SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Klara Nesterović

SCHWARTZ - ZIPPELOV TEOREM I NEKE NJEGOVE PRIMJENE

Diplomski rad

Voditelj rada:
Prof.dr.sc. Juraj Šiftar

Zagreb, srpanj, 2015.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu bit će riječi o rezultatu poznatom već otprilike 35 godina kao Schwartz - Zippelova lema ili Schwartz - Zippelov teorem. Teorem je u osnovi algebarske prirode, no ima značajne aspekte i u drugim područjima, naročito u kreiranju probabilističkih algoritama za testiranje jednakosti dvaju polinoma, odnosno različitih algebarskih i kombinatoričkih svojstava koja se mogu formulirati pomoću polinoma. U radu ćemo izložiti neke od takvih primjena, kao što su problem savršenog sparivanja u grafu i ispitivanje asocijativnosti u grupoidu.

Osnovni smisao Schwartz - Zippelovog teorema nije teško objasniti. Znamo da polinom P u jednoj varijabli, stupnja $d > 0$, nad poljem F, ima najviše d nultočaka u polju F računajući njihove kratnosti. Stoga, ako je S neki konačni podskup polja F, uzmimo da ima k elemenata, vjerojatnost da slučajno izabrani element od S bude nultočka polinoma P nije veća od $\frac{d}{k}$ (omjer najvećeg mogućeg broja "povoljnih slučajeva" i ukupnog broja mogućih izbora). Schwartz - Zippelov teorem zapravo govori da vrlo jednostavan analogni rezultat vrijedi i za polinom P u n varijabli.

Navedimo još nekoliko osnovnih podataka o matematičarima čija su imena vezana uz ovaj teorem. Jack Schwartz (1930 - 1979) bio je znameniti američki matematičar koji je pružio značajne doprinose različitim područjima matematike i teorije računarstva. Među njegovim brojnim knjigama naročito je poznata trilogija *Linear operators* koju je napisao zajedno s Nelsonom Dunfordom. J. Schwartz je osnovao *Department of Computer Science* na sveučilištu *New York University*. Između ostalog, radio je na dizajnu novih programskih jezika i razvoju paralelnih algoritama.

Richard E. Zippel američki je matematičar koji se najviše bavi primjenom matematičkih metoda u računarstvu. Njegova doktorska disertacija, obranjena 1979. godine na glasovitom *Massachusetts Institute of Technology*, nosi naslov *Probabilistic algorithms for sparse polynomials* i u njoj se nalazi njegova varijanta rezultata koji se danas najčešće naziva Schwartz - Zippelova lema ili teorem.

Cilj rada je razmotriti zanimljivu povijest ovog jednostavnog, ali jako korisnog rezultata, dokazati samu tvrdnju te opisati neke njezine primjene u matematici.

Poglavlje 1

Izvori i motivacija teorema

1.1 Kratka povijest teorema

Kao i kod mnogih drugi rezultata u povijesti matematike, za tvrdnju koja se najčešće naziva Schwartz - Zippelovom lemom ili teoremom nije sasvim jasno ili jednoznačno utvrđeno kome bi sve trebalo pripisati autorstvo [3], odnosno kome pripada prioritet u formuliranju i objavljivanju rezultata. I ovdje je takav slučaj da se više autora otprilike u isto vrijeme nezavisno bavilo sličnim idejama, što je dovelo do vrlo sličnih, ali ne i identičnih rezultata. Način i redoslijed u znatnoj mjeri proizlaze i iz stjecaja određenih okolnosti.

Osim Jack Schwartza i Richarda Zippela, koji su svoje ideje razvijali neovisno, u ovom kontekstu ističu se i imena Richard DeMilloa i Richarda J. Liptona. Ovi autori objavili su 1978. godine članak [1], koji prethodi publikacijama Zippela 1979. godine [6] i Schwartza 1980. godine [5].

Pitanja prioriteta i autorstva još uvijek su otvorena za raspravu, kao i usporedbe različitih varijanti objavljenih rezultata. S jedne strane, teorem bi se mogao nazvati jednostavno Schwartzov, jer je upravo on jedini koji je objavio njegovu ”jaku” formu. Međutim, kako se u mnogim primjenama ovog teorema koristi ”slaba” forma koju je otkrio Zippel, mogli bismo ga nazvati Schwartz - Zippelov teorem. Nije potpuno jasno zašto se imena DeMillo i Lipton ne nalaze u nazivu, no pretpostavlja se da je tako iz dva razloga. Prvi je taj što su Schwartz i Zippel zajedno prezentirali svoja otkrića na konferenciji 1979. godine, pa su vjerojatno zato citirani zajedno. Drugi razlog bi mogao biti taj što DeMillo i Lipton nikad prije nisu svoj raniji članak istaknuli u razgovoru sa Schwartzom, a kad je Schwartzov članak izašao u *JACM* časopisu uvidjeli su da se njih nigdje ne spominje no nisu ništa poduzimali po tom pitanju.

Kako bismo ukratko izložili i usporedili rezultate spomenutih autora, a prije nego što se detaljno pozabavimo glavnim teoremom i njegovim dokazom, navest ćemo opći oblik svih ključnih tvrdnji i nazvat ćemo ga jednostavno lemom.

Lema 1.1.1. *Pretpostavimo da je $p(x_1, x_2, \ldots, x_n)$ polinom stupnja $d \geq 0$, dakle različit od nulpolinoma, nad nekim poljem $\mathbb{K}$ i neka je S neprazan podskup od $\mathbb{K}$. Tada vjerojatnost da za slučajno izabrane elemente $r_1, r_2, \ldots, r_n \in S$ vrijedi $p(r_1, r_2, \ldots, r_n) = 0$ nije veća od $\delta(n, d, |S|)$. Pritom je δ neka funkcija koja ovisi o broju varijabli polinoma, njegovom stupnju i veličini skupa S.*

Cilj je, dakle, pronaći funkciju δ za koju će teorem biti istinit, odnosno dati što bolju ocjenu vjerojatnosti da polinom poprimi vrijednost 0 za slučajni izbor vrijednosti njegovih varijabli. U radovima spomenutih autora zapravo je dokazana jedna od sljedeće dvije ocjene:

1. $\delta(n, d, |S|) = \frac{d}{|S|}$, tzv. jaka forma,
2. $\delta(n, d, |S|) = \frac{nd}{|S|}$, tzv. slaba forma.

Jaka forma ima očitu prednost u tome što ne ovisi o broju varijabli n. U daljnjem ćemo ukratko navesti koji su rezultati pojedinih radova i u kakvom su međusobnom odnosu.

1.2 Različiti oblici i usporedba

Izložit ćemo vrlo sažeto sadržaj radova u kronološkom redosljedu.

DeMillo - Liptonov članak (1978.)

DeMillo i Lipton su objavili svoj članak u časopisu *Information Processing Letters* 1978. godine. To je zapravo bio tehnički izvještaj iz 1977. godine. Misao vodilja im je bila primjena na testiranje programa, na čemu su i radili neko vrijeme. Oni su zapravo i dokazali ono što zovemo slaba forma, no njihov članak je bio pomalo neobičan. Bio je neobičan po tome što nisu strogo matematički napisali lemu, nego su rezultat iskazali donekle neformalno. Razlog tome je što su smatrali da vrlo formalan članak ne bi zadobio pažnju njihovog auditorija, koji se sastojao od softverskih inžinjera, a kojima je bio prvenstveno namijenjen.

Zippelov članak (1979.)

Zippel je dokazao puno složeniju formu nego Schwartz u svom članku. Taj njegov rezultat je značajan barem koliko i slaba forma. No, postoje određene teškoće kao na primjer ta da je Zippel koristio drugačiji model, odnosno uzimao je maksimalni stupanj pojedine varijable umjesto ukupnog stupnja polinoma. Također, dosta je teško usporediti Zippelov rezultat s preostala dva upravo zbog toga što je koristio drugačiji model.

Njegov članak je objavljen na istoj konferenciji kao i Schwartzov 1979. godine, gdje je on prema programu konferencije imao riječ odmah nakon Schwartza. Bio je potaknut radom stvarnih simboličkih sustava i posvetio je dosta vremena stvarnoj implementaciji svog algoritma za testiranje jednakosti polinoma. Time se uvjerio da njegove metode stvarno daju rezultate.

Schwartzov članak (1980.)

Schwartz je objavio svoj rad u časopisu *JACM* 1980. godine. Njegov izvorni članak je poprilično dug i obuhvaća mnogo drugih aspekata testiranja jednakosti polinoma. Međutim, najbitniji njegov rezultat je poznati test jednakosti, odnosno "jaka" forma za testiranje jednakosti polinoma. Dosta pažnje posvetio je i primjeni u planimetriji.

Uočimo da je Schwartzov rad objavljen kasnije od ostalih, ali jedino je on pronašao jaku formu ocjene. S druge strane, svi autori ustanovili su da nije neophodan eksponencijalni, nego već i polinomijalni broj evaluacija vrijednosti polinoma kako bi se testiralo je li svugdje jednak 0. Lipton je napisao i sljedeći komentar o ovim rezultatima:

Zanimljivo je da sva tri članka imaju dvije zajedničke ključne ideje:

1. Polinom u jednoj varijabli, različit od nulpolinoma, može imati najviše onoliko nultočaka koliki mu je stupanj.

2. Polinom u n varijabli može se zapisati kao polinom u jednoj varijabli čiji koeficijenti su polinomi u $n - 1$ varijabli.

Prethodne tvrdnje moguće je dokazati nekim oblikom matematičke indukcije.

Lipton dalje navodi kako je glavna zamisao njegovog i DeMillovog članka u stvari bila da se jednakosti mogu testirati u daleko manje vrijednosti od $(d + 1)^n$. Oni nisu implementirali svoj algoritam, ali su dali veliki broj podataka da bi pokazali efikasnost slučajnog algoritma za različite parametre.

Upravo to se vidi u Tablici 1 koja prikazuje kako se kod primjene slučajnog algoritma vjerojatnost pogreške mijenja u ovisnosti o broju varijabli, stupnju polinoma i veličini skupa iz kojeg biramo točke u kojima evaluiramo polinom.

Označit ćemo sa t broj evaluacija polinoma, sa d maksimalni stupanj polinoma, sa m broj varijabli, te sa r veličinu skupa iz kojeg biramo točke za evaluaciju. Iz dane tablice možemo zaključiti da je vjerojatnost pogreške vrlo mala, odnosno da je pogreška zanemariva u slučaju kada je kardinalitet skupa iz kojeg biramo točke za evaluaciju barem 10 puta veći od umnoška maksimalnog stupnja i broja varijabli, a broj evaluacija je najmanje 20. S druge strane, vrlo velika vjerojatnost pogreške je u slučaju kada imamo skup čiji je kardinalitet barem 10 puta manji od umnoška maksimalnog stupnja polinoma i broja varijabli, i tu vjerojatnost dobivamo već za 10 izvršenih evaluacija. Također možemo zaključiti da se

dm	r	$t = 10$	$t = 20$	$t = 30$	$t = 50$	$t = 100$
10	10	$10 \cdot 10^{-3}$	$106 \cdot 10^{-6}$	$1 \cdot 10^{-6}$	$109 \cdot 10^{-12}$	$12 \cdot 10^{-21}$
10	10^2	$61 \cdot 10^{-12}$	$< 10^{-20}$	$< 10^{-20}$	$< 10^{-20}$	~ 0
10^2	10	~ 1	~ 1	~ 1	~ 1	~ 1
50	10	$935 \cdot 10^{-3}$	$873 \cdot 10^{-3}$	$816 \cdot 10^{-3}$	$713 \cdot 10^{-3}$	$509 \cdot 10^{-3}$
50	10^3	$76 \cdot 10^{-15}$	$< 10^{-20}$	$< 10^{-20}$	~ 0	~ 0

Slika 1.1: Tablica 1

vjerojatnost pogreške s povećanjem evaluacija brže smanjuje u slučaju kada je kardinalitet skupa jednak umnošku maksimalnog stupnja polinoma i broja varijabli.

1.3 Efikasnost i pouzdanost algoritama

Premda se ključni rezultat kojim se bavimo u ovom radu može formulirati samo algebarski, glavne njegove primjene nalaze se u tzv. probabilističkim algoritmima. Već u naslovima članaka J. Schwartza i R. Zippela istaknut je upravo taj aspekt - brzi probabilistički algoritmi za provjeru polinomijalnih identiteta. Ovdje se nećemo detaljno baviti razmatranjem efikasnosti algoritama, no navest ćemo neke napomene u tom smislu. Radi toga potrebno je uvesti nekoliko pojmova, oznaka i objašnjenja.

Djelotvornost algoritma obično se izražava pomoću vremena potrebnog za njegovo izvršenje. Kaže se, primjerice, da se za neki "problem veličine n" određeni algoritam izvršava u vremenu $O(n^2)$. To znači da vrijeme izvršavanja algoritma nije veće od $C \cdot n^2$, pri čemu je C neka konstanta koja ne ovisi o n. Općenito ako su $f(x)$ i $g(x)$ dvije funkcije definirane na nekom podskupu skupa $\mathbb{R}$, piše se $f(x) = O(g(x))$ (kada $x \to \infty$) ako postoje konstante C i N takve da vrijedi $|f(x)| \leq C|g(x)|$ za svaki $x > N$. To zapravo znači da f ne raste brže od g.

Uzmimo primjer množenja dvaju kvadratnih matrica reda n. Standardno izračunavanje umnoška zahtijeva otprilike n^3 aritmetičkih operacija pa se može reći da je "izravni algoritam" tipa $O(n^3)$ za taj problem veličine n. No, postoje algoritmi koji su znatno brži asimptotički, tj. kada n neograničeno raste pa tako postoji algoritam tipa $O(n^{2.376})$ za isti problem. Valja imati u vidu da pritom konstanta C može biti tako velika da algoritam ipak bude od interesa više teorijski nego praktično.

Probabilistički algoritmi

Za razliku od deterministčkih algoritama, koji za jednaki unos podataka uvijek daju jednake izlazne podatke, probabilistički algoritmi mogu pružati različite izlazne rezultate jer se njihova primjena temelji na generatorima slučajnih brojeva. Ovakvi algoritmi često se koriste kako bi se određena tvrdnja provjerila s velikom vjerojatnošću istinitog ishoda i u znatno kraćem vremenu izvršenja u odnosu na deterministički algoritam koji jedini može pružiti potpunu sigurnost rezultata. Kod probabilističkog algoritma podaci za unos biraju se slučajno, ali iz uniformne distribucije, to jest s jednakom vjerojatnosti izbora.

Vratimo se na primjer množenja matrica. Za kvadratne matrice A, B i C reda n s koeficijentima npr. iz polja racionalnih brojeva (ili bilo kojeg drugog polja) potrebno je provjeriti vrijedi li $AB = C$. Pomoću generatora slučajnih brojeva bira se vektor x kao uređena n-torka čije su koordinate 0 ili 1. Takvih vektora ima 2^n pa vjerojatnost izbora bilo kojeg vektora iz $\{0,1\}^n$ iznosi 2^{-n}. Algoritam izračunava vektore $A(Bx)$ i Cx, a to je račun reda $O(n^2)$. Ako se dobiveni vektori za isti x podudaraju, algoritam daje odgovor "DA", u protivnom "NE". Može se pokazati da vjerojatnost pogrešnog odgovora (tj. da bude $C \neq AB$, ali $Cx = ABx$) ne premašuje $\frac{1}{2}$. Samo jedna primjena ovakvog algoritma očito ne daje pouzdan odgovor, no nezavisnim ponavljanjem postupka za iste matrice A, B, C na primjer 50 puta, vjerojatnost pogrešnog odgovora bit će najviše 2^{-50}, što je manje od 10^{-15}, dakle praktički zanemariva. Upravo takve primjere imat ćemo kod primjene Schwartz - Zippelovog teorema.

Poglavlje 2

Schwartz - Zippelov teorem i dokaz

2.1 Problemi evaluacije polinoma i testiranja jednakosti polinoma

Najprije treba precizirati u čemu se sastoji problem ispitivanja ili testiranja jednakosti dvaju polinoma, odnosno testiranja je li neki polinom identički jednak 0. Pritom je ključno pitanje i što točno znači da je polinom ”zadan”. Naime, iako polinom obično zamišljamo napisanim, po definiciji, kao algebarski izraz kojem su koeficijenti zadani elementi nekog polja (ili prstena), u konkretnoj situaciji polinom može biti zadan u nekom drugom obliku [2] koji dopušta evaluaciju za bilo koji izbor vrijednosti varijabli, a da koeficijenti nisu eksplicitno ispisani ili ih nije sasvim lako izračunati.

Promatrat ćemo općenito polinome u n varijabli, ukupnog stupnja d, nad poljem $\mathbb{F}$. Takav polinom $p(x_1, \ldots, x_n)$ je suma članova (monoma) u kojima zbroj eksponenata pojedinih varijabli nije veći od d, a barem jedan član ima stupanj jednak d. Dakle, polinom je suma izraza oblika $\alpha \cdot \prod_{i=1}^{n} x_i^{\beta_i}$ gdje je $\alpha \in \mathbb{F}$, a $\beta_1, \ldots, \beta_n$ su nenegativni cijeli brojevi. Broj različitih mogućih monoma stupnja d jednak je $\binom{d+n-1}{n-1}$, a broj monoma stupnja najviše d jednak je $\binom{d+n}{n} = \binom{d+n}{d}$. Izračunavanje i usporedba svih pojedinih koeficijenata stoga nije uvijek najpraktičniji način kako bi se ustanovilo jesu li dva polinoma jednaka.

Važno je također i nad kakvim poljem je zadan polinom. Nad beskonačnim poljem kao što je $\mathbb{R}$ ili $\mathbb{C}$, polinom je identički jednak 0 (kao preslikavanje) ako i samo ako je to nulpolinom, to jest ako su mu svi koeficijenti jednaki 0. U takvom slučaju jednakost polinoma p i q ekvivalentna je činjenici da je njihova razlika p–q nulpolinom. No, nad konačnim poljem nije tako. Primjerice, polinom $x^2 + x$ poprima vrijednost 0 za svaki x iz polja $\mathbb{F}_2 = \mathbb{Z}_2$, a $x^3 - x$ poprima vrijednost 0 za svaki x iz polja $\mathbb{F}_3 = \mathbb{Z}_3$. Iscrpno ispitivanje polinoma u n varijabli nad konačnim poljem $\mathbb{F}$ zahtijeva $|\mathbb{F}|^n$ evaluacija, što opet može biti vrlo zahtjevno i nepraktično.

Polinom može biti zadan npr. u faktoriziranom obliku ili pomoću determinante, primjerice

$$p(x_1, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & {x_1}^2 & \ldots & {x_1}^{n-1} \\ 1 & x_2 & {x_2}^2 & \ldots & {x_2}^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & {x_n}^2 & \ldots & {x_n}^{n-1} \end{vmatrix}.$$

Tada je p zapravo polinom u n varijabli $x_1, \ldots, x_n$ čiji je ukupni stupanj najviše $n(n-1)$. Lako možemo izabrati numeričke vrijednosti za $x_1, \ldots, x_n$ i evaluirati p u toj točki, jednostavno uvrštavanjem tih brojeva u matricu i računanjem determinante numerički. Međutim može se dogoditi i slučaj da p nema sažeti prikaz u obliku eksplicitne formule. U ovom konkretnom primjeru imamo Vandermondeovu determinantu čija eksplicitna formula nam je poznata $p(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j)$.

Zbog svih navedenih razloga, pokazalo se korisnim razvijati algoritme za testiranje jednakosti dvaju polinoma, odnosno testiranje poprima li polinom vrijednost 0 na cijeloj domeni, koji nisu deterministički nego probabilistički. Cilj je da se evaluacijom polinoma na nekom konačnom skupu vrijednosti ustanovi, s po volji malenom vjerojatnosti pogreške, da polinom nije identički jednak nuli.

2.2 Schwartz - Zippelov teorem

Teorem 2.2.1. *Neka je $\mathbb{K}$ proizvoljno polje, neka je d prirodan broj, te neka je S konačan podskup u polju $\mathbb{K}$. Tada za svaki ne-nul polinom $p(x_1, \ldots, x_n)$ stupnja d u n varijabli s koeficijentima u polju $\mathbb{K}$, broj n-torki $(r_1, r_2, \ldots, r_n) \in S^n$ takvih da vrijedi $p(r_1, r_2, \ldots, r_n) = 0$ nije veći od $d|S|^{n-1}$. Drugim riječima, ako su $r_1, r_2, \ldots, r_n \in S$ nezavisno izabrani slučajno i uniformno, tada vjerojatnost da bude $p(r_1, r_2, \ldots, r_n) = 0$ iznosi najviše $\frac{d}{|S|}$.*

Prije samog dokaza, navedimo nekoliko napomena radi boljeg razumijevanja smisla ove tvrdnje. Ona otprilike govori da ako izračunamo vrijednost polinoma u nekoj nasumičnoj točki, onda je mala vjerojatnost da smo našli upravo nultočku polinoma. To, dakako, ne znači da polinomi nad poljem $\mathbb{R}$ imaju konačno mnogo nultočaka. Čim uzmemo $n \geq 2$, dakle polinom s barem dvije varijable, vidimo da na primjer $p(x_1, x_2) = x_1$, ukupnog stupnja 1, ima beskonačno mnogo nultočaka, jer treba uzeti $x_1 = 0$ i bilo koju vrijednost za x_2 iz $\mathbb{R}$.

Međutim, ako izaberemo podskup $S = \{0, 1\}$ u $\mathbb{R}$, i nasumce izaberemo $x_1, x_2 \in S$, vjerojatnost "pogađanja" nultočke bit će točno $\frac{1}{2}$. Naime, mogući su izbori $(0, 0), (0, 1), (1, 0)$ i $(1, 1)$ od kojih samo prva dva daju nultočke i stoga je tražena vjerojatnost jednaka $\frac{2}{4} = \frac{1}{2}$, što odgovara tvrdnji teorema. Uočimo da tvrdnja ne ovisi o broju varijabli n.

Dokaz. Provodimo matematičkom indukcijom po broju varijabli polinoma. Za $n = 1$ imamo slučaj polinoma u jednoj varijabli, stupnja d, koji znamo da ima najviše d korijena jer se može rastaviti u produkt najviše d ireducibilnih polinoma stupnja 1. Stoga vjerojatnost da x_1 bude nultočka iznosi najviše $\frac{d}{|S|}$.
Neka je sada $n > 1$. Pretpostavimo da se x_1 pojavljuje u najmanje jednom članu polinoma $p(x_1, x_2, \ldots, x_n)$ s ne-nul koeficijentima (ako se ne pojavljuje, preimenujemo varijable). Napišimo $p(x_1, x_2, \ldots, x_n)$ u obliku polinoma u varijabli x_1 s koeficijentima kao polinomima u $x_2, \ldots, x_n$:

$$p(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{k} {x_1}^i p_i(x_2, \ldots, x_n),$$

pri čemu je k maksimalni eksponent od x_1 u polinomu $p(x_1, x_2, \ldots, x_n)$.

Podijelit ćemo n-torke $r_1, r_2, \ldots, r_n$ za koje vrijedi $p(r_1, r_2, \ldots, r_n) = 0$ u dvije klase. Prva klasa, koju ćemo nazvati R_1, sastoji se od n-torki s $p_k(r_2, \ldots, r_n) = 0$. Budući da polinom $p_k(x_2, \ldots, x_n)$ nije identički jednak nuli i stupanj mu iznosi najviše $d - k$, broj mogućih odabira $(r_2, \ldots, r_n)$ prema pretpostavci matematičke indukcije iznosi najviše $(d - k)|S|^{n-2}$, te je stoga $|R_1| \leq (d - k)|S|^{n-1}$.

Drugu klasu R_2 čine preostale n-torke, dakle, one za koje je $p(r_1, r_2, \ldots, r_n) = 0$ ali $p_k(r_2, \ldots, r_n) \neq 0$. Ovu klasu prebrojavamo na sljedeći način: r_2 od r_n možemo izabrati na najviše $|S|^{n-1}$ način, te ako su $r_2, \ldots, r_n$ neke fiksne vrijednosti za koje $p_k(r_2, \ldots, r_n) \neq 0$, tada r_1 mora biti korijen polinoma $q(x_1) = p(x_1, r_2, \ldots, r_n)$ u jednoj varijabli. Taj polinom je stupnja (točno) k, stoga on ima najviše k nultočaka. Tako druga klasa ima najviše $k|S|^{n-1}$ n-torki, što ukupno daje $d|S|^{n-1}$. Time je dokazan korak indukcije, a ujedno i Schwartz - Zippelov teorem. □

Dakle, ako uzmemo skup S čiji će kardinalitet biti barem dvostruko veći od stupnja danog polinoma, moći ćemo ograničiti vjerojatnost pogreške na $\frac{1}{2}$. Međutim, taj iznos možemo i smanjiti na bilo koji po volji malen broj tako što ćemo ponavljati pokus.

Primjena Schwartz - Zippelovog teorema redovito će imati sljedeći oblik. Pretpostavimo da je zadan polinom $p(x_1, \ldots, x_n)$ ukupnog stupnja d i neka je d manji od broja $|\mathbb{K}|$ elemenata polja. Algoritam nezavisno bira slučajne i uniformno distribuirane vrijednosti $r_1, r_2, \ldots, r_n$ iz polja $\mathbb{K}$ odnosno, ako je $\mathbb{K}$ beskonačno polje, iz njegovog dovoljno velikog podskupa S. Ukoliko se dobije $p(r_1, r_2, \ldots, r_n) \neq 0$, algoritam javlja da p nije identički nula i pritom nema mogućnosti pogreške. U suprotnom, ako je $p(r_1, r_2, \ldots, r_n) = 0$, algoritam daje odgovor da je p identički nula. U tom slučaju, teorem pokazuje da vrijednost pogreške nije veća od $\frac{d}{|S|} < 1$. Naravno, ako izaberemo skup S čiji je kardinalitet barem dvostruko veći od stupnja polinoma d, vjerojatnost pogreške neće biti veća od $\frac{1}{2}$.

Vjerojatnost pogreške možemo učiniti po volji malenom tako da ponavljamo više puta isti algoritam. Na taj način, s m ponavljanja možemo vjerojatnost pogreške smanjiti na $\frac{1}{2^m}$ ako je $|S| \geq 2d$. No, čak i ako uzmemo $|S| = d + 1$, ponavljanje algoritma $m = |S|$ puta

smanjuje vjerojatnost pogreške na najviše

$$\left(\frac{m-1}{m}\right)^m \leq \left(1-\frac{1}{m}\right)^m \leq \frac{1}{e}.$$

Poglavlje 3

Primjene Schwartz - Zippelovog teorema

3.1 Savršena sparivanja u grafovima i determinante

Općenito o grafovima

Grafovi su jedna od osnovnih i najčešće primjenjivanih matematičkih struktura. Mnoge se pojave i životne situacije mogu modelirati uz pomoć grafova. Graf se sastoji od točaka i njihovih spojnica. Tako točke mogu biti ljudi u određenom društvu, a spojnice parovi prijatelja, ili točke mogu biti električne komponente, a spojnice električna mreža itd.

Grubo govoreći, graf je familija točaka, koje nazivamo vrhovima, zajedno sa spojnicama među njima, koje nazivamo bridovima. Precizna definicija glasi:

Definicija 3.1.1. *Graf je uređena trojka $G = (V, E, \varphi)$, gdje je V neprazan skup vrhova, E skup bridova koji je disjunktan s V, a φ funkcija koja svakom bridu iz E pridružuje dva, ne nužno različita vrha iz V. Graf često zapisujemo kao par $G = (V, E)$ ili samo G.*

Ako su nekom bridu $e \in E$ pridruženi vrhovi $u, v \in V$, kažemo da su u i v krajevi brida e. Kažemo još i da su vrhovi u i v incidentni s bridom e, da su u i v susjedni vrhovi te pišemo $e = uv$. Bridovi s barem jednim zajedničkim krajem zovu se susjedni bridovi. Brid čiji se krajevi podudaraju zove se petlja, a brid čiji su krajevi različiti naziva se pravi brid ili karika. Dva ili više bridova koji imaju isti par krajeva zovu se višestruki bridovi. Graf koji nema petlji i višestrukih bridova nazivamo jednostavnim grafom. Mi ćemo se ovdje baviti samo jednostavnim grafovima i pod pojmom graf podrazumijevati samo takve grafove.

Da bismo dobili predodžbu o tome kakvim se problemima bavi teorija sparivanja grafova, počnimo s dva jednostavna primjera koja dobro ilustriraju taj problem.

Primjer 3.1.2. *U nekom studentskom domu ostalo je još* 5 *slobodnih soba u koje upravitelj doma treba smjestiti* 5 *studenata prema određenim pravilima. Označimo studente sa* $S_1, S_2, \ldots, S_5$*, a sobe sa* $U_1, U_2, \ldots, U_5$*. Studenta* S_1 *može smjestiti u sobe* U_3 *i* U_4*, studenta* S_2 *u sobu* U_3*, studenta* S_3 *u sobe* U_1*,* U_2 *i* U_3*, studenta* S_4 *u sobe* U_3 *i* U_4 *te studenta* S_5 *u sobe* U_2 *i* U_5*. Ispitajte je li moguće rasporediti studente po sobama tako da su popunjene sve sobe i da njihov smještaj odgovara unaprijed određenim pravilima?*

Primjer 3.1.3. *U dječjoj igraonici majstor treba obojiti* 8 *zidova s* 8 *različitih boja prema određenom pravilu. Označimo boje s* $B_1, B_2, \ldots, B_8$*, a zidove sa* $Z_1, Z_2, \ldots, Z_8$*. Bojom* B_1 *smije obojiti zidove* Z_4 *i* Z_7*, bojom* B_2 *zidove* Z_1, Z_3, Z_5, Z_6 *i* Z_8*, bojom* B_3 *zidove* Z_2*,* Z_4*,* Z_6*, bojom* B_4 *zid* Z_8*, bojom* B_5 *zidove* Z_4 *i* Z_5*, bojom* B_6 *zid* Z_2*, bojom* B_7 *zidove* Z_4*,* Z_6 *i* Z_7 *i bojom* B_8 *zidove* Z_1*,* Z_5*,* Z_7*. Može li to učiniti tako da iskoristi sve boje i da je svaki zid obojan odgovarajućom bojom?*

Ako studente i sobe, odnosno boje i zidove, uzmemo za vrhove grafa, a bridovima spojimo svakog studenta sa slobodnom sobom, odnosno sve odgovarajuće zidove i boje, onda naš problem glasi: odredite maksimalan broj bridova od kojih nikoja dva nisu susjedna. Rješenje prvog primjera možemo dosta brzo odrediti s obzirom da imamo manji broj podataka nego u drugom primjeru. Stavit ćemo u tablicu studente $S_1, \ldots, S_5$ i sobe $U_1, \ldots, U_5$. Znakovi "+" i "-" u tablici označavaju odgovara li student određenoj sobi ili ne. Sada vidimo da u sobu U_5 možemo smjestiti jedino studenta S_5. Nakon toga za sobu U_2 postoji samo jedna mogućnost tj. tamo možemo smjestiti jedino studenta S_3. Međutim, tu dolazi do kontradikcije s činjenicom da u sobu U_1 možemo smjestiti jedino studenta S_3. Dakle, u ovom slučaju ne postoji rješenje, odnosno nije moguće rasporediti studente prema zadanom pravilu tako da popunimo sve sobe.

Sada znamo da prvi primjer nema rješenja, no kasnije ćemo za oba primjera pokazati detaljno rješenje preko determinante određene matrice.

	U_1	U_2	U_3	U_4	U_5
S_1	−	−	+	+	−
S_2	−	−	+	−	−
S_3	+	+	+	−	−
S_4	−	−	+	+	−
S_5	−	+	−	−	+

Slika 3.1: Raspored studenata po sobama

Sparivanje u grafovima

Definicija 3.1.4. *Sparivanje u grafu $G = (V, E)$ je skup bridova $M \subseteq E$ koji su karike i koji nisu međusobno susjedni. Kažemo da su vrhovi u i v spareni u M ako su u i v krajevi nekog brida iz M.*

Ako je $E \neq \emptyset$, onda je svaki jednočlani podskup od E jedan primjer sparivanja u G. No, zanimljivo je naći sparivanje sa što većim brojem bridova. Stoga definiramo:

Definicija 3.1.5. *Sparivanje M u grafu G je maksimalno sparivanje u G ako ne postoji sparivanje u G s većim brojem bridova od broja bridova u M.*

Definicija 3.1.6. *Kažemo da sparivanje M u grafu $G = (V, E)$ zasićuje vrh $v \in V$ ili da je vrh v M-zasićen ako je v kraj nekog brida iz M. U protivnom kažemo da je vrh v M-nezasićen. Kažemo da je sparivanje M savršeno sparivanje ako je svaki vrh iz G M-zasićen.*

Drugim riječima, savršeno sparivanje u grafovima je sparivanje takvo da obuhvaća sve vrhove. U literaturi se savršeno sparivanje često zove Kekuléova struktura, prema njemačkom kemičaru Augustu Kekuléu (1829. – 1896.). Očito je svako savršeno sparivanje ujedno i maksimalno, dok obrat općenito ne vrijedi. Nadalje, broj bridova u savršenom sparivanju je konstantan i iznosi $\frac{|V|}{2}$. Za postojanje savršenog sparivanja nužno je da graf ima paran broj vrhova. No, to je samo nužan, ali ne i dovoljan uvjet za postojanje savršenog sparivanja. Osnovni problem teorije sparivanja jest ispitati postoji li savršeno sparivanje i ako postoji, konstruirati ga. U slučaju da se ne može konstruirati savršeno sparivanje, cilj je konstruirati sva ili bar neka maksimalna sparivanja.

U ovom dijelu vidjet ćemo kako možemo izračunati savršena sparivanja grafova preko determinanti. Koristit ćemo determinante u jednostavnim algoritmima kako bismo testirali situacije u kojima dani graf ima savršeno sparivanje. Osnovni pristup je sličan pristupu ispitivanja množenja matrica. Razmatrat ćemo samo bipartitne grafove.

Sparivanje u bipartitnom grafu

Definicija 3.1.7. *Za graf G kažemo da je bipartitan ili dvodjelan ako se skup njegovih vrhova može podijeliti u dva disjunktna podskupa X i Y tako da svaki brid grafa G ima jedan kraj u X, a drugi u Y. Particija (X, Y) naziva se biparticija grafa G. Bipartitni graf s biparticijom (X, Y) označava se $G(X, Y)$.*

Definicija 3.1.8. *Kažemo da bipartitni graf $G(X, Y)$ ima potpuno sparivanje u X ako postoji sparivanje u G koje zasićuje sve vrhove iz X.*

Potpuno sparivanje, dakle, definira jedno $1-1$ preslikavanje između vrhova iz X i jednog dijela vrhova iz Y koje odgovarajuće vrhove iz X i Y spaja bridom. Stoga za svakih k vrhova iz X mora postojati barem k vrhova iz Y takvih da je svaki susjedan barem jednom od tih k vrhova iz X. To je, dakle, očigledan nužni uvjet za postojanje savršenog sparivanja. Sljedeći teorem kazuje da je to i dovoljan uvjet.

Teorem 3.1.9. *(P. Hall, 1935.) Bipartitni graf G s biparticijom (X, Y) ima potpuno sparivanje ako i samo ako za svaki $S \subseteq X$ vrijedi Hallov uvjet:*

$$|N(S)| \geq |S|,$$

gdje je $N(S) \subseteq Y$ skup svih vrhova grafa G koji su susjedni barem jednom od vrhova iz S.

Ako particije X i Y imaju jednak broj elemenata, onda su potpunim sparivanjem u X zasićeni i svi vrhovi iz Y, pa je riječ o savršenom sparivanju u bipartitnom grafu. O tome govori sljedeći teorem popularno nazvan *Teorem o braku*.

Teorem 3.1.10. *(Teorem o braku) Bipartitni graf G s particijom (X, Y) ima savršeno sparivanje ako i samo ako je $|X| = |Y|$ i $|N(S)| \geq |S|$, za svaki $S \subseteq X$.*

Primjenjujući ovaj teorem na uvodne primjere, lako ćemo odgovoriti na pitanja koja se u njima postavljaju. Označimo li sa $S = \{S_1, S_2, S_3, S_4, S_5\}$ skup svih studenata, a sa $U = \{U_1, U_2, U_3, U_4, U_5\}$ skup svih soba, tada problem možemo predstaviti bipartitnim grafom $G = (S, U)$, a pitanje je li moguće rasporediti studente u sobe tako da su sve sobe popunjene i da se poštuje pravilo raspoređivanja u sobe, ekvivalentno je pitanju postoji li u tom grafu savršeno sparivanje. Pogledajmo skup $T = \{S_1, S_2, S_4\} \subseteq S$. Kako studenta S_1 možemo smjestiti u sobe U_3, U_4, studenta S_2 u sobu U_3, a studenta S_4 u sobe U_3, U_4, tako je skup svih vrhova koji su susjedni skupu T jednak $N(T) = U_3, U_4$. Stoga je $|N(T)| < |T|$, pa nije zadovoljen Hallov uvjet, što znači da ne postoji savršeno sparivanje u ovom grafu. Dakle, nije moguće rasporediti studente u sobe tako da sve sobe budu popunjene, a da se pritom poštuje zadano pravilo za raspoređivanje studenata po sobama. No, u drugom primjeru ćemo se susresti sa drugačijom situacijom što ćemo kasnije detaljnije pokazati.

Sada ćemo vidjeti kako možemo egzistenciju (postojanje) savršenog sparivanja u grafovima izraziti preko determinante [4]. Neka je zadan bipartitni graf G. Njegove vrhove podijelit ćemo u dva skupa $\{u_1, u_2, \ldots, u_n\}$ i $\{v_1, v_2, \ldots, v_n\}$ tako da su bridovi uvijek sadržani u dvjema klasama, nikada u jednoj. Oba skupa su iste veličine, inače u grafu ne postoji savršeno sparivanje. Neka m označava broj bridova u grafu G i neka je S_n skup svih permutacija skupa $\{1, 2, \ldots, n\}$. Tada svako savršeno sparivanje grafa G odgovara permutaciji $\pi \in S_n$. To možemo zapisati i u sljedećem obliku: $\{\{u_1, v_{\pi(1)}\}, \{u_2, v_{\pi(2)}\}, \ldots, \{u_n, v_{\pi(n)}\}\}$.

Determinanta pomoću koje možemo izraziti postojanje savršenog sparivanja u grafu bit će determinanta matrice $A = (a_{ij})$ reda n čiji koeficijenti nisu brojevi nego varijable oblika x_{ij}. Definiramo matricu A na sljedeći način:

$$a_{ij} := \begin{cases} x_{ij}, & \text{ako } \{u_i, v_j\} \in E(G), \\ 0, & \text{inače, tj. ako } \{u_i, v_j\} \text{ nije brid u G.} \end{cases}$$

Determinanta matrice A je polinom u m varijabli x_{ij}, pa iz definicije determinante dobivamo:

$$\begin{aligned} detA &= \sum_{\pi \in S_n} sgn(\pi) \cdot a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)} \\ &= \sum_{\pi \text{ označava savršeno sparivanje u G}} sgn(\pi) \cdot x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{n,\pi(n)}. \end{aligned}$$

Naime, očito će članovi determinante, pridruženi permutacijom, koji ne pripadaju savršenom sparivanju biti jednaki 0, budući da barem jedan vrh u_i neće biti spojen s nekim vrhom $v_{\pi(i)}$ pa će odgovarajući koeficijent matrice biti jednak 0. Stoga se $detA$ svodi na sumu samo onih polinoma stupnja n koji su zadani savršenim sparivanjima.

Prikažimo sada početna dva primjera tablicom koja se sastoji od varijabli, odnosno za svaki odgovarajući par ćemo zapisati pripadajuću varijablu, a u ostala polja upisujemo nule na sljedeći način:

	U_1	U_2	U_3	U_4	U_5
S_1	0	0	x_{13}	x_{14}	0
S_2	0	0	x_{23}	0	0
S_3	x_{31}	x_{32}	x_{33}	0	0
S_4	0	0	x_{43}	x_{44}	0
S_5	0	x_{52}	0	0	x_{55}

	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8
B_1	0	0	0	x_{14}	0	0	x_{17}	0
B_2	x_{21}	0	x_{23}	0	x_{25}	x_{26}	0	x_{28}
B_3	0	x_{32}	0	x_{34}	0	x_{36}	0	0
B_4	0	0	0	0	0	0	0	x_{48}
B_5	0	0	0	x_{54}	x_{55}	0	0	0
B_6	0	x_{62}	0	0	0	0	0	0
B_7	0	0	0	x_{74}	0	x_{76}	x_{77}	0
B_8	x_{81}	0	0	0	x_{85}	0	x_{87}	0

Lema 3.1.11. *Polinom detA je identički nula ako i samo ako u grafu G ne postoji savršeno sparivanje.*

Dokaz. Već smo uočili da su u *detA* različiti od 0 samo članovi koji odgovaraju savršenim sparivanjima. Dakle, ako u grafu G nema savršenog sparivanja, onda je $detA = 0$ identički, to jest *detA* je nulpolinom. Obrnuto, pokažimo da ako u grafu G postoji savršeno sparivanje, onda *detA* nije identički jednaka 0, to jest postoji izbor vrijednosti varijabli x_{ij} tako da se uvrštavanjem u polinom *detA* dobiju vrijednosti različite od 0. Izaberimo permutaciju π koja definira savršeno sparivanje (takvih može biti više). Nadalje uvrstimo $X_{i\pi(i)} = 1$ za svaki $i = 1, 2, \ldots, n$, dok za sve ostale x_{ij} uvrstimo 0. Tada imamo:

$$sgn(\pi) \cdot x_{1\pi(1)} \cdot \cdots \cdot x_{n\pi(n)} = sgn(\pi) = \pm 1.$$

Za svaku drugu permutaciju $\sigma \neq \pi$ postoji i takav da je $\pi(i) \neq \sigma(i)$ pa je tada $x_{i\sigma(i)} = 0$. Dakle, član zadan pemutacijom σ jednak je 0 za svaki $\sigma \neq \pi$. To znači da je za naš izbor vrijednosti x_{ij} $detA = \pm 1$, različita od 0. □

Prema prethodnom teoremu vidimo da sada možemo odrediti rješenje početna dva primjera računajući determinante pripadajućih matrica. Pripadajuće matrice dobijemo iz prethodno navedenih tablica varijabli. Označimo sa A determinatu prvog primjera sa B determinantu drugog primjera.

$$detA = \begin{vmatrix} 0 & 0 & x_{13} & x_{14} & 0 \\ 0 & 0 & x_{23} & 0 & 0 \\ x_{31} & x_{32} & x_{33} & 0 & 0 \\ 0 & 0 & x_{43} & x_{44} & 0 \\ 0 & x_{52} & 0 & 0 & x_{55} \end{vmatrix} = x_{55} \cdot \begin{vmatrix} 0 & 0 & x_{13} & x_{14} \\ 0 & 0 & x_{23} & 0 \\ x_{31} & x_{32} & x_{33} & 0 \\ 0 & 0 & x_{43} & x_{44} \end{vmatrix} = x_{55} \cdot (-x_{23}) \cdot \begin{vmatrix} 0 & 0 & x_{14} \\ x_{31} & x_{32} & 0 \\ 0 & 0 & x_{44} \end{vmatrix} =$$

$$= x_{55} \cdot (-x_{23}) \cdot (-x_{31}) \cdot \begin{vmatrix} 0 & x_{14} \\ 0 & x_{44} \end{vmatrix} = x_{23} \cdot x_{31} \cdot x_{55} \cdot (0 \cdot x_{44} - x_{14} \cdot 0) = x_{23} \cdot x_{31} \cdot x_{55} \cdot 0 = 0.$$

$$detB = \begin{vmatrix} 0 & 0 & 0 & x_{14} & 0 & 0 & x_{17} & 0 \\ x_{21} & 0 & x_{23} & 0 & x_{25} & x_{26} & 0 & x_{28} \\ 0 & x_{32} & 0 & x_{34} & 0 & x_{36} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{48} \\ 0 & 0 & 0 & x_{54} & x_{55} & 0 & 0 & 0 \\ 0 & x62 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_{74} & 0 & x_{76} & x_{77} & 0 \\ x_{81} & 0 & 0 & 0 & x_{85} & 0 & x_{87} & 0 \end{vmatrix} = -x_{23} \cdot \begin{vmatrix} 0 & 0 & x_{14} & 0 & 0 & x_{17} & 0 \\ 0 & x_{32} & x_{34} & 0 & x_{36} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x_{48} \\ 0 & 0 & x_{54} & x_{55} & 0 & 0 & 0 \\ 0 & x_{62} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & x_{74} & 0 & x_{76} & x_{77} & 0 \\ x_{81} & 0 & 0 & x_{85} & 0 & x_{87} & 0 \end{vmatrix} =$$

$$= (-x_{23}) \cdot x_{48} \cdot \begin{vmatrix} 0 & 0 & x_{14} & 0 & 0 & x_{17} \\ 0 & x_{32} & x_{34} & 0 & x_{36} & 0 \\ 0 & 0 & x_{54} & x_{55} & 0 & 0 \\ 0 & x_{62} & 0 & 0 & 0 & 0 \\ 0 & 0 & x_{74} & 0 & x_{76} & x_{77} \\ x_{81} & 0 & 0 & x_{85} & 0 & x_{87} \end{vmatrix} = (-x_{23}) \cdot x_{48} \cdot (-x_{81}) \cdot \begin{vmatrix} 0 & x_{14} & 0 & 0 & x_{17} \\ x_{32} & x_{34} & 0 & x_{36} & 0 \\ 0 & x_{54} & x_{55} & 0 & 0 \\ x_{62} & 0 & 0 & 0 & 0 \\ 0 & x_{74} & 0 & x_{76} & x_{77} \end{vmatrix} =$$

$$= (-x_{23}) \cdot x_{48} \cdot (-x_{81}) \cdot x_{55} \cdot \begin{vmatrix} 0 & x_{14} & 0 & x_{17} \\ x_{32} & x_{34} & x_{36} & 0 \\ x_{62} & 0 & 0 & 0 \\ 0 & x_{74} & x_{76} & x_{77} \end{vmatrix} = (-x_{23}) \cdot x_{48} \cdot (-x_{81}) \cdot x_{55} \cdot x_{62} \cdot \begin{vmatrix} x_{14} & 0 & x_{17} \\ x_{34} & x_{36} & 0 \\ x_{74} & x_{76} & x_{77} \end{vmatrix} =$$

$$= (-x_{23}) \cdot x_{48} \cdot (-x_{81}) \cdot x_{55} \cdot x_{62} \cdot (x_{14}x_{36}x_{77} + x_{17}x_{34}x_{76} - x_{17}x_{36}x_{74}) =$$

$$= x_{14}x_{23}x_{36}x_{48}x_{55}x_{62}x_{77}x_{81} + x_{17}x_{23}x_{34}x_{48}x_{55}x_{62}x_{76}x_{81} - x_{17}x_{23}x_{36}x_{48}x_{55}x_{62}x_{74}x_{81}.$$

Za polinom *detA* smo već prije uočili da je jednak nulpolinomu, to jest da ne postoji savršeno sparivanje. Polinom *detB* smo sada izračunali te iz dobivenog rezultata vidimo da je različit od nulpolinoma, štoviše, dobili smo tri polinoma u varijablama x_{ij}, odnosno tri rješenja.

Sada bismo željeli testirati je li *detA* jednaka nulpolinomu, ali bez eksplicitnog računanja *detA* kao polinoma. Naime, taj polinom ima onoliko članova različitih od 0 koliki je broj savršenih sparivanja, a taj broj može biti prevelik za efikasno izračunavanje. Međutim, ako za sve varijable x_{ij} uvrstimo konkretne brojčane vrijednosti, može se izračunati pripadna vrijednost determinante, na primjer Gaussovom metodom eliminacije. Dakle, zamislimo da vrijednosti determinante dobivamo nekim postupkom koji zahtijeva unos (samo) konkretnih brojeva, odnosno da nam taj postupak daje vrijednosti *detA* kao vrijednosti polinoma u bilo kojoj zadanoj točki. Za razliku od polinoma, ako bismo imali neku općenitu funkciju, ovakvim pristupom (izračunavanje vrijednosti u zadanim točkama, bez ikakvih

drugih podataka) nikad ne bismo mogli biti sigurni da je ta funkcija identički jednaka 0 dok god ne provjerimo njezinu vrijednost u *svim* točkama.

Vratimo se još na bipartitne grafove. Pretpostavimo da u grafu G postoji savršeno sparivanje i da je $detA$ polinom stupnja n različit od nul-polinoma. Schwartz - Zippelov teorem nam kaže da ako izračunamo $detA$ za slučajno i nezavisno odabrane vrijednosti varijabli x_{ij} iz skupa $S := \{1, 2, \ldots, n\}$, onda vjerojatnost da dobijemo nulu nije veća od $\frac{1}{2}$. Međutim, kako bismo odredili je li determinanta jednaka nuli za danu supstituciju, trebali bismo je izračunati. No, u takvom izračunu mogu nam se pojaviti ogromni brojevi, sa otprilike n znamenaka, pa možemo zaključiti da je zapravo bolje raditi s konačnim poljima.

Najjednostavniji način je taj da izaberemo prost broj p takav da vrijedi $2n \leq p < 4n$ te računamo nad konačnim poljem $\mathbb{F}_p$ cijelih brojeva modulo p. Koristeći Gaussovu metodu eliminacije za računanje determinante, dobivamo vjerojatnosni algoritam za testiranje egzistencije savršenog sparivanja u bipartitnom grafu koji se izvršava u $O(n^3)$ vremenu. Vjerojatnost neuspjeha tog algoritma iznosi najviše $\frac{1}{2}$. Kao i obično, vjerojatnost neuspjeha može se smanjiti na 2^{-k} ponavljajući algoritam k puta. Determinanta se također može računati algoritmom za brzo množenje matrica i u tom slučaju dobivamo najbrži mogući asimptotski algoritam za testiranje egzistencije savršenog sparivanja u bipartitnom grafu, s vremenom izvršavanja $O(n^{2.376})$.

Spomenuti algoritam je u praksi mnogo brži, te može odrediti postoji li savršeno sparivanje, ali nam ne pokazuje kako točno izgleda to sparivanje. S druge strane, ovaj algoritam može se implementirati veoma uspješno na paralelna računala, te niti jedan poznati pristup ne daje usporedivo brže paralelne algoritme.

3.2 Asocijativnost grupoida

Svojstvo asocijativnosti jedno je od najvažnijih svojstava koje može imati binarna operacija i koje u velikoj mjeri olakšava izvođenje operacija kao što su zbrajanje i množenje u bilo kojem polju, zbrajanje u vektorskom prostoru, kompozicija funkcija, množenje matrica i tako dalje. Postoje i specifične binarne operacije koje nemaju svojstvo asocijativnosti, na primjer vektorsko množenje u prostoru V^3. Podsjetimo se osnovnih definicija:

Definicija 3.2.1. *Neka je X neprazan skup i $\odot : X \times X \to X$ bilo koje preslikavanje, tada $\odot$ nazivamo binarnom operacijom na skupu X, a uređeni par $(X, \odot)$ nazivamo grupoid.*

Sliku uređenog para $(x, y) \in X \times X$ u preslikavanju $\odot$ označavamo jednostavno s $x \odot y$. Najčešće oznake za binarnu operaciju su $+, \cdot, \circ, \times, *$, itd.

Kažemo da je binarna operacija $\odot$ na skupu X asocijativna ako za sve $x, y, z \in X$ vrijedi:

$$(x \odot y) \odot z = x \odot (y \odot z).$$

Grupoid u kojem vrijedi asocijativnost naziva se polugrupa. Iako smo naviknuti da je svojstvo asocijativnosti obično ispunjeno u grupoidu, to općenito nije tako. Uređenu trojku $(x, y, z) \in X^3$, pri čemu je $(X, \odot)$ grupoid, nazivat ćemo asocijativnom ako vrijedi $(x \odot y) \odot z = x \odot (y \odot z)$, a u suprotnom neasocijativnom.

Nije uvijek sasvim lako ustanoviti koliko je trojki u grupoidu asocijativno a koliko nije, čak i ako je $(X, \odot)$ konačan grupoid. Uzmimo da X ima n elemenata i ako pretpostavimo da je operacija $\odot$ zadana svojom tablicom, iz te tablice nije lako očitati vrijedi li asocijativnost za sve uređene trojke. Naprotiv, primjerice komutativnost binarne operacije lako je prepoznatljiva iz simetričnog oblika tablice operacije s obzirom na dijagonalu. Broj asocijativnih trojki u grupoidu može biti vrlo malen tako da ne možemo zaključiti je li grupoid asocijativan ako je "velika većina" pojedinačnih trojki asocijativna.

Uzmimo sada jednostavan primjer binarne operacije na skupu od 4 elementa, $S = \{x_1, x_2, x_3, x_4\}$. Za tako definiran skup S tablica izgleda ovako:

$\odot$	x_1	x_2	x_3	x_4
x_1	x_1	x_1	x_1	x_1
x_2	x_1	x_2	x_3	x_4
x_3	x_1	x_3	x_1	x_3
x_4	x_1	x_4	x_1	x_2

Izravnom provjerom možemo ustanoviti da je svega jedna trojka iz S^3, od ukupno 64 trojke, asocijativna i to (x_4, x_4, x_3). Dakle, općenito trebamo provjeriti asocijativnost svih n^3 trojki, a za svaki izbor $(x, y, z) \in X^3$ potrebna su po dva očitanja vrijednosti u tablici za $(x \odot y) \odot z$ i $x \odot (y \odot z)$ što ukupno iznosi $4n^3$. To znači da je utrošak vremena za ovakav postupak reda veličine n^3. Ako bismo pokušali ubrzati testiranje jednostavno ponavljanjem nasumičnog izbora trojki $(x, y, z) \in X^3$ za koje se provjerava jesu li asocijativne, to općenito ne bi dalo dobre rezultate. U prethodnom primjeru imamo svega jednu neasocijativnu trojku, pa je vjerojatnost izbora jedne od njih svega $\frac{1}{64}$. Međutim, izložit ćemo jedan znatno pouzdaniji probabilistički algoritam za provjeru asocijativnosti koji zahtjeva bitno manje vremena za izvršenje, reda svega n^2.

Teorem 3.2.2. *Postoji probabilistički algoritam koji "prihvaća" binarnu operaciju $\odot$ na n-članom skupu danom tablicom, čije je vrijeme izvršenja najviše $O(n^2)$, i koji daje jedan od odgovora "DA" ili "NE". Ako je operacija $\odot$ asocijativna, odgovor je uvijek "DA". Ako operacija $\odot$ nije asocijativna onda odgovor može biti ili "DA" ili "NE", ali odgovor "DA" se u tom slučaju pojavljuje s vjerojatnošću koja iznosi najviše $\frac{1}{2}$.*

Za dokaz ovog teorema najprije treba izabrati prikladno polje $\mathbb{K}$, koje ima barem 7 elemenata. Glavna ideja algoritma jest u tome da se na vektorskom prostoru $\mathbb{K}^X$ definira binarna operacija $\boxdot$ koja će biti proširenje operacije $\odot$, a u kojoj će broj neasocijativnih

trojki (čak i ako u $(X, \odot)$ postoji samo jedna takva) biti znatno veći pa će se povećati vjerojatnost da se nasumičnim izborom "pogodi" neasocijativna trojka. Pretpostavljamo tako da se operacije zbrajanja i množenja u polju $\mathbb{K}$ izvršavaju u konstantnom vremenu. Neka je, dakle, $\mathbb{K}^X$ vektorski prostor uređenih n-torki skalara iz $\mathbb{K}$, pri čemu je $|X| = n$. Te n-torke možemo indeksirati elementima iz X, to jest uvesti neki poredak $x_1, x_2, \ldots, x_n$ u X i onda svakom $x_i \in X$ pridružiti i-tu koordinatu uređene n-torke. Nadalje, zadajemo preslikavanje $e : X \to \mathbb{K}^X$, tako da vektor $e(x_i)$ bude vektor kojemu je i-ta koordinata jednaka 1, a sve ostale su 0. Na taj način definirana je bijekcija između skupa X i standardne (kanonske) baze prostora $\mathbb{K}^X$. Na prostoru $\mathbb{K}^X$ sada ćemo zadati binarnu operaciju $\boxdot$ na prirodan način, kao "linearno proširenje" binarne operacije $\odot$. Za vektore $u, v \in \mathbb{K}^X$, koji imaju svoje jednoznačne prikaze oblika:

$$u = \sum_{i=1}^{n} \alpha_i e(x_i), \qquad v = \sum_{j=1}^{n} \beta_j e(x_j),$$

definiramo:

$$u \boxdot v = \left(\sum_{i=1}^{n} \alpha_i e(x_i) \right) \boxdot \left(\sum_{j=1}^{n} \beta_j e(x_j) \right) = \sum_{i,j=1}^{n} \alpha_i \beta_j e(x_i \odot x_j).$$

Ovakvom definicijom operacije $\boxdot$ postižemo da se linearne kombinacije "množe" član po član, jer najprije dobivamo:

$$\sum_{i,j=1}^{n} (e(x_i) \odot e(x_j)),$$

a onda zamijenimo $e(x_i) \odot e(x_j) = e(x_i \odot x_j)$. Na taj način $\boxdot$ je doista "linearno proširenje" od $\odot$, jer $e(x_i) \boxdot e(x_j) = e(x_i) \odot e(x_j) = e(x_i \odot x_j)$. Izravno se može primjeniti da ako je (x, y, z) asocijativna, odnosno neasocijativna trojka u grupoidu $(X, \odot)$ onda je $(e(x), e(y), e(z))$ asocijativna, odnosno neasocijativna trojka u grupoidu $(\mathbb{K}^X, \boxdot)$.

Naime iz:

$$(x \odot y) \odot z = x \odot (y \odot z)$$

slijedi

$$e((x \odot y) \odot z) = e(x \odot (y \odot z))$$

i dalje iz

$$e(x \odot y) \boxdot e(z) = e(x) \boxdot e(y \odot z)$$

dobivamo

$$(e(x) \boxdot e(y)) \boxdot e(z) = e(x) \boxdot (e(y) \boxdot e(z)).$$

Dakako, u slučaju $(x \odot y) \odot z \neq x \odot (y \odot z)$, budući da je e bijekcija imamo:

$$(x \odot y) \odot z \neq x \odot (y \odot z)$$

slijedi

$$e((x \odot y) \odot z) \neq e(x \odot (y \odot z))$$

i dalje iz

$$e(x \odot y) \boxdot e(z) \neq e(x) \boxdot e(y \odot z)$$

dobivamo

$$(e(x) \boxdot e(y)) \boxdot e(z) \neq e(x) \boxdot (e(y) \boxdot e(z)).$$

Uočimo da ako je na primjer $|\mathbb{K}| = 7$ (što je najmanja moguća vrijednost za polje s barem 6 elemenata) onda skup $\mathbb{K}^X$ ima 7^n elemenata.

Opišimo sada algoritam za testiranje asocijativnosti. Fiksiramo podskup $S \subset \mathbb{K}$ koji se sastoji od 6 elemenata:

1. korak: Za svaki $x_i \in X$, izaberemo slučajno i uniformno elemente $\alpha_i, \beta_i, \gamma_i \in S$, pri čemu su ti izbori nezavisni.

2. korak: Neka je $u := \sum_{i=1}^{n} \alpha_i e(x_i)$, $v := \sum_{j=1}^{n} \beta_j e(x_j)$ i $w := \sum_{k=1}^{n} \gamma_k e(x_k)$.

3. korak: Izračunamo vektore $(u \boxdot v) \boxdot w$ i $u \boxdot (v \boxdot w)$. Ako su oni jednaki, odgovor glasi "DA", a ako su različiti, odgovor glasi "NE".

Za dana dva proizvoljna vektora $u, v \in \mathbb{K}^X$, vektor $u \boxdot v$ možemo izračunati iz definicije, pri čemu ćemo $O(n^2)$ puta koristiti tablicu operacije $\odot$ i $O(n^2)$ operacija u polju $\mathbb{K}$. Ako pretpostavimo da je za pojedinu operaciju u $\mathbb{K}$ potrebno konstantno vrijeme, očito je da će se algoritam izvršavati u vremenu $O(n^2)$. Jasno je da ćemo za neasocijativnu trojku (x, y, z) dobiti također neasocijativne trojke vektora $(\alpha e(x), \beta e(y), \gamma e(z))$ za svaki izbor $\alpha, \beta, \gamma \in \mathbb{K} \setminus \{0\}$. Na taj način ukupni broj neasocijativnih trojki u $\mathbb{K}^X$ svakako je mnogo veći od onog u X, no budući da smo značajno povećali i ukupni broj trojki, jer $|\mathbb{K}^X| = |K|^n$, pitanje je koliki je relativni udio neasocijativnih trojki u grupoidu $(\mathbb{K}^X, \boxdot)$. Odgovor je sadržan u sljedećoj tvrdnji: Ako operacija $\odot$ nije asocijativna i u, v, w su slučajno odabrani kao i u algoritmu, onda $(u \boxdot v) \boxdot w \neq u \boxdot (v \boxdot w)$ s vjerojatnošću barem $\frac{1}{2}$.

Očito preostaje dokazati još samo ovu tvrdnju kako bi dokaz teorema bio potpun.

Dokaz. Fiksirajmo neasocijativnu uređenu trojku $(a, b, c) \in X^3$. Dakako, $a, b, c \in \{x_1, x_2, \ldots, x_n\}$ i neki od tih elemenata mogu se ponavljati u trojki (a, b, c). Takav je slučaj i u našem primjeru s $n = 4$.

Svakom od elemenata a, b, c pridružuju se po tri skalara iz S. Zamislimo da su α_a, β_b i γ_c skalari koji će se izabrati posljednji, nakon što su izabrane konkretne vrijednosti za

sve ostale $\alpha_i, \beta_j, \gamma_k \in S$. U našem primjeru, budući da je (x_4, x_4, x_3) jedina neasocijativna trojka, to znači da se posljednji biraju α_4, β_4 i γ_3. Pokazat ćemo da ako fiksiramo sve $\alpha_x, \beta_y, \gamma_z$, $x \neq a$, $y \neq b$, $z \neq c$ kao potpuno proizvoljne vrijednosti, a zatim slučajno odaberemo α_a, β_b i γ_c, onda će vjerojatnost da je $(u \boxdot v) \boxdot w \neq u \boxdot (v \boxdot w)$ iznositi barem $\frac{1}{2}$. Budući da je $(a \odot b) \odot c \neq a \odot (b \odot c)$ za očekivati je da će se ovi vektori razlikovati u koeficijentima uz vektor $e(r)$, pri čemu je $r = (a \odot b) \odot c \in X$. Pokazat ćemo da se ti koeficijenti doista razlikuju, s vjerojatnošću barem $\frac{1}{2}$.

Pri izračunavanju vektora $(u \boxdot v) \boxdot w$ dobivamo najprije $n \cdot n \cdot n = n^3$ umnožaka od kojih će se formirati izrazi koji su koeficijenti uz $e(x_1), e(x_2), \ldots, e(x_n)$. Promatramo li te izraze kao polinome u tri varijable α_a, β_b i γ_c, uočavamo da ćemo samo uz vektor $e(r)$ dobiti polinom s članom stupnja 3, a to je $\alpha_a\beta_b\gamma_c$ jer $(a \odot b) \odot c = r$. Ostali članovi uz $e(r)$ su stupnja najviše 2.

Na drugoj strani, u vektoru $u \boxdot (v \boxdot w)$ zbog $a \odot (b \odot c) \neq r$ koeficijent uz vektor $e(r)$ neće sadržavati monom $\alpha_a\beta_b\gamma_c$ i bit će to polinom stupnja najviše 2 u varijablama α_a, β_b i γ_c. Označimo te koeficijente uz $e(r)$ na lijevoj i na desnoj strani s $f(\alpha_a, \beta_b, \gamma_c)$ i $g(\alpha_a, \beta_b, \gamma_c)$. Njihova razlika nije nulpolinom, a po Schwartz - Zippelovom teoremu vjerojatnost da se slučajnim izborom $\alpha_a, \beta_b, \gamma_c \in S$ dobiju jednake vrijednosti polinoma, odnosno vrijednost njihove razlike 0, nije veća od $\frac{3}{|S|} = \frac{1}{2}$. Time je tvrdnja dokazana. □

Ilustrirajmo još prethodno razmatranje na našem primjeru grupoida s $n = 4$. Imamo $(x_4 \odot x_4) \odot x_3 = x_2 \odot x_3$, $x_4 \odot (x_4 \odot x_3) = x_4 \odot x_1 = x_1$. Dakle, $r = x_3$. Sada je

$$u = \alpha_1 e(x_1) + \alpha_2 e(x_2) + \alpha_3 e(x_3) + \alpha_4 e(x_4),$$

$$v = \beta_1 e(x_1) + \beta_2 e(x_2) + \beta_3 e(x_3) + \beta_4 e(x_4),$$

$$w = \gamma_1 e(x_1) + \gamma_2 e(x_2) + \gamma_3 e(x_3) + \gamma_4 e(x_4).$$

Kako bismo istaknuli da su α_4, β_4 i γ_3 trenutačno još uvijek varijable, za njih pišemo samo α, β, i γ. U vektoru $(u \boxdot v) \boxdot w$ izdvojit ćemo samo komponentu uz $e(x_3)$.

Izračunavanjem koeficijenata uz vektor $e(x_3)$ u tom primjeru dobivamo da odgovarajuća komponenta u vektoru $(u \boxdot v) \boxdot w$ glasi:

$$(\alpha_2\beta_2\gamma_3 + \alpha_2\beta_3\gamma_2 + \alpha_2\beta_3\gamma_4 + \alpha_3\beta_2\gamma_2 + \alpha_3\beta_2\gamma_4 + \alpha_3\beta_4\gamma_2 + \alpha_3\beta_4\gamma_4 + \alpha_4\beta_4\gamma_3)e(x_3),$$

dok u vektoru $u \boxdot (v \boxdot w)$ glasi:

$$(\alpha_2\beta_2\gamma_3 + \alpha_2\beta_3\gamma_2 + \alpha_2\beta_3\gamma_4 + \alpha_3\beta_2\gamma_2 + \alpha_3\beta_2\gamma_4 + \alpha_3\beta_4\gamma_2 + \alpha_3\beta_4\gamma_4)e(x_3).$$

Uočavamo da se koeficijenti uz $e(x_3)$ razlikuju samo za član $\alpha_4\beta_4\gamma_3$. Pritom, dok vrijednosti α_4, β_4 i γ_3 smatramo varijablama, u skladu s dokazom naše tvrdnje imamo polinom stupnja 3 s jedne strane, a polinom stupnja 1 s druge strane. U ovom primjeru, razlika tih polinoma jednostavno je monom $\alpha_4\beta_4\gamma_3$, zato što u grupoidu $(X, \odot)$ postoji samo jedna neasocijativna trojka.

3.3 Prebrojavanje kompozicija

Razmotrit ćemo sljedeći algoritamski problem: Neka je dan skup P permutacija skupa $\{1, 2, \ldots, n\}$, te bismo željeli izračunati kardinalitet skupa $P \circ P := \{\sigma \circ \tau : \sigma, \tau \in P\}$ koji sadrži sve kompozicije parova permutacija skupa P. Prisjetit ćemo se najprije definicije permutacije.

Definicija 3.3.1. *Neka je n proizvoljan prirodan broj. Permutacija skupa $\{1, 2, \ldots, n\}$ je bijektivno preslikavanje $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.*

Na primjer, za $n = 4$, možemo imati $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 4$ i $\sigma(4) = 1$. Uobičajeno je zapisivati permutacije tako da njezine vrijednosti zapišemo u redak, kao na primjer, u našem slučaju bi zapisali $\sigma = (3, 2, 4, 1)$. Tako prikazanu permutaciju, kao niz sa indeksima iz skupa $\{1, 2, \ldots, n\}$ također možemo pohraniti u računalo.

Permutacija je, kao što smo već prethodno spomenuli, definirana kao preslikavanje. Kako bismo dobili kompoziciju $\rho := \sigma \circ \tau$ dvaju permutacija σ i τ najprije primijenimo τ a zatim σ, te tako dobijemo $\rho(i) = \sigma(\tau(i))$. Na primjer, neka je σ definirana ne prethodni način i $\tau = (2, 3, 4, 1)$ dobijemo $\sigma \circ \tau = (2, 4, 1, 3)$, dok je $\tau \circ \sigma = (4, 3, 1, 2)$. Zaključujemo da je $\tau \circ \sigma \neq \sigma \circ \tau$. Koristeći prikaz preko niza, kompoziciju možemo izračunati u $O(n)$ vremenu. Prisjetit ćemo se još što znamo o kompoziciji permutacija.

Definicija 3.3.2. *Skup svih permutacija skupa $\{1, 2, \ldots, n\}$ zajedno sa binarnom operacijom kompozicije čini grupu koju nazivamo simetrična grupa, a označavamo ju S_n.*

Simetrična grupa je vrlo važan objekt u teoriji grupa, kao zaseban pojam, te također iz razloga što se svaka konačna grupa može prikazati kao podgrupa neke simetrične grupe S_n. Problem efikasnog računanja $|P \circ P|$ je prirodno jednostavno pitanje koje se postavlja u algoritamskoj teoriji brojeva. Koliko velik može biti skup $P \circ P$? Jedan ekstremni slučaj je kada P čini podgrupu grupe S_n, konkretnije, ako $\sigma \circ \tau \in P$ za sve $\sigma, \tau \in P$ onda $|P \circ P| = |P|$.

Drugi ekstremni slučaj je taj da su kompozicije disjunktne, to jest, $\sigma_1 \circ \tau_1 \neq \sigma_2 \circ \tau_2$ ako i samo ako $\sigma_1, \sigma_2, \tau_1, \tau_2 \in P$ i $(\sigma_1, \tau_1) \neq (\sigma_2, \tau_2)$, te tada vrijedi $|P \circ P| = |P|^2$. Neposredan način pronalaženja $|P \circ P|$ je da izračunamo kompoziciju $\sigma \circ \tau$ za sve $\sigma, \tau \in P$, dobivajući pri tome listu od $|P|^2$ permutacija u $O(|P|^2 n)$ vremenu. Na toj listi, neke permutacije možda će se pojaviti nekoliko puta. Standardni algoritamski pristup računanju broja disjunktnih permutacija na spomenutoj listi je taj da se permutacije sortiraju prema leksikografskom poretku, a zatim se jednim prolaskom po sortiranoj listi izbace one permutacije koje se pojavljuju više puta.

Uz malo domišljatosti, sortiranje može biti izvršeno u $O(|P|^2 n)$ vremenu. Za sad nećemo ulaziti u detalje prethodnog algoritma jer je naš cilj razmotriti drugi algoritam. Nije jednostavno doći do asimptotski bržeg algoritma. Međutim, korištenjem nekih alata, možemo

to učiniti bolje, uz uvjet da toleriramo zanemarivo malu vjerojatnost pogreške. Da bismo razvili brži algoritam, najprije ćemo kompoziciju permutacija dovesti u vezu sa skalarnim produktom pojedinih vektora. Neka su $x_1, x_2, \ldots, x_n$ i $y_1, y_2, \ldots, y_n$ dane varijable. Za permutaciju σ definiramo vektor $x(\sigma) := (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$, na primjer, za $\sigma = (3, 2, 4, 1)$ imamo vektor $x(\sigma) = (x_3, x_2, x_4, x_1)$. Na sličan način postavimo $y(\sigma) := (y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)})$. Sada uzmimo da nam τ^{-1} označava inverz permutacije τ, to jest, jedinstvenu permutaciju takvu da vrijedi $\tau^{-1}(\tau(i)) = i$ za svaki i. Za $\tau = (2, 3, 4, 1)$ kao gore, imamo da je $\tau^{-1} = (4, 1, 2, 3)$. Pogledajmo sada skalarni produkt

$$x(\sigma)^T y(\tau^{-1}) = x_{\sigma(1)} y_{\tau^{-1}(1)} + \cdots + x_{\sigma(n)} y_{\tau^{-1}(n)}.$$

Uočimo da je to zapravo polinom stupnja 2 u varijablama $x_1, \ldots, x_n, y_1, \ldots, y_n$. Svi nenul koeficijenti ovog polinoma su jedinice. Pritom podrazumijevamo da su koeficijenti polinoma cijeli brojevi. Za naše konkretne σ i τ imamo

$$x(\sigma)^T y(\tau^{-1}) = x_3 y_4 + x_2 y_1 + x_4 y_2 + x_1 y_3.$$

Polinom $x(\sigma)^T y(\tau^{-1})$ kao gore sadrži točno jedan član koji u sebi ima koeficijent y_1, točno jedan koji ima koeficijent y_2, itd. Razlog tome je što je τ^{-1} permutacija. Pogledajmo sada član koji u sebi sadrži koeficijent y_1. Možemo ga zapisati kao $x_{\sigma(k)} y_{\tau^{-1}(k)}$, pri čemu je k indeks sa $\tau^{-1}(k) = 1$, to jest, $k = \tau(1)$. Prema tome, član koji u sebi sadrži koeficijent y_1 je $x_{\sigma(\tau(1))} y_1$, i dalje slično dobijemo član $x_{\sigma(\tau(i))} y_i$ uz y_i. Dakle, ako uzmemo da je $\rho := \sigma \circ \tau$, možemo drukčije zapisati

$$x(\sigma)^T y(\tau^{-1}) = \sum_{i=1}^{n} x_{\rho(i)} y_i.$$

Time smo pokazali da polinom $x(\sigma)^T y(\tau^{-1})$ kodira kompoziciju $\sigma \circ \tau$. Bitno je uočiti sljedeću činjenicu: Ako su $\sigma_1, \sigma_2, \tau_1, \tau_2$ permutacije skupa $\{1, 2, \ldots, n\}$ onda su $x(\sigma_1)^T y({\tau_1}^{-1})$ i $x(\sigma_2)^T y({\tau_2}^{-1})$ jednaki (u smislu polinoma) ako i samo ako $\sigma_1 \circ \tau_1 = \sigma_2 \circ \tau_2$.

Neka je $P = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$ skup permutacija kao u našem početnom problemu. Neka je X $n \times m$ matrica čiji je j-ti stupac vektor $x(\sigma_j)$, $j = 1, 2, \ldots, m$, i neka je Y $n \times m$ matrica koja u j-tom stupcu ima vektor $y({\sigma_j}^{-1})$. Tada umnožak matrica $X^T Y$ ima na mjestu (i, j) polinom $x(\sigma_i)^T y({\sigma_j}^{-1})$. Kada pogledamo gornja razmatranja možemo zaključiti da je kardinalitet skupa $P \circ P$ jednak broju različitih koeficijenata matrice $X^T Y$, pri čemu su ti koeficijenti polinomi stupnja 2 u varijablama $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots y_n$.

Možda nije odmah jasno zašto bi ova neuobičajena formulacija bila algoritamski jednostavnija od računanja $|P \circ P|$. Ma kako bilo, u ovom slučaju od velike pomoći su nam Schwartz - Zippelov teorem, te brzo množenje matrica. Neka je $s := 4m^4$, i neka je $S := \{1, 2, \ldots, s\}$. Naš algoritam za računanje $|P \circ P|$ će raditi na sljedeći način:

1. Izaberemo nasumično cijele brojeve $a_1, a_2, \ldots, a_n$ i $b_1, b_2, \ldots, b_n$. Svaki a_i i svaki b_i su izabrani iz S uniformno i nasumično, te su svi ti odabiri nezavisni.

2. Zadamo matricu A, dobivenu iz X zamjenom cijelih brojeva a_i varijablama x_i, $i = 1, 2, \ldots, n$. Slično, zadamo matricu B koju dobijemo iz Y zamjenom svakog y_i sa b_i, $i = 1, 2, \ldots, n$. Zatim izračunamo produkt: $C := A^T B$.

3. Izračunamo broj različitih koeficijenata matrice C. Taj broj predstavlja nam izlazni rezultat algoritma.

Lema 3.3.3. *Izlazni rezultat prethodnog algoritma nikad nije veći od $|P \circ P|$, a jednak je $|P \circ P|$ sa vjerojatnošću najmanje $\frac{1}{2}$.*

Dokaz. Ako su dva unosa matrice $X^T Y$ jednaki polinomi, onda oni daju jednake unose i u matrici $A^T B$, te na taj način broj različitih koeficijenata matrice $A^T B$ nikad nije veći od $|P \circ P|$. Pretpostavimo sada da su unosi na mjestima (i_1, j_1) i (i_2, j_2) u matrici $X^T Y$ različiti polinomi. Tada je njihova razlika ne-nul polinom p stupnja 2. Schwartz - Zippelov teorem nam kaže da ako varijable u polinomu p supstituiramo nezavisno i nasumično odabranim elementima iz S, dobit ćemo nula sa vjerojatnošću najviše $\frac{2}{|S|} = \frac{1}{2m^4}$. Stoga, svaka dva različita ulaza matrice $X^T Y$ poprimaju jednake vrijednosti u matrici $A^T B$ sa vjerojatnošću najviše $\frac{1}{2m^4}$. Sada imamo da je $X^T Y$ $m \times m$ matrica, i tako zasigurno ne može imati više od m^4 parova različitih ulaza. Vjerojatnost da bilo koji par različitih ulaza matrice $X^T Y$ postane jednak u matrici $A^T B$ nije veća od $\frac{m^4}{2m^4} = \frac{1}{2}$. Dakle, sa vjerojatnošću najmanje $\frac{1}{2}$, broj različitih ulaza u $A^T B$ i u $X^T Y$ su jednaki, te je time teorem dokazan. □

Teorem pokazuje da algoritam radi pravilno sa vjerojatnošću najmanje $\frac{1}{2}$. Ako pokrenemo algoritam k puta i uzmemo najveći od dobivenih odgovora, vjerojatnost da nismo dobili $|P \circ P|$ iznosi najviše 2^{-k}. Zanima nas koliko brzo se algoritam može implementirati.

Radi jednostavnosti, razmotrit ćemo samo slučaj kada je $m = n$, to jest, n permutacija od n brojeva. Prisjetimo se još da se algoritam koji izravno izračunava broj različitih kompozicija izvršava u vremenu reda n^3. U slučajnom algoritmu kojeg smo upravo opisali, korak kojem treba najviše vremena je izračunavanje umnoška matrica $A^T B$. Za $m = n$, A i B su kvadratne matrice čiji članovi su cijeli brojevi ne veći od $s = 4n^4$, te se takve matrice u teoriji mogu izmnožiti unutar vremena $O(n^{2.376})$. To je znatan asimptotski dobitak u odnosu na $O(n^3)$.

Bibliografija

[1] R. A. Demillo i R. J. Lipton, *A Probabilistic Remark on Algebraic Program testing*, Information Processing Letters **7** (1978), br. 4, 193–195.

[2] N. Harvey, *Polynomial Identity Testing*, (2012), `http://www.cs.ubc.ca/~nickhar/W12/Lecture9Notes.pdf`.

[3] R. J. Lipton, *The Curious History of the Schwartz-Zippel Lemma*, (2009), `https://rjlipton.wordpress.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma/`.

[4] J. Matoušek, *Thirty-three Miniatures: Mathematical and Algorithmic Applications of Linear Algebra*, AMS, 2012.

[5] J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, Journal of the ACM **27** (1980), 701–717.

[6] R. E. Zippel, *Probabilistic algorithms for sparse polynomials, Proceedings of EUROSAM 1979*, Springer Lecture Notes in Computer Science **72** (1979), 216–226.

Sažetak

U ovom radu izložen je rezultat poznat pod nazivom Schwartz - Zippelova lema ili Schwartz - Zippelov teorem. Tema rada pripada pretežno algebri, ali ima značajne primjene u drugim matematičkim područjima kao što je na primjer teorija algoritama, te kombinatorika.

Rad se sastoji od tri poglavlja. U uvodu je ukratko opisana tema i cilj rada. Prvo poglavlje sadrži kratku povijest nastanka teorema, različite oblike rezultata pojedinih autora, te kratki opis pojmova korištenih u samom radu. Drugo poglavlje sastoji se od iskaza i dokaza Schwartz - Zippelovog teorema, a u trećem poglavlju izložene su neke primjene tog teorema na probleme koji se mogu svesti na testiranje jednakosti polinoma. Takvi su, primjerice, problem postojanja savršenog sparivanja u grafu i ispitivanje svojstva asocijativnosti u grupoidu. Uz svaku primjenu navedeni su i prikladni primjeri.

Summary

In this diploma thesis we present the result usually called the Schwartz-Zippel lemma or the Schwartz-Zippel theorem. The nature of this theorem is basically algebraic, but it has significant applications in other areas of mathematics, such as the theory of algorithms and combinatorial theory.

The thesis consists of three chapters. The main theme and objective are briefly described in the introduction. The first chapter contains a short history of the theorem's origins, various forms of the main results by different authors and some comments of basic concepts related to this topic. The statement and a proof of the Schwartz-Zippel theorem are given in the second chapter, together with the general outline of its applications. The third and final chapter consists of some applications to problems which can be reduced to polynomial identity testing, including the existence of a perfect matching in a graph and testing of the associativity property in a groupoid.

Životopis

Rođena sam 29. prosinca 1988. godine u Požegi. Nakon završene osnovne škole (O.Š. Dragutina Lermana, Brestovac) upisala sam Opću gimnaziju u Požegi. Maturirala sam 2007. godine s vrlo dobrim uspjehom. Iste godine upisala sam Preddiplomski sveučilišni studij Matematika - smjer nastavnički na Prirodoslovno-matematičkom fakultetu u Zagrebu, koji sam završila 2013. godine. Nakon završenog preddiplomskog studija upisala sam Diplomski sveučilišni studij Matematika - smjer nastavnički.