripada nekom idealu.

Teorema 3.67. *Neka je dat graf $G = (V, E)$ sa n čvorova $V = \{1, 2, ..., n\}$. Tada je $b(G) \geq k+1$ ako i samo ako polinom*

$$Q_{G,k}(x_1, ..., x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \prod_{ij \in E, i<j} \prod_{k<|l|<n} (x_i - x_j - l)$$

pripada idealu koji je generisan polinomima $g_i(x_i) = \prod_{j=1}^{n}(x_i - j)$, za sve $i = 1, ..., n$.

Dokaz. Prvo pretpostavimo da $Q_{G,k}$ pripada opisanom idealu. Treba pokazati da je $b(G) > k$. Sada umjesto promjenljivih $x_1, ..., x_n$ u polinomima g_i uvrstimo brojeve $1, ..., n$, nebitno kojim redom, ali tako da svi x_i budu različiti. Na taj način ćemo dobiti n-torku $(x_1, ..., x_n)$ takvu da je $g_1(x_1) = g_2(x_2) = ... = g_n(x_n) = 0$. Kako je polinom $Q_{G,k}$ linearna kombinacija polinoma g_i, za $i = 1, ..., n$, slijedi da je i

$$Q_{G,k}(x_1, ..., x_n) = 0.$$

Kako smo izabrali vrijednosti tako da je $x_i \neq x_j$, za $i \neq j$, slijedi da je prvi proizvod u polinomu $Q_{G,k}$ različit od nule. Stoga drugi proizvod mora biti jednak nuli, tj. postoji neka grana $ij \in E$ tako da je

$$|x_i - x_j| = |l| > k.$$

Time smo pokazali da je $b(G) > k$.

U drugom smjeru, pretpostavimo da je $b(G) > k$. Treba pokazati da $Q_{G,k}$ pripada opisanom idealu, što je ekvivalentno sa:

$$Q_{G,k}(x_1, ..., x_n) = 0, \text{ kada } x_i \in \{1, 2, ..., n\} \text{ za sve } i = 1, ..., n.$$

Ako je slučajno $x_i = x_j$, za neke $i, j \in \{1, 2, ..., n\}$, gdje $i \neq j$, onda

$$\prod_{1 \leq i < j \leq n} (x_i - x_j) = 0,$$

pa je i $Q_{G,k}(x_1, ..., x_n) = 0$, što je i trebalo pokazati. U suprotnom, za neko $x_i \in \{1, ..., n\}$ postoji neko x_j gdje je $ij \in E$ tako da je $|x_i - x_j| > k$, zbog pretpostavke da je $b(G) > k$. U ovom slučaju je

$$\prod_{ij \in E, i<j} \prod_{k<|l|<n} (x_i - x_j - l) = 0,$$

što nas opet dovodi do zaključka da je $Q_{G,k}(x_1, ..., x_n) = 0$. Time je dokaz završen. □

3.7.4 Bojenje hipergrafa

Ako u definiciji grafa dopustimo da svaka grana e bude incidentna sa skupom čvorova V_e, gdje je $|V_e| \geq 2$, onda dobijemo hipergraf.

Definicija 3.40. Hipergraf H je par (V, E), gdje V predstavlja konačan skup čije elemente nazivamo čvorovi hipegrafa, a E je skup nekih podskupova skupa V i njegove elemente nazivamo grane ili ivice.

Definicija 3.41. Hipergraf $H = (V, E)$ je k-uniforman ako su svi elementi skupa E skupovi kardinalnosti k, odnosno ako je svaka grana incidentna sa tačno k čvorova.

Hipergraf koji je 2-uniforman je takav da mu je svaka grana incidentna sa tačno 2 čvora. Dakle, u pitanju je običan graf.

Definicija 3.42. Hipergraf $H = (V, E)$ je k-obojiv ako postoji bojenje njegovih čvorova u k ili manje boja tako da nijedna grana nije monohromatska tj. jednobojna (gdje za granu kažemo da je jednobojna ako su svi čvorovi incidentni sa tom granom obojeni istom bojom).

Stoga je pravilno bojenje hipergrafa svako bojenje koje boji njegove čvorove tako da ne postoji grana čiji su svi čvorovi obojeni istom bojom.

Više o bojenju hipergrafa se može pronaći u [20].

Teorema koja slijedi daje potreban i dovoljan uslov da 3-uniforman hipergraf ne bude 2-obojiv.

Teorema 3.68. *Neka je $H = (V, E)$ 3-uniforman hipergraf. Tada H nije 2-obojiv ako i samo ako polinom*

$$g_H = \prod_{e \in E} \left(\Big(\sum_{v \in e} x_v \Big)^2 - 9 \right)$$

pripada idealu koji je generisan polinomima

$$p_v = x_v^2 - 1, \;\; za \;\; \forall v \in V.$$

Dokaz. Pretpostavimo da je H 3-uniforman hipergraf koji nije 2-obojiv. To znači da ako obojimo čvorove $V(H)$ u 2 boje koje ćemo označiti sa 1 i -1, mora postojati neka grana $\tilde{e}$ čija su sva 3 čvora iste boje (svaka grana ima 3

čvora jer je H 3-uniforman). Bez umanjena opštosti neka je to boja označena sa 1. Pridružimo svakom čvoru v neku promjenljivu x_v. Tada imamo da je

$$\Big(\sum_{v\in\tilde{e}} x_v\Big)^2 = 3^2 = 9.$$

Primijetimo da nije bitno da li su čvorovi sa grane $\tilde{e}$ obojeni bojom označenom sa 1 ili -1. Zbog kvadrata koji se javlja, dobijamo istu vrijednost u oba slučaja.

Dakle, dobili smo da se g_H anulira kada god za x_v uzmemo 1 ili -1, a kako su to baš nule polinoma p_V, za $v \in V$, iz Kombinatornog „Nullstellensatza" tj. teoreme 2.2 slijedi da dati polinom pripada idealu generisanom polinomima p_v, za sve $v \in V$.

Obratno, neka g_H pripada opisanom idealu. Tada je

$$g_H = 0 \text{ kada } x_v \in \{-1, 1\}, \text{ za } \forall v \in V.$$

Slijedi da je za neko $e \in E$

$$\Big(\sum_{v\in e} x_v\Big)^2 = 9,$$

što je moguće samo ako su sva 3 čvora na grani e iste boje. Dakle, postoji jednobojna grana, pa H nije 2 obojiv. □

Teorema koja slijedi je uopštenje prethodne teoreme i riječ je o rezultatu iz 2019. Yulia Alexandr je u radu [2] formulisala potreban i dovoljan uslov da m-uniforman hipergraf ne bude k-obojiv.

Teorema 3.69. *Neka je $H = (V, E)$ m-uniforman hipergraf. Tada H nije k-obojiv ako i samo ako polinom*

$$g_H = \prod_{e\in E}\Big(\Big(\sum_{v\in e} x_v\Big)^k - m^k\Big)$$

pripada idealu koji je generisan polinomima

$$p_v = x_v^k - 1, \text{ za } \forall v \in V.$$

Dokaz. Pretpostavimo da je H m-uniforman hipergraf koji nije k-obojiv. Obojimo sada čvorove tog hipergrafa sa k boja koje ćemo označiti sa k-tim korijenima iz 1. Kako H nije k-obojiv, slijedi da postoji neka grana $\tilde{e}$ koja je

jednobojna i neka je svih m čvorova na njoj obojeno bojom t (gdje je t neki k-ti korijen iz 1). Tada je

$$\Big(\sum_{v\in\tilde{e}} x_v\Big)^k = (m\cdot t)^k = m^k\cdot t^k = m^k.$$

Dakle, dobili smo da se polinom g_H anulira kada god za promjenljive x_v uzmemo k-te korijene iz 1. Kako su to baš nule polinoma p_v, za $v\in V$, iz Kombinatornog „Nullstellensatza", odnosno teoreme 2.2, slijedi da g_H pripada idealu generisanom polinomima p_v, što je i trebalo pokazati.

Obratno, pretpostavimo da g_H pripada opisanom idealu. Tada je

$$g_H = 0 \text{ kada je } x_v \text{ } k\text{-ti korijen iz 1, za sve } v\in V.$$

Posmatrajmo neko bojenje čvorova hipergrafa H u k boja koje ćemo redom označiti kao k-te korijene iz 1. Treba pokazati da H nije k-obojiv, stoga je dovoljno pokazati da postoji neka jednobojna grana.

Kako je $g_H = 0$, slijedi da postoji neka grana $\tilde{e}\in E$ tako da je

$$\Big(\sum_{v\in\tilde{e}} x_v\Big)^k = m^k.$$

Neka su $z_1,...,z_m$ boje koje su pridružene čvorovima sa grane $\tilde{e}$ i to su k-ti korijeni iz 1. Ako pokažemo da je $z_1 = ... = z_m$, završili smo, jer bismo tako pronašli jednobojnu granu koja svjedoči da H nije k-obojiv.

Pridružimo sada svakom k-tom korijenu z_i jedinični vektor w_{z_i} čija je početna tačka koordinatni početak, a krajnja z_i, i tako za sve $i = 1,...,m$. Kako je $(z_1+...+z_m)^k = m^k$, gdje su k i m prirodni brojevi, slijedi da je

$$|z_1+...+z_m|^k = |w_{z_1}+...+w_{z_m}|^k = m^k.$$

Pretpostavimo da je $z_i\neq z_j$, za neke $1\le i<j\le m$ i pokažimo da je tada $|w_{z_i}+w_{z_j}|<2$. Označimo sa θ ugao između vektora w_{z_i} i w_{z_j} i kako ti vektori nisu kolinearni, slijedi da je $\cos\theta<1$. Tada je

$$\begin{aligned}
|w_{z_i}+w_{z_j}| &= \sqrt{(w_{z_i}+w_{z_j})\cdot(w_{z_i}+w_{z_j})}\\
&= \sqrt{|w_{z_i}|^2+2w_{z_i}\cdot w_{z_j}+|w_{z_j}|^2}\\
&= \sqrt{|w_{z_i}|^2+2|w_{z_i}||w_{z_j}|\cos\theta+|w_{z_j}|^2}\\
&= \sqrt{2+2\cos\theta}\\
&< 2.
\end{aligned}$$

Sada imamo da je

$$\begin{aligned}|z_1 + ... + z_i + z_j + ... + z_m| &= |w_{z_1} + ... + wz_i + w_{z_j} + ... + w_{z_m}| \\ &\leq |w_{z_1}| + ... + |w_{z_i} + w_{z_j}| + ... + |w_{z_m}| \\ &= (m-2) \cdot 1 + |w_{z_i} + w_{z_j}| \\ &< m - 2 + 2 = m.\end{aligned}$$

Time smo došli u kontradikciju, jer smo dobili da je

$$|z_1 + ... + z_m|^k < m^k,$$

pa je jedina opcija da je $z_1 = z_2 = ... = z_m$. Tada je grana $\tilde{e}$ jednobojna, pa H nije k-obojiv, što je i trebalo pokazati. □

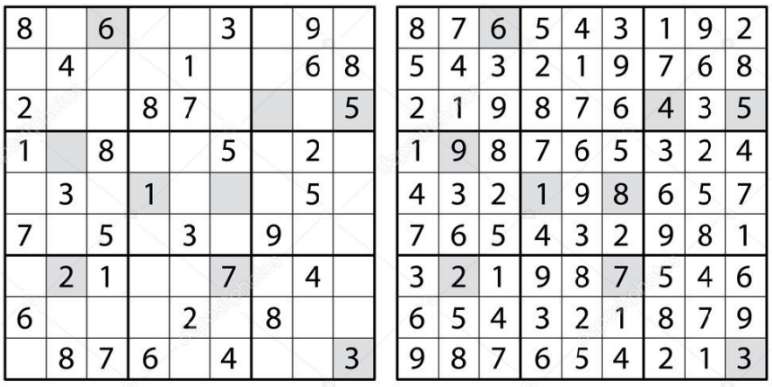
3.7.5 Sudoku u teoriji grafova

Yulia Alexandr je u pomenutom radu ([2]) pokazala još jednu vrlo zanimljivu primjenu teoreme 3.66 i Kombinatornog „Nullstellensatza". Riječ je o teoremi koja daje potreban i dovoljan uslov da sudoku bude rješiv.

Naime, poznata logička igra sudoku se može predstaviti kao problem iz oblasti bojenja grafova. Prvo ćemo objasniti pravila igre, a potom ćemo naći odgovarajuću interpretaciju tih pravila u teoriji grafova.

Klasičan sudoku se sastoji od 9 kolona i 9 redova, tj. mreže 9×9 koja je organizovana u 9 3×3 blokova, koja je djelimično ispunjena brojevima od 1 do 9. Cilj je popuniti ostatak mreže brojevima iz istog intervala, ali tako da se ni u jednoj koloni, redu ili bloku ne smiju javiti dva ista broja. Ako je moguće dopuniti mrežu tako da opisano pravilo bude ispunjeno, onda kažemo da je sudoku rješiv. Naglasimo da nije svaki sudoku rješiv, ali i da postoje oni koji imaju više rješenja. Za sudoku kažemo da je dobar ako ima jedinstveno rješenje.

Za svaki sudoku definišimo graf S koji mu odgovara. Kvadrate 1×1 u mreži 9×9 zovemo ćelijama i ima ih ukupno 81. Svaku ćeliju iz mreže interpretiramo kao čvor grafa S i kažemo da su dva čvora povezana ako i samo ako njima odgovarajuće ćelije leže u istoj koloni, redu ili bloku. Kako imamo 9 blokova, 9 kolona i 9 redova, njihovi elementi će u S formirati kompletne podgrafove K_9, kojih onda ukupno ima 27 i označimo ih sa $K_9^{(i)}$, za $i = 1, ..., 27$. Dopunjavanje djelimično popunjene mreže sada interpretiramo kao pravilno bojenje grafa S u tačno 9 boja, pri čemu su neki čvorovi unaprijed obojeni.



Slika 3.3. Početna mreža i riješen sudoku

Ako sa R označimo te unaprijed zadate restrikcije, označimo sa S_R graf S sa nekim čvorovima koji su unaprijed obojeni, prateći restrikcije iz R. Sada je sudoku rješiv ako i samo ako postoji pravilno bojenje grafa S_R u boje iz skupa $\{1, 2, ..., 9\}$.

Sada svakom čvoru $v \in V(S)$ dodijelimo promjenljivu x_v, a svakom kompletnom podgrafu $K_9^{(i)}$ odgovarajući polinom q_i, $i = 1, ..., 27$, gdje je

$$q_i = \prod_{\{v,w\} \in E(K_9^{(i)})} (x_v - x_w).$$

Još je preostalo razjasniti kako zadate restrikcije uključiti u priču o polinomima. Uzmimo neki proizvoljan čvor v čija boja je unaprijed zadata i primijetimo sa se taj čvor javlja u tačno 3 kompletna podgrafa, koje ćemo označiti sa $K_9^{(i1)}, K_9^{(i2)}$ i $K_9^{(i3)}$. Kako čvor v u grafu S odgovara jednoj ćeliji sa 9×9 mreže, on sa nekih preostalih 8 čini jedan blok, a to je u grafu S jedan kompletan podgraf, i slično sa preostalih 8 koji se nalaze u istoj koloni kao pomenuta ćelija formira drugi kompletna podgraf, i slično za treći sa preostalih 8 koji su u istom redu. Recimo da čvor v mora biti obojen bojom k_v. Tu restrikciju intepretiramo tako što u polinomima q_{i_j}, $j = 1, 2, 3$, koji odgovaraju trima gore pomenutim podgrafovima, umjesto promjenljive x_v koja odgovara čvoru v uvrstimo k_v i tako dobijeni polinom nazovimo f_{i_j}. Naravno, $f_i = q_i$, ako u podgrafu $K_9^{(i)}$ nema unaprijed zadatih restrikcija.

Odaberimo jednu bijekciju između skupa $\{1, 2, ..., 9\}$ i skupa koji sadrži sve devete korijene iz 1. Dakle, bojenje grafa S u 9 boja ili popunjavanje sudoku table sa devetim korijenima iz 1 možemo smatrati ekvivalentnim zadacima.

Za više detalja i rezultata koji povezuju sudoku i bojenje grafova pogledati [46], [47] i [21].

Sada imamo sav potreban alat da dokažemo teoremu koja daje čisto algebarski uslov kojim možemo provjeriti da li je sudoku rješiv ili ne.

Teorema 3.70. *Graf S_R nije 9-obojiv ako i samo ako polinom*

$$h_R = \prod_{i=1}^{27} f_i$$

pripada idealu generisanom polinomima

$$p_v = x_v^9 - 1, \ \ gdje \ \ v = 1, ..., 81.$$

Dokaz. Prvo pretpostavimo da S_R nije 9-obojiv. Tada, ako definišemo neko bojenje tog grafa u 9 boja koje ćemo označiti sa devetim korijenima iz 1, mora postojati grana čiji čvorovi su obojeni istom bojom. Dakle, za neko $i = 1, ..., 27$ će važiti $f_i = 0$, pa samim tim i $h_R = 0$. Time smo dobili da je $h_R(x_1, ..., x_{81}) = 0$ kada god za svih 81 promjenljivih uvrstimo neke devete korijene iz 1. Kako su to baš nule polinoma p_v, gdje $v = 1, ..., 81$, iz Kombinatornog „Nullstellensatza" 2.2 slijedi da h_R pripada idealu koji je generisan pomenutim polinomima.

U suprotnom smjeru, pretpostavimo da h_R pripada datom idealu, što znači da je

$$h_R(x_1, ..., x_{81}) = 0, \ \text{ kada god } \ x_i \in A \ \ za \ \ i = 1, ..., 81,$$

gdje smo sa A označili skup svih devetih korijena iz 1. Odatle slijedi da je za neko $i = 1, ..., 27$ polinom $f_i = 0$, što je moguće samo ako su neka dva susjedna čvora obojena istom bojom, gdje boje biramo iz skupa A. Stoga, ne postoji pravilno bojenje grafa S_R u 9 boja, te on nije 9-obojiv što je i trebalo pokazati. □

3.8 Pokrivanje tjemena hiperkocke

U ovom odjeljku ćemo predstaviti jedan zanimljiv rezultat koji spada u domen višedimenzionalne kombinatorne geometrije.

Definicija 3.43. Hiperravan u n-dimenzionalnom prostoru je potprostor dimenzije $n - 1$. Može biti opisana jednom linearnom jednačinom sljedećeg oblika:

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b,$$

gdje je bar jedno $a_i \neq 0$ za $1 \leq i \leq n$ i b je neka fiksirana vrijednost.

Definicija 3.44. Jedinična hiperkocka u n-dimenzionalnom prostoru je konveksna cjelina sa n tjemena, koja su takva da pripadaju skupu $\{0,1\}^n$.

Problem koji ćemo ovdje predstaviti je formulisao Bárány[27], a malo slabiju verziju Komjáth[28]. Više informacija o samom problemu se može pronaći u [41], a dokaz i još nekoliko povezanih rezultata u [12].

Teorema 3.71. *Neka je data familija hiperravni $H_1, H_2, ..., H_m$ u $\mathbb{R}^n$ koje pokrivaju sva tjemena jedinične hiperkocke $\{0,1\}^n$ osim jednog. Tada je broj potrebnih ravni $m \geq n$.*

Za originalni dokaz nam je potrebna jedna pomoćna lema.

Lema 3.72. *Neka je $Q = Q(x_1, ..., x_n)$ multilinearan polinom u $\mathbb{Z}[x_1, x_2, ..., x_n]$. Ako je $Q(\mathbf{0}) = c \neq 0$ i $Q(\boldsymbol{x}) = 0$ za sve $\boldsymbol{x} \in \{0,1\}^n \setminus \mathbf{0}$, onda je*

$$Q(x_1, x_2, ..., x_n) = c(1 - x_1)(1 - x_2)...(1 - x_n).$$

Specijalno, $deg(Q) = n$.

Dokaz. Definišimo

$$Q(\boldsymbol{x}) := \sum_{I \subset \{1,2,...,n\}} c_I \prod_{i \in I} x_i.$$

Ovako definisan polinom Q jeste linearan po svakoj promjenljivoj. Neka je

$$Q(\mathbf{0}) = c \neq 0 \ i \ Q(\boldsymbol{x}) = 0, \text{ za sve } \boldsymbol{x} \in \{0,1\}^n \setminus \mathbf{0}.$$

Treba pokazati da je $c_I = (-1)^{|I|}c$. Dokaz dajemo indukcijom po kardinalnosti skupa I.

Ako je $I = \emptyset$, onda je $c_\emptyset = c = Q(\mathbf{0})$. Sada neka je $|I| \geq 1$ i pretpostavimo da tvrđenje važi za sve podskupove $J \subset I$, $J \neq I$ i pokažimo da važi i za I. Označimo sa $e(I) \in \{0,1\}^n$ vektor čija je i-ta koordinata 1 ako i samo ako $i \in I$, a inače je nula. Kako je $|I| \geq 1$, bar jedna koordinata vektora e je jednaka 1, odnosno nije u pitanju nula vektor, te je stoga na osnovu date pretpostavke

$$Q(e(I)) = 0.$$

Dalje, primijetimo da je

$$Q(e(I)) = \sum_{J \subset I} c_J = \sum_{J \subset I,\, J \neq I} c_J + c_I.$$

[27]Imre Bárány (1947–), mađarski matematičar
[28]Péter Komjáth (1953–), mađarski matematičar

Sada možemo iskoristiti induktivnu hipotezu za sve c_J, pa slijedi da je

$$\begin{aligned}\sum_{J\subset I,\, J\neq I} c_J + c_I &= \sum_{J\subset I,\, J\neq I} (-1)^{|J|}c + c_I \\ &= c\Big(\sum_{0\leq j<|I|} \binom{|I|}{j}(-1)^j\Big) + c_I \\ &= c\Big((1-1)^{|I|} - (-1)^{|I|}\Big) + c_I \\ &= c(-1)^{|I|+1} + c_I \\ &= c(-1)^{|I|-1} + c_I.\end{aligned} \tag{3.30}$$

Time je dokaz završen. □

Sada smo spremni za dokaz teoreme 3.71.

Dokaz. Bez umanjenja opštosti možemo pretpostaviti da je jedino nepokriveno tjeme $(0, 0, ..., 0)$.

Neka je svaka hiperravan H_i data jednačinom $(a_i, x) = b_i$, za sve $i = 1, ..., m$, gdje je x proizvoljni vektor dimenzije n, a sa (x, y) je označen skalarni proizvod vektora.

Posmatrajmo sljedeći polinom:

$$P(x) = \prod_{i=1}^{m}((a_i, x) - b_i).$$

Svaki polinom u standardnoj reprezentaciji možemo zapisati kao sumu monoma, pa tako i P.

Definišimo polinom $Q(x)$ koji se dobija od polinoma $P(x)$ tako što se u njegovoj standardnoj reprezentaciji svako javljanje x_i^m, gdje je $m > 1$, zamijeni sa x_i. Tim postupkom ćemo dobiti polinom koji je linearan po svakoj promjenljivoj, a ima iste nule kao polinom P.

Kako su nule polinoma P sva tjemena jedinične kocke sem nula vektora, slijedi da su to nule i $Q(x)$, odnosno

$$Q(\boldsymbol{x}) = 0, \text{ za sve } \boldsymbol{x} \in \{0, 1\}^n \setminus \mathbf{0} \text{ i } Q(\mathbf{0}) = P(\mathbf{0}) \neq 0.$$

Tada je na osnovu pomoćne leme 3.72

$$n = \deg(Q) \leq \deg(P) = m.$$

Time je dokaz završen.

□

Daćemo i drugi dokaz koji slijedi direktno iz Kombinatornog „Nullstellensatza" (teorema 2.3).

Dokaz. Pretpostavimo da je tvrđenje netačno, tj. da važi $m < n$.

Bez umanjenja opštosti možemo pretpostaviti da je jedino nepokriveno tjeme $(0, 0, ..., 0)$. Neka je svaka hiperravan H_i data jednačinom $(a_i, x) = b_i$, za sve $i = 1, ..., m$, gdje je x proizvoljni vektor dimenzije n, a sa (x, y) je označen skalarni proizvod vektora.

Dalje, kako date hiperravni ne pokrivaju nula vektor, slijedi da je $b_i \neq 0$ za sve $i = 1, ..., m$. Posmatrajmo sljedeći polinom:

$$P(x) = (-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n} (x_i - 1) - \prod_{i=1}^{m} \left((a_i, x) - b_i \right).$$

Lako uočavamo da je $\deg(P) = n$ i koeficijent uz monom $\prod_{i=1}^{n} x_i$ je

$$(-1)^{n+m+1} \prod_{j=1}^{m} b_j.$$

Kako smo zaključili da je $b_i \neq 0$, za sve i, pomenuti koeficijent je različit od nule. Sada su ispunjeni uslovi teoreme 2.3, i ako stavimo da je $S_i = \{0, 1\}$ za sve $i = 1, ..., n$, dobićemo da postoji vektor $x = (x_1, x_2, ..., x_n)$ takav da $x_i \in S_i$ i $P(x) \neq 0$.

Kako je $P(\mathbf{0}) = 0$, slijedi da je $x_i \neq 0$ za bar jedno $i = 1, ..., n$. Baš za taj indeks i je

$$(-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n} (x_i - 1) = 0.$$

Takođe primijetimo da, kako $x = (x_1, x_2, ..., x_n)$ nije nula vektor, onda je to jedno tjeme jedinične kocke koje je pokriveno nekom hiperravni, pa je za neko $i = 1, ..., m$ ispunjeno

$$(a_i, x) - b_i = 0.$$

Time smo dobili da je $P(x) = 0$, što je u kontradikciji sa našim zaključkom da je $P(x) \neq 0$. Dakle, pretpostavka je bila pogrešna, pa je $m \geq n$. Time je dokaz završen.

□

Primijetimo da je naizgled vrlo komplikovan polinom P iz posljednjeg dokaza definisan na taj način da bi nas doveo do željenog rješenja.

3.9 Sabiranje skupova u vektorskim prostorima nad $GF(p)$

Hopf–Stiefelov uslov je pojam koji se javlja u topologiji. Predstavićemo nekoliko rezultata u kojima se potpuno neočekivano javlja pomenuti uslov i dati dokaze nekih.

Definicija 3.45. Uređena trojka (r, s, n) prirodnih brojeva zadovoljava Hopf–Stiefelov uslov ako je

$$\binom{n}{k} \text{ paran broj za } \forall k \in \mathbb{N} \text{ koje zadovoljava } n - r < k < s.$$

Definicija 3.46. Uređena trojka (r, s, n) prirodnih brojeva zadovoljava Hopf–Stiefelov uslov u odnosu na prost broj p ako

$$p \mid \binom{n}{k} \text{ za } \forall k \in \mathbb{N} \text{ koje zadovoljava } n - r < k < s.$$

Uvodimo oznaku:

$$\beta_p(r, s) = \min\{n \in \mathbb{N} : (r, s, n) \text{ zadovoljava Hopf–Stiefelov uslov}\}.$$

Sljedeću teoremu je formulisao i dokazao Yuzvinsky. Dajemo je bez dokaza, koji je daleko od nezanimljivog, ali se u njemu ne koriste algebarske tehnike koje su u centru našeg interesovanja. Detaljan dokaz se može pronaći u [65].

Teorema 3.73. *([65]) Posmatrajmo beskonačan vektorski prostor nad $GF(2)$. Tada postoje skupovi $A, B \subset V$ takvi da je*

$$|A| = r,\ |B| = s \ \textit{i}\ |A + B| \leq n,$$

ako i samo ako trojka (r, s, n) zadovoljava Hopf–Stiefelov uslov.

Teorema koja slijedi je uopštenje prethodne teoreme i Cauchy–Davenport teoreme 3.8. Daćemo originalni dokaz koji koristi algebarske metode iz [7] i [6] i drugi pomoću Kombinatornog „Nullstellensatza".

Teorema 3.74. *([26]) Ako su A i B dva konačna i neprazna podskupa vektorskog prostora V nad $GF(p)$, kardinalnosti r i s redom, onda je*

$$|A + B| \geq \beta_p(r, s).$$

Za dokaz nam je potrebna pomoćna lema, koja sumira neke od rezultata Alona i Tarsija. Sama formulacija, ali i dokaz, podsjećaju dosta na pomoćnu lemu (2.1) iz prve glave, ali ipak tvrde različite stvari, stoga ćemo je i dokazati. Prvo, uvedimo pojam koji će nam biti potreban.

Neka je $f = f(x_1, ..., x_n) \in F[x_1, ..., x_n]$, gdje je F neko polje. Označimo sa $\text{top}(f)$ njegovu homogenu komponentu najvećeg stepena. U standardnoj reprezentaciji polinoma kao suma monoma, $\text{top}(f)$ je suma monoma istog stepena koji je pritom najveći stepen koji se javlja u f, i dodefinišimo dodatno $\text{top}(0) = 0$.

Primjer 3.75. Odrediti $\text{top}(p)$, gdje je $p = p(x, y) = xy + 3xy^2 + 4x^2y^3 - xy^4 + 8x^2y - 11x^3y^2$.

Kako je $\deg(p) = 5$, u $\text{top}(p)$ se javljaju svi monomi petog stepena, odnosno

$$\text{top}(p) = 4x^2y^3 - xy^4 - 11x^3y^2.$$

Lema 3.76. *([26]) Neka su $\emptyset \neq A_1, ..., A_n \subset F$ i $|A_i| = r_i$, za $i = 1, ..., n$. Neka je $f = f(x_1, ..., x_n) \in F[x_1, ..., x_n]$ polinom koji ispunjava sljedeći uslov*

$$f(x_1, ..., x_n) = 0, \text{ za sve } n\text{-torke } (x_1, ..., x_n) \in A_1 \times ... \times A_n.$$

Tada $\text{top}(f)$ pripada idealu generisanom sa $x_i^{r_i}$, gdje $i = 1, ..., n$.

Dokaz. Dokaz dajemo indukcijom po broju promjenljivih.

Za $n = 1$, lema tvrdi da polinom po jednoj promjenljivoj sa r_1 nula mora biti stepena bar r_1, tako da u ovom slučaju nemamo šta da dokazujemo.

Pretpostavimo da tvrđenje važi za $n - 1$ ($n \geq 2$) i dokažimo za n. Ako su svi monomi u $\text{top}(f)$ djeljivi sa $x_n^{r_n}$, onda teorema važi. U suprotnom, označimo sa $v_1, ..., v_m$ one koji nisu i pokažimo da oni pripadaju idealu generisanom polinomima $x_i^{r_i}$, gdje $i = 1, ..., n - 1$. Definišimo polinom

$$g(x_n) = \prod_{a \in A_n} (x_n - a)$$

i primijetimo da je $\deg(g) = |A_n| = r_n$. Potom, definišimo i polinom $\tilde{f}$, koji se od polinoma f dobija tako što se svako javljanje $x_n^{r_n}$ zamijeni sa $h(x_n) = x_n^{r_n} - g$. Tada je

$$f \equiv \tilde{f} \pmod{q}.$$

Primijetimo da se na ovaj način ne mijenjaju nule polinoma, odnosno važi

$$\tilde{f}(x_1, ..., x_n) = 0, \text{ za sve } n\text{-torke } (x_1, ..., x_n) \in A_1 \times ... \times A_n.$$

Kako je $\deg(h) < r_n$, opisanim postupkom se smanjuje stepen svakog monoma u kome se javljao član $x_n^{r_n}$, te dobijeni monomi nisu u $\text{top}(\tilde{f})$. Stoga su $v_1, ..., v_m$ upravo monomi koji pripadaju $\text{top}(\tilde{f})$.

Uvijek možemo polinom $\tilde{f}$ posmatrati kao polinom po x_n, sa koeficijentima iz $F[x_1, ..., x_{n-1}]$. Zapišimo ga onda u sljedećem obliku

$$\tilde{f} = \tilde{f}_0 + \tilde{f}_1 x_n + ... + \tilde{f}_k x_n^k,$$

gdje je $k < r_n$ i $\tilde{f}_i \in F[x_1, ..., x_{n-1}]$ za sve $i = 1, ..., k$.

Neka je $a = (a_1, ..., a_{n-1}) \in A_1 \times ... \times A_{n-1}$ i neka je

$$\tilde{f}_a(x_n) = \tilde{f}_0(a) + \tilde{f}_1(a)x_n + ... + \tilde{f}_k(a)x_n^k.$$

Tada je $\tilde{f}_a(x_n) = 0$ za $\forall x_n \in A_n$, jer $\tilde{f}(x_1, ..., x_n) = 0$ za $(x_1, ..., x_n) \in A_1 \times ... \times A_n$. Kako je $\tilde{f}_a$ polinom koji ima $|A_n| = r_n$ nula, a $\deg(\tilde{f}_a) = k < r_n$, slijedi da je $\tilde{f}_a \equiv 0$. Stoga, mora $\tilde{f}_i(x_1, ..., x_{n-1}) = 0$ za sve $(x_1, ..., x_{n-1}) \in A_1 \times ... A_{n-1}$, za sve $i = 1, ..., k$. Kako su to sve polinomi sa $n-1$ promjenljivom, slijedi da za njih važi indukcijska hipoteza, pa $\text{top}(\tilde{f}_i)$, gdje $i = 1, ..., k$, pripada idealu generisanom sa $x_j^{r_j}$ za $j = 1, ..., n-1$.

Uočimo da važi sljedeća jednakost:

$$\text{top}(\tilde{f}) = \text{top}\Big(\text{top}(\tilde{f}_0) + \text{top}(\tilde{f}_1)x_n + ... + \text{top}(\tilde{f}_k)x_n^k\Big).$$

Stoga, $\text{top}(\tilde{f})$ pripada idealu generisanom sa $x_i^{r_i}$ gdje $i = 1, ..., n-1$. Konačno, time dobijamo da $\text{top}(f)$ pripada idealu generisanom sa $x_i^{r_i}$ gdje $i = 1, ..., n$, što je i trebalo dokazati. □

U nastavku slijedi prvi dokaz teoreme 3.74.

Dokaz. Pretpostavimo da je dati vektorski prostor konačan i identifikujmo ga sa nekim konačnim poljem F_q, gdje je $q = p^d$ za neko $d \geq 1$.

Neka su onda $\emptyset \neq A, B \subset F_q$ i $|A| = r$, $|B| = s$, i označimo $C = A + B$.

Definišimo polinom $f = f(x, y) \in F_q[x, y]$ sa

$$f(x, y) = \prod_{c \in C}(x + y - c).$$

Primijetimo da je $f(x, y) = 0$ kada god $x \in A, y \in B$, i uočimo da je $\text{top}(f) = (x + y)^{|C|}$.

Tada iz prethodne leme 3.76 slijedi da $(x + y)^{|C|}$ pripada idealu generisanom sa x^r i y^s u $F_q[x, y]$, ali samim tim i u $F_p[x, y]$, jer su svi koeficijenti datog polinoma u F_p. Sada slijedi da je $|C| \geq \beta_p(r, s)$ po definiciji, što je i trebalo pokazati. □

Drugi dokaz slijedi direktno iz Kombinatornog „Nullstellensatza". Dajemo ga u nastavku.

Dokaz. Pretpostavimo da je dati vektorski prostor konačan i identifikujmo ga sa nekim konačnim poljem F, koje ima isto elemanata kao V.

Neka su onda $\emptyset \neq A, B \subset F$ i $|A| = r$, $|B| = s$ i označimo $C = A + B$. Pretpostavimo da tvrđenje ne važi, odnosno $n = |C| < \beta_p(r, s)$.

Potom, definišemo polinom $Q = Q(x, y) \in F[x, y]$ sa

$$Q(x, y) = \prod_{c \in C} (x + y - c).$$

Primijetimo da je $Q(x, y) = 0$ kada god $x \in A$, $y \in B$, jer je $C = A + B$. Dalje, kako je $n < \beta_p(r, s)$, trojka (r, s, n) ne zadovoljava Hopf–Stiefelov uslov. Odnosno, postoji neko k tako da je $n - r < k < s$, za koje p ne dijeli binomni koeficijent $\binom{n}{k}$. To je koeficijent koji stoji uz $x^{n-k}y^k$ u polinomu Q, pa kako pomenuti koeficijent nije djeljiv sa p, različit je od nule u $GF(p)$. Kako je $|A| = r > n - k$ i $|B| = s > k$, ispunjeni su uslovi Kombinatornog „Nullstellensatza" odnosno teoreme 2.3.

Slijedi da postoje neki $a \in A$ i $b \in B$ takvi da je $Q(a, b) \neq 0$, što je u kontradikciji sa jednim od prethodnih zaključaka.

Dakle, pretpostavka je bila pogrešna i važi $|C| = |A + B| \geq \beta_p(r, s)$, što je i trebalo pokazati. □

Zaključak

U radu smo se bavili rezultatom Noge Alona, koji je poznat pod nazivom Kombinatorni „Nullstellensatz". Riječ je o dvije teoreme koje predstavljaju vrlo moćan i koristan algebarski alat. Nakon što smo u uvodu objasnili sve o pomenutom rezultatu, sljedeću glavu smo posvetili detaljnim dokazima dvije glavne teoreme na kojima se temelji ovaj rad.

Centralni dio rada posvećen je primjenama Kombinatornog „Nullstellensatza". Osnovna ideja je bila da se za odabrane teoreme predstave njihovi klasični i originalni dokazi, koji su nerijetko dugi i zahtijevaju dosta pomoćnih tvrđenja, a potom i dokazi pomoću Kombinatornog „Nullstellensatza", koji su znatno kraći i elegantniji i sva njihova težina se ogleda u odabiru odgovarajućeg polinoma koji će nas dovesti do rješenja.

Prvo smo predstavili dvije klasične primjene, kako ih je nazvao i sam Alon, a to su Chevalley–Warning teorema i Cauchy–Davenport teorema. Za obje smo dali i klasične i nove dokaze. Potom smo prešli na priču o restrikovanim sumama, gdje smo dokazali jedan rezultat Alona, Nathansona i Ruzse, ponovo na dva načina. U nastavku smo pokazali kako se, koristeći taj rezultat, može doći do još jednog dokaza Cauchy–Davenport teoreme. Dali smo još nekoliko primjena pomenutog rezultata, među kojima su između ostalog i Erdős–Heilbronn teorema.

Sljedeće poglavlje smo posvetili poznatoj EGZ teoremi, koju su formulisali Erdős, Ginzbur i Ziv i po kojima nosi i ime. Prvo smo pokazali da je dovoljno dokazati teoremu za jedan specijalan slučaj, a potom smo dali čak pet dokaza tog slučaja, jer se u njima koriste tehnike koje smo već upoznali u ovom radu. Prvi dokaz se dobija pomoću Cauchy–Davenport teoreme, a drugi pomoću Chevalley–Warning teoreme. Treći dokaz je poznat kao argument o prebrojavanju, a za četvrti nam je bio potreban pojam Davenportove konstante. Nakon što smo definisali taj pojam i dali nekoliko reprezentativnih primjera, dokazali smo Olsonovu teoremu, kao i jednu njenu posljedicu koje su nam bile potrebne više puta u radu. Pomoću Olsonove teoreme dali smo četvrti dokaz EGZ teoreme.

U nastavku uvodimo pojam permanente matrice i formulišemo poznati

rezultat iz linearne algebre, a to je lema o permanentama. Dokazujemo jedan pomoćni rezultat, a potom pomenutu lemu na dva načina, gdje ponovo koristimo Kombinatorni „Nullstellensatz". Zatim, navodimo primjene ove leme među kojima se našao i peti dokaz EGZ teoreme. Osim njega uvodimo i Harborthov problem, poznatu Jaegerovu hipotezu i nekoliko rezultata o aditivnim bazama. Naposletku, dajemo i jedan rezultat o digrafu, gdje smo posmatrali permanentu matrice incidencije grafa. U tom duhu nastavljamo i sljedeće poglavlje, koje je posvećeno grafovima i podgrafovima.

Prvo smo napravili uvod u teoriju grafova, gdje smo definisali sve pojmove koji su nam bili potrebni iz ove oblasti. U centralnom dijelu dokazujemo jedan moćan rezultat, koji se može smatrati uopštenjem poznate Berge-Sauer hipoteze. Za originalni dokaz tog rezultata, uvodimo definiciju pojma p-djeljivog grafa, dokazujemo pomoćnu teoremu i formulišemo dvije pomoćne leme i konačno dajemo klasični dokaz. Nakon toga slijedi dokaz pomoću Kombinatornog „Nullstellensatza". U nastavku smo dali i jednu primjenu pomenutog rezultata, a to je Erdős–Sauerov problem. Zatim, slijedi još jedan rezultat iz teorije grafova čiji dokaz se dobija pomoću Kombinatornog „Nullstellensatza" i koji prikazuje njegovu šarenoliku primjenu.

Sljedeće poglavlje je posvećeno problemima u vezi sa bojenjem grafova. Prvenstveno smo uveli sve standardne definicije iz ove oblasti, a zatim i pojam f-birljivog grafa kao i broja izbora grafa. Dali smo kriterijum bojenja koji su uveli Alon i Tarsi. Ponovo dajemo klasični dokaz koji zahtijeva nekolicinu pomoćnih rezultata i dokaz u svega nekoliko redova pomoću Kombinatornog „Nullstellensatza". Naveli smo i nekoliko najvažnijih primjena ovog rezultata, a to su problem o konturi i trouglovima, potom teorema o broju izbora planarnog bipartitnog grafa, kao i linijskog grafa.

Sve do sada smo u radu koristili samo Kombinatorni „Nullstellensatz" 2. Međutim, u nastavku slijedi nekoliko rezultata u kojima smo koristili Kombinatorni „Nullstellensatz" 1. Riječ je o rezultatima koji tvrde da graf ispunjava određena svojstva ako dati polinom pripada nekom idealu. Takođe, ovi rezultati su dokazani baš zahvaljujući Kombinatornom „Nullstellensatzu" 1, te stoga za njih predstavljamo baš taj dokaz. Dali smo četiri rezultata tog tipa, od čega smo dva dokazali koristeći pomenutu teoremu.

Dalje, definišemo hipergraf i bojenje hipergrafa i formulišemo dva rezultata koji daju potreban i dovoljan uslov da hipergraf sa određenim osobinama bude obojiv određenim brojem boja. Oba smo dokazali koristeći Kombinatorni „Nullstellensatz" 1. Pri tome je drugi rezultat zapravo uopštenje prvog i riječ je o jednoj od dvije teoreme iz ovog rada, koje su pokazane 2019. a koje prikazuju primjenu Alonovih teorema. Druga teorema je data u nastavku i ima vrlu zanimljivu primjenu u logičkoj igri sudoku. Naime, riječ je o teoremi koja daje potreban i dovoljan uslov da sudoku bude rješiv

i ponovo je dokazana pomoću glavnog alata ovog rada.

Onda smo dali jedan zanimljiv rezultat iz višedimenzionalne kombinatorne geometrije o pokrivanju jediničnih hiperkocki sa hiperravnima. Ponovo dajemo dva dokaza.

Naposletku, tu je i jedan rezultat koji uključuje Hopf–Stiefelov uslov, pojam iz topologije. I njega smo dokazali na dva načina.

Literatura

[1] S. D. Adhikari, M. N. Chintamani Geeta and B. K. Moriya, *The Cauchy–Davenport theorem: various proofs and some early generalizations*, Math. Student. 79 (1–4): (1995), 109–119.

[2] Y. Alexandr, *Combinatorial Nullstellensatz:Various Proofs , Extensions and Applications*, Undergraduate honors thesis, Wesleyan University (2019), 26–33.

[3] N. Alon, *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing 8 (1999), 7–29.

[4] N. Alon and M. Tarsi, *Colorings and orientations of graphs*, Combinatorica 12 (1992), 125–134.

[5] N. Alon and M. Tarsi, *A nowhere-zero point in linear mappings*, Combinatorica 9 (1989), 393–395.

[6] N. Alon, M. B. Nathanson, and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, J. Number Theory 56 (1996), 404–417.

[7] N. Alon, M. B. Nathanson, and I. Z. Ruzsa, *Adding distinct congruence classes modulo a prime*, Amer. Math. Monthly 102 (1995), 250–255.

[8] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, D. Miklós (ed.) V.T. Sós (ed.) T. Szönyi (ed.), Combinatorics, Paul Erdös is Eighty, Bolyai Society Mathematical Studies, 1 , Keszthely (Hungary) (1993), 33—50.

[9] N. Alon, S. Friedland and G. Kalai, *Regular subgraphs of almost regular graphs*, J. Combinatorial Theory, Ser. B, 37 (1984), 79–91.

[10] N. Alon, Linial and R. Meshulam, *Additive bases of vector spaces over prime fields*, J. Combinatorial Theory Ser. A 57 (1991), 203–210.

[11] N. Alon, S. Friedland, and G. Kalai, *Every 4-regular graph plus an edge contains a 3-regular subgraph*, J. Combin. Theory, Ser. B37 (1984), 92-–93.

[12] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes*, European J. Combinatorics 14 (1993), 79–83.

[13] N. Alon, *Restricted colorings of graphs*, Surveys in Combinatorics, Proc. 14th British Combinatorial Conference, London Mathematical Society Lecture Notes Series 187, edited by K. Walker, Cambridge University Press (1993), 1–33.

[14] N. Alon, C. McDiarmid, and B. Reed, *Star arboricity*, Combinatorica 12 (1992), 375—380.

[15] R. C. Baker and W. Schmidt, *Diophantine problems in variables restricted to the values 0 and 1*, J. Number Theory 12 (1980), 460–486.

[16] A. Blokhuis, *Polynomials in finite geometries and combinatorics*, Proc. 14th British Combinatorial Conference, London Mathematical Society Lecture Notes Series 187, edited by K. Walker, Cambridge University Press (1993), 35–52.

[17] B. Bollobás, *Extremal Graph Theory*, Academic Press, (1978).

[18] B. Bollobás and A. J. Harris, *List colorings of graphs*, Graphs and Combinatorics 1 (1985), 115–127.

[19] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, Macmillan & Co. London, (1976).

[20] C. Bujtás, Z. Tuza and V. Voloshin, *Hypergraph coloring*, Topics in Chromatic Graph Theory, Chapter: 11, 230–254.

[21] L. Chiraag, *Graph Theory of Sudoku*, Indian institute of science education and research BHOPAL (2013).

[22] F. R. K. Chung, *Labelings of graphs*, Selected Topics in Graph Theory 3, Academic Press (1988), 151–168.

[23] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. 10 (1935), 30-–32.

[24] H. Davenport, Proceedings of the Midwestern Conference on Group Theory and Number Theory, Ohio State University, (1966).

[25] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory* , The Bulletin of the London Mathematical Society, 26 No.2 (1994), 140—146.

[26] S. Eliahou and M. Kervaire, *Sumsets in vector spaces over finite fields*, J. Number Theory 71 (1998), 12–39.

[27] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups III*, Stichting Mathematisch Centrum (1969).

[28] P. Erdős, *Some problems in number theory*, Computers in Number Theory, edited by A.O.L. Atkin and B.J. Birch, Academic Press, (1971) 405-–414.

[29] P. Erdős, and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographs of L'Enseignement Mathématique, volume 28, Université de Genéve L'Enseignement Mathématique, (1980).

[30] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), 201–206.

[31] P. Erdős, A. Ginzburg and A. Ziv, *A theorem in additive number theory*, Bull. Res. Council Israel 10F (1961), 41–43.

[32] P. Erdős, A. L. Rubin and H. Taylor, *Choosability in graphs*, Proc. West Coast Conf. on Combinatorics, Graph Theory and Computing, Congressus Numerantium XXVI (1979), 125–157.

[33] H. Fleischner and M. Stiebitz, *A solution to a coloring problem of P. Erdős*, Discrete Math. 101 (1992), 39–48.

[34] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. 262/263 (1973), 356–360.

[35] D. Hilbert, *Ueber die vollen Invariantensysteme*, Mathematische Annalen 42 (1893), 313–373.

[36] F. Jaeger, Problem presented in the 6th Hungar. Comb. Coll., Eger, Hungary (1981), and: *Finite and Infinite Sets* (eds.: A. Hajnal, L. Lovász, V. T. Sós), North Holland, Amsterdam, (1982) II, 879.

[37] F. Jaeger, N. Linial, C. Payan and M. Tarsi, *Group connectivity of graphs- a nonhomogeneous analogue of nowhere-zero flow*, J. Combinatorial Theory Ser. B 56 (1992), 165–182.

[38] F. Jaeger, *On the Penrose number of cubic diagrams*, Discrete Math. 74 (1989), 85–97.

[39] M. Jerrum, *#P-completeness, Counting, Sampling and Integrating: Algorithm and Complexity*, Lectures in Mathematics, ETH Zürich (2003).

[40] A. Kemnitz, *On a lattice point problem*, Ars Combinatoria 16b (1983), 151–160.

[41] P. Komjáth, *Partitions of vector spaces*, Periodica Mathematica Hungarica Vol. 28 (3), (1994), 187-193.

[42] S. Kopparty, *The Cauchy–Davenport Theorem*, Lectures in Arithmetic Combinatorics, Rutgers University (2016).

[43] S. Y. R. Li and W. C. W. Li, *Independence numbers of graphs and generators of ideals*, Combinatorica 1 (1981), 55–61.

[44] L. Lovász, *Bounding the independence number of a graph*, Bonn Workshop on Combinatorial Optimization, (A. Bachem, M. Grötschel and B. Korte, eds.), Math. Studies 66, Annals of Discrete Math. 16 (1982), 213–223.

[45] L. Lovász, *Stable sets and polynomials*, Discrete Math. 124 (1994), 137–153.

[46] N. Malini, P. Malliga, R.G. Balamurugan and P. Suganya, *A study on graph colouring in sudoku*, Advances and Applications in Mathematical Sciences, Vol. 21, Issue 3 (2022), 1359–1364.

[47] K. Oddson, *Math and Sudoku: Exploring Sudoku Boards Through Graph Theory, Group Theory, and Combinatorics*, Student Research Symposium. 4, Portland State University (2016).

[48] J. E. Olson, *A combinatorial problem on finite abelian groups, I* , J. Number Theory 1 (1969), 8–10.

[49] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley (1994).

[50] L. Pyber, *Regular subgraphs of dense graphs*, Combinatorica 5 (1985), 347–349.

[51] L. Pyber, V. Rödl and E. Szemerédi, *Dense Graphs without 3-regular Subgraphs*, J. Combinatorial Theory Ser. B 63 (1995), 41–54.

[52] T. Redmond and C. Ryavec, The Mathematical Intelligencer 2 (1980), 106.

[53] C. Reiher, *On Kemnitz' conjecture concerning lattice-points in the plane*, Ramanujan J. 13 (2007), 333–337.

[54] K. Rogers, *A combinatorial problem in Abelian groups*, Math. Proc. Cambridge Philos. Soc. 59 (1963), 559-–562.

[55] D. E. Scheim, *The number of edge 3-colorings of a planar cubic graph as a permanent*, Discrete Math. 8 (1974), 377–382.

[56] W. Schmidt, *Equations over Finite Fields, an Elementary Approach*, Lecture Notes in Mathematics, Vol. 536 (134-140), Springer, Berlin (1976).

[57] M. Tarsi, *On the decomposition of a graph into stars*, Discrete Math. 36 (1981), 299–304.

[58] V. A. Taśkinov, *Regular subgraphs of regular graphs*, Soviet Muth. Dokl. 26 (1982), 37–38.

[59] C. Thomassen, *A remark on the factor theorems of Lovász and Tutte*, J. Graph Theory 5 (1981), 441–442.

[60] I. Vardi, *Permanents*, §6.1 in Computational Recreations in Mathematica. Reading, MA: Addison-Wesley (1991) 108, 110–112.

[61] L. Vigneron, *Remarques sur les réseaux cubiques de classe 3 associés au probléme des quatre couleurs*, C. R. Acad. Sc. Paris, t. 223 (1946), 770–772.

[62] V. G. Vizing, *Coloring the vertices of a graph in prescribed colors*, Diskret. Analiz. No. 29, Metody Diskret. Anal. v. Teorii Kodov i Shem 101 (1976), 3–10 (in Russian).

[63] G. Weidong, *Any* $2n-1$ *integers contain exactly* n *integers whose sum is a multiple of* n, J. of Northeast Normal University 4 (1985) (in Chinese).

[64] C. Wrenn, *Group rings*, Masters Essays, John Carroll University (2018).

[65] S. Yuzvinsky, *Orthogonal pairings of Euclidean spaces*, Michigan Math. J. 28 (1981), 109–119

[66] http://www.mathpuzzle.com/4Dec2001.htm

Biografija

Nikolina Miholjčić je rođena 8. aprila 1999. godine u Zvorniku. Pohađala je osnovnu školu „Jovan Dučić" u Bijeljini, koju je završila 2014. godine, kao nosilac Vukove diplome. Iste godine je upisala Gimnaziju „Filip Višnjić", koju je takođe završila kao nosilac Vukove diplome 2018. godine. Zatim je upisala osnovne akademske studije matematike u trajanju od tri godine, na Prirodno-matematičkom fakultetu u Novom Sadu, smjer Matematika. Studije je završila 2021. godine sa prosjekom 9.66, nakon čega je na istom fakultetu upisala master studije u trajanju od dvije godine, smjer Matematika. Položila je sve ispite predviđene nastavnim planom i programom master studija u julskom ispitnom roku 2023. godine, sa prosjekom 10.0.

Novi Sad, septembar 2023.

Nikolina Miholjčić

UNIVERZITET U NOVOM SADU
PRIRODNO - MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR

Identifikacioni broj:
IBR

Tip dokumentacije: Monografska dokumentacija
TD

Tip zapisa: Tekstualni štampani materijal
TZ

Vrsta rada: Master rad
VR

Autor: Nikolina Miholjčić
AU

Mentor: dr Bojan Bašić
ME

Naslov rada: Kombinatorni "Nullstellensatz"
NR

Jezik publikacije: Srpski (latinica)
JP

Jezik izvoda: srpski / engleski
JI

Zemlja publikovanja: Republika Srbija
ZP

Uže geografsko područje: Vojvodina
UGP

Godina: 2023.
GO

Izdavač: Autorski reprint
IZ

Mesto i adresa: Novi Sad, Trg D. Obradovića 4
MA

Fizički opis rada: (3/104/66/0/3/0/0)(broj poglavlja/broj strana/broj literarnih citata/broj tabela/broj slika/broj grafika/broj priloga)
FO:

Naučna oblast: Matematika
NO

Naučna disciplina: Kombinatorika
ND

Ključne reči: Kombinatorni „Nullstellensatz", Chevalley–Warning teorema, Cauchy–Davenport teorema, EGZ teorema, permanenta matrice, p-djeljivi grafovi, bojenje grafova, ideali polinoma, polinom grafa, hipergraf, hiperkocka
PO, UDK

Čuva se: U biblioteci Departmana za matematiku i informatiku, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
ČU

Važna napomena:
VN

Izvod: U ovom radu se bavimo čuvenom algebarskom tehnikom pod nazivom Kombinatorni „Nullstellensatz". U uvodnom dijelu opisujemo povezanost ovog rezultata sa Hilbertovim „Nullstellensatzom". Potom u sljedećoj glavi dajemo glavne teoreme sa detaljnim dokazima. Centralni dio rada posvećen je primjenama Kombinatornog „Nullstellensatza". Prvo smo dali nekoliko primjena u aditivnoj teoriji brojeva, kao što su Chevalley–Warningova teo-

rema, Cauchy–Davenportova teorema i EGZ teorema. Pokazali smo i lemu o permanentama, rezultat iz linearne algebre, kao i razne njene primjene. Potom smo naveli nekoliko rezultata iz teorije grafova, sa posebnim osvrtom na bojenje grafova. Naposletku, dokazujemo jedan rezultat o pokrivanju hiperkocke hiperravnima i jednu teoremu koja uključuje Hopf–Stiefelov uslov.
IZ

Datum prihvatanja teme od strane NN veća: 5. jun 2023.
DP

Datum odbrane:
DO

Članovi komisije:
ČK

Predsednik: dr Rozalija Madaras-Silađi, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
Mentor: dr Bojan Bašić, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
Član: dr Petar Marković, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCES
KEY WORDS DOCUMENTATION

Accession number:
ANO

Identification number:
INO

Document type: Monograph type
DT

Type of record: Printed text
TR

Contents Code: Master's thesis
CC

Author: Nikolina Miholjčić
AU

Mentor: Bojan Bašić, PhD
MN

Title: Combinatorial "Nullstellensatz"
TI

Language of text: Serbian (Latin)
LT

Language of abstract: serbian / english
LA

Country of publication: Republic of Serbia
CP

Locality of publication: Vojvodina
LP

Publication year: 2023.
PY

Publisher: Author's reprint
PU

Publication place: Novi Sad, Trg D. Obradovića 4
PP

Physical description: (3/104/66/0/3/0/0)(chapters/ pages/ quotations/ tables/ pictures/ graphics/ enclosures)
PD

Scientific field: Mathematics
SF

Scientific discipline: Combinatorics
SD

Subject/Key words: Combinatorial "Nullstellensatz", Chevalley–Warning theorem, Cauchy–Davenport theorem, EGZ theorem, permanent, p-divisible graphs, graph coloring, ideals of polynomials, graph polynomial, hypergraph, hypercube
SKW

Holding data: The Library of the Department of Mathematics and Informatics, Faculty of Science and Mathematics, University of Novi Sad
HD

Note:
N

Abstract: In this paper, we delve into the renowned algebraic technique known as the Combinatorial "Nullstellensatz". In the introductory section, we elucidate its connection with Hilbert's "Nullstellensatz". Subsequently, in the following section, we present the principal theorems along with detailed proofs. The central part of this work is dedicated to the applications of the Combinatorial "Nullstellensatz".

Initially, we provided several applications in additive number theory, such as the Chevalley–Warning theorem, the Cauchy–Davenport theorem, and the Erdős–Ginzburg–Ziv theorem. Additionally, we establish the lemma on permanents, a result of linear algebra, along with various applications thereof. Furthermore, we outline several results from graph theory, with a particular focus on graph coloring. Finally, we prove a result concerning hypercube covering by hyperplanes and a theorem encompassing the Hopf–Stiefel condition.
AB

Accepted by the Scientific Board on: June 5, 2023.
ASB

Defended:
DE

Thesis defend board:
DB

President: Rozalija Madaras-Silađi, PhD, Full Professor, Faculty of Science and Mathematics, University of Novi Sad
Mentor: Bojan Bašić, PhD, Full Professor, Faculty of Science and Mathematics, University of Novi Sad
Member: Petar Marković, PhD, Full Professor, Faculty of Science and Mathematics, University of Novi Sad