SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ana Milošević

PRIMJENE VJEROJATNOSNE METODE NA DETERMINISTIČKE IGRE

Diplomski rad

Voditelj rada:
doc. dr. sc. Vjekoslav Kovač

Zagreb, veljača, 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

Vjerojatnosna metoda je nedavno intenzivno razvijena i postala je jedan od najmoćnijih i najraširenijih alata koji se koriste u kombinatorici. Jedan od glavnih razloga za taj brzi razvoj je važna uloga slučajnosti u teorijskom računarstvu, koje je u posljednje vrijeme postalo izvor mnogih zanimljivih kombinatornih problema. Metodu je razvio Paul Erdős sredinom prošlog stoljeća.

Deterministička igra je igra čiji je rezultat potpuno određen zadanim parametrima na početku igre i početnim stanjem igre. U ovisnosti o tim zadanim parametrima i početnom stanju igre, deterministička igra ima samo jedan ishod pa kažemo da je ishod igre unaprijed određen. Prema tome, budući da u deterministčkim igrama nema slučajnosti, iste početne informacije (isti parametri, isto početno stanje) uvijek će dati jednak rezultat na kraju igre ukoliko igrači igraju „optimalno“.

U prvom poglavlju opisujemo osnovni princip vjerojatnosne metode i ilustriramo ju pomoću dva primjera, a zatim objašnjavamo algoritamski aspekt te metode.

Nakon toga, u drugom poglavlju objašnjavamo proces derandomizacije, odnosno proces pretvaranja randomiziranih algoritama u determinističke. Opisujemo dvije metode koje se najviše koriste za derandomizaciju: metodu uvjetnih vjerojatnosti i metodu pesimističnih procjenitelja.

Zatim, u trećem poglavlju prezentiramo ideje randomizacije, derandomizacije i antirandomizacije na primjerima triju determinističkih igara za dva igrača sa savršenom informacijom. Te tri igre su igra sigurnosti, igra uravnoteženih vektora i igra lažova. Najprije pokazujemo da u svakoj od igara postoji savršena pobjednička strategija za jednog od igrača, a zatim i eksplicitno dajemo tu pobjedničku strategiju odnosno efektivnu kontra-strategiju za drugog igrača kada nisu ispunjeni uvjeti potrebni da prvi igrač pobijedi.

U posljednjem poglavlju dajemo još dvije varijante igre sigurnosti i nekoliko konkretnih primjera strategija u igri lažova. Na kraju otkrivamo koji je najmanji broj pitanja potreban kako bi se utvrdio cijeli broj x u igri lažova sa zadanim parametrima $k = 1$ i $n = 10^6$.

Poglavlje 1

Vjerojatnosna metoda

Vjerojatnosna metoda je moćan alat za rješavanje mnogih problema u diskretnoj matematici. Grubo govoreći, metoda radi na sljedeći način: da bismo dokazali da struktura s određenim željenim svojstvima postoji, definiramo prikladni vjerojatnosni prostor za tu strukturu i zatim pokažemo da tražena svojstva vrijede na tom prostoru s pozitivnom vjerojatnosti. Metodu je najbolje ilustrirati pomoću primjera. Prije prvog primjera, definirajmo karakterističnu funkciju skupa koja će nam često biti potrebna.

Definicija 1.0.1. *Funkcija* $\mathbb{1}_A \colon X \to \{0,1\}$*, gdje je* $A \subseteq X$*, definirana formulom*

$$\mathbb{1}_A(x) = \begin{cases} 1\,, & x \in A, \\ 0\,, & x \notin A \end{cases}$$

naziva se ***karakteristična funkcija skupa*** *A.*

Primjer 1.0.2. *Hipergraf je uređeni par* $(V, \mathcal{E})$ *konačnog skupa vrhova* V *i familije* $\mathcal{E}$ *podskupova od* V *koje zovemo bridovi. Ako je* $(V, \mathcal{E})$ *hipergraf u kojem svaki brid ima točno* $n \geq 2$ *vrhova i bridova ima* $|\mathcal{E}| \leq 2^{n-1}$*, dokažite da se tada vrhovi* V *mogu obojiti u dvije boje tako da svaki brid sadrži vrhove obiju boja.*

Dokaz. Nezavisno i slučajno obojimo svaki vrh $v \in V$ ili crvenom ili plavom bojom, s vjerojatnosti $\frac{1}{2}$. Preciznije, to znači da je skup elementarnih događaja $\Omega = \{c, p\}^V$, a vjerojatnosna mjera svakoj njegovoj točki pridružuje broj $2^{-|V|}$. Ako s N označimo broj

jednobojnih bridova nastalih prilikom ovog bojenja, tada za tu slučajnu varijablu imamo

$$\begin{aligned}
\mathbb{E}N &= \sum_{e\in\mathcal{E}} \mathbb{E}\left(\mathbb{1}_{\{e \text{ je jednobojan}\}}\right) \\
&= \sum_{e\in\mathcal{E}} \mathbb{E}\left(\mathbb{1}_{\{e \text{ je cijeli crven ili cijeli plav}\}}\right) \\
&= \sum_{e\in\mathcal{E}} \mathbb{E}\left(\mathbb{1}_{\{e \text{ je cijeli crven}\}} + \mathbb{1}_{\{e \text{ je cijeli plav}\}}\right) \\
&= \sum_{e\in\mathcal{E}} \left(\frac{1}{2^n} + \frac{1}{2^n}\right) \\
&= \frac{|\mathcal{E}|}{2^{n-1}}.
\end{aligned}$$

Tada, ako je $|\mathcal{E}| \leq 2^{n-1}$, imamo da je $\mathbb{E}N \leq 1$, pa postoje dva moguća slučaja:

- $\mathbb{P}(N = 0) = 0$. U ovom slučaju bi bilo

  $$1 \geq \mathbb{E}N \geq \mathbb{P}(N = 1) + 2\mathbb{P}(N \geq 2) = \mathbb{P}(N = 1) + 2(1 - \mathbb{P}(N = 1)) = 2 - \mathbb{P}(N = 1),$$

  tj. $\mathbb{P}(N = 1) \geq 1$ pa bismo imali da je $N = 1$ s vjerojatnosti 1, ali to je očito nemoguće jer svaki graf koji ima više od jednog brida može biti obojen tako da postoji više jednobojnih bridova; naprosto sve vrhove obojimo npr. crvenom bojom. Dakle, ovo se ne može dogoditi, osim u trivijalnom slučaju kada je $|\mathcal{E}| = 1$, a tada tvrdnja očigledno vrijedi.

- $\mathbb{P}(N = 0) > 0$. U ovom slučaju postoji pozitivna vjerojatnost da je $N = 0$ pa možemo jednostavno izabrati neko bojenje koje svjedoči ovom događaju. To nam daje bojenje hipergrafa u dvije boje koje smo nastojali pronaći.

□

Uvedimo sada nekoliko definicija koje će nam biti potrebne za razumijevanje sljedećeg primjera.

Definicija 1.0.3. ***Graf*** *je uređeni par skupova $(V, \mathcal{E})$, gdje je V konačan skup vrhova, a $\mathcal{E}$ skup 2-podskupova od V koje zovemo bridovi.*

Definicija 1.0.4. ***Potpuni graf*** *je graf u kojemu je svaki par vrhova brid. Potpuni graf s n vrhova označavamo s K_n.*

Definicija 1.0.5. ***Podgraf*** *grafa $G = (V, \mathcal{E})$ je graf kojemu su skup vrhova i skup bridova podskupovi od V i $\mathcal{E}$, respektivno. Ukoliko je $G' = (V', \mathcal{E}')$ podgraf od G, tada za svaki brid $e \in \mathcal{E}'$ vrijedi da su oba njegova vrha u V'.*

Definicija 1.0.6. ***Inducirani podgraf*** *grafa G induciran skupom V' je podgraf $G' = (V', \mathcal{E}')$, gdje se $\mathcal{E}'$ sastoji od svih bridova od G čija oba kraja leže u V', dok je V' neki (zadani) podskup od V.*

Primjer 1.0.7. *Ramseyev broj $R(k,l)$ je najmanji prirodni broj n takav da za svako bojenje bridova potpunog grafa K_n s n vrhova u dvije boje, crvenu i plavu, postoji potpun podgraf K_k s k vrhova čiji su svi bridovi obojeni crvenom bojom ili postoji potpun podgraf K_l s l vrhova čiji su svi bridovi obojeni plavom bojom. Ramsey je* 1929. *godine pokazao da je broj $R(k,l)$ konačan za svaka dva prirodna broja k i l. Pronađimo donju ogradu za dijagonalne Ramseyeve brojeve $R(k,k)$, odnosno dokažimo da ako je $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$, onda je $R(k,k) > n$ pa posebno slijedi $R(k,k) > \lfloor 2^{\frac{k}{2}} \rfloor$ za sve $k \geq 3$.*

Dokaz. Promatrajmo slučajno bojenje bridova potpunog grafa K_n u dvije boje, dobivenog nezavisnim bojenjem svakog od bridova ili u crvenu ili u plavu boju, pri čemu je odabir obje boje jednako vjerojatan. Dakle, ovog puta je prostor elementarnih događaja $\Omega = \{c, p\}^{\mathcal{E}(K_n)}$ pa ima $2^{\binom{n}{2}}$ točaka. Za svaki fiksan skup R od k vrhova, neka je A_R događaj da je inducirani podgraf od K_n na skupu R jednobojan (drugim riječima, svi njegovi bridovi su ili crveni ili plavi). Tada je

$$\mathbb{P}(A_R) = 2 \cdot \frac{2^{\binom{n}{2}-\binom{k}{2}}}{2^{\binom{n}{2}}} = 2^{1-\binom{k}{2}}.$$

Budući da postoji $\binom{n}{k}$ mogućih izbora za skup R, vjerojatnost pojavljivanja barem jednog od događaja A_R je ograničena izrazom

$$\mathbb{P}\left(\bigcup_{|R|=k} A_R\right) \leq \sum_{|R|=k} \mathbb{P}(A_R) = \binom{n}{k} \cdot 2^{1-\binom{k}{2}}.$$

Ako pokažemo da je $\binom{n}{k} \cdot 2^{1-\binom{k}{2}}$ manje od 1, onda znamo da s pozitivnom vjerojatnošću postoji neko bojenje grafa u dvije boje u kojem se ne pojavljuje niti jedan događaj A_R. Drugim riječima, postoji dvobojan potpun graf K_n bez jednobojnog potpunog podgrafa K_k, tj. $R(k,k) > n$. Primjetimo da ako je $k \geq 3$ i ako uzmemo $n = \lfloor 2^{\frac{k}{2}} \rfloor$, tada vrijedi

$$\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < \frac{n^k}{k!} \cdot 2^{1+\frac{k}{2}-\frac{k^2}{2}} = \frac{2^{1+\frac{k}{2}}}{k!} \cdot \frac{n^k}{2^{\frac{k^2}{2}}} < 1$$

jer je $3! = 6 > 2^{5/2}$ i

$$k! > 2^{k-1} \geq 2^{1+\frac{k}{2}} \text{za } k \geq 4$$

pa je stoga $R(k,k) > \lfloor 2^{\frac{k}{2}} \rfloor$ za sve $k \geq 3$. □

Ovaj jednostavan primjer demonstrira suštinu vjerojatnosne metode. Da bismo dokazali postojanje „dobrog“ bojenja, ne predstavljamo ga izravno, nego radije na nekonstruktivan način pokažemo da ono postoji. Ovaj primjer se pojavio u radu P. Erdősa iz 1947. godine. Iako je Szele primjenio vjerojatnosnu metodu na drugi kombinatorni problem već 1943. godine, Erdős je svakako bio prvi koji je razumio punu snagu ove metode i godinama ju uspješno primjenjivao na brojnim problemima. Naravno, mogli bismo tvrditi da vjerojatnost nije neophodna u gore danom dokazu. Jednako jednostavan dokaz može biti dan prebrojavanjem, potrebno je samo provjeriti da je ukupan broj bojenja bridova potpunog grafa K_n u dvije boje veći od broja onih bojenja koja sadrže jednobojni potpuni podgraf K_k.

Štoviše, budući da većinu vjerojatnosnih prostora, razmatranih u proučavanju kombinatornih problema, čine konačni prostori, ova napomena vrijedi za većinu primjena vjerojatnosne metode u diskretnoj matematici. Teoretski, to je, uistinu, slučaj. Međutim, u praksi je vjerojatnost neophodna. Bilo bi beznadno zamijeniti primjene mnogih alata vjerojatnosne metode običnim prebrojavanjem, čak i kad su primjenjeni na konačne vjerojatnosne prostore.

Vjerojatnosna metoda ima zanimljiv algoritamski aspekt. Promotrimo dokaz primjera 1.0.7 koji pokazuje da postoji bojenje bridova potpunog grafa K_n u dvije boje bez jednobojnog potpunog podgrafa $K_{\lceil 2\log_2 n\rceil}$. Pitamo se možemo li zapravo pronaći takvo bojenje. Budući da je ukupan broj mogućih bojenja konačan, možemo ih sve isprobati dok ne nađemo traženo bojenje. Međutim, ovaj postupak može zahtijevati $2^{\binom{n}{2}}$ koraka pa je količina vremena potrebna za ovaj postupak eksponencijalna u odnosu na veličinu problema. U većini slučajeva se algoritmi čije je vrijeme izvršavanja veće od polinomijalnog smatraju nepraktičnim. Klasa problema koji mogu biti riješeni u polinomijalnom vremenu je u principu klasa svih rješivih problema. U tom smislu, gore naveden iscrpan pristup pretraživanjem za pronalazak „dobrog“ bojenja potpunog grafa K_n je neprihvatljiv i to je razlog za našu primjedbu da je dokaz primjera 1.0.7 nekonstruktivan, odnosno ne daje konstruktivan, učinkovit i deterministički način bojenja grafa koje ima željena svojstva. Međutim, kad bolje pogledamo dokaz, vidimo da ustvari može biti iskorišten za efektivno dobivanje bojenja koje će vrlo vjerojatno biti „dobro“. Razlog tome je što za velike k i ako je $n = \lfloor 2^{\frac{k}{2}} \rfloor$, onda je

$$\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < \frac{2^{1+\frac{k}{2}}}{k!} \cdot \frac{n^k}{2^{\frac{k^2}{2}}} \leq \frac{2^{1+\frac{k}{2}}}{k!} \ll 1.$$

Stoga, slučajno bojenje potpunog grafa K_n vrlo vjerojatno neće sadržavati jednobojan potpun podgraf $K_{\lceil 2\log_2 n\rceil}$. To znači da ako, na primjer, želimo pronaći bojenje bridova potpunog grafa K_{1024} u dvije boje bez jednobojnog potpunog podgrafa K_{20}, možemo jednostavno stvoriti slučajno bojenje bacanjem simetričnog novčića $\binom{1024}{2}$ puta. Budući da je vjerojatnost da se u tom slučaju ipak pojavi jednobojni potpuni podgraf K_{20} vrlo mala (manja od $\frac{2^{11}}{20!}$ što je približno $8.42 \cdot 10^{-16}$), u nekim slučajevima možemo reći da vjerojatnosna nekonstruktivna metoda daje efektivne vjerojatnosne algoritme. Štoviše, ti algoritmi mogu

ponekad biti pretvoreni u determinističke, o čemu ćemo više govoriti u sljedećem poglavlju.

Vjerojatnosna metoda je moćan alat u Kombinatorici i Teoriji grafova. Također je veoma korisna u Teoriji brojeva i u Kombinatornoj geometriji. U zadnje vrijeme korištena je u razvoju efikasnih algoritamskih tehnika i u proučavanju različitih računskih problema.

Poglavlje 2

Derandomizacija

Kao što je spomenuto u prethodnom poglavlju, vjerojatnosna metoda daje učinkovite randomizirane algoritme za raznovrsne algoritamske probleme. U nekim slučajevima, ti algoritmi mogu biti derandomizirani i pretvoreni u determinističke. U ovom poglavlju objasnit ćemo taj proces derandomizacije na dva primjera.

2.1 Uvodni primjer

Prije nego što počnemo s primjerima spomenimo jednu varijantu formule potpune vjerojatnosti, koju ćemo često koristiti. U bilo kojem vjerojatnosnom prostoru za događaje A, B, C takve da su B i C nezavisni imamo

$$\mathbb{P}(A|B) = \mathbb{P}(C)\mathbb{P}(A|B,C) + \mathbb{P}(C^c)\mathbb{P}(A|B,C^c), \tag{2.1}$$

kad god napisane uvjetne vjerojatnosti postoje, tj. ne dijelimo s nulom u njihovim definicijama. Za dokaz se trebamo prisjetiti kako su definirane uvjetne vjerojatnosti i raspisati formulu (2.1) kao

$$\frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} = \mathbb{P}(C)\frac{\mathbb{P}(A \cap B \cap C)}{\mathbb{P}(B \cap C)} + \mathbb{P}(C^c)\frac{\mathbb{P}(A \cap B \cap C^c)}{\mathbb{P}(B \cap C^c)}.$$

Nadalje, na lijevoj strani možemo iskoristiti aditivnost od $\mathbb{P}$ i transformirati je u

$$\frac{\mathbb{P}(A \cap B \cap C)}{\mathbb{P}(B)} + \frac{\mathbb{P}(A \cap B \cap C^c)}{\mathbb{P}(B)},$$

tj.

$$\frac{\mathbb{P}(B \cap C)}{\mathbb{P}(B)} \cdot \frac{\mathbb{P}(A \cap B \cap C)}{\mathbb{P}(B \cap C)} + \frac{\mathbb{P}(B \cap C^c)}{\mathbb{P}(B)} \cdot \frac{\mathbb{P}(A \cap B \cap C^c)}{\mathbb{P}(B \cap C^c)}.$$

Preostaje još samo dokazati $\frac{\mathbb{P}(B\cap C)}{\mathbb{P}(B)} = \mathbb{P}(C)$ i $\frac{\mathbb{P}(B\cap C^c)}{\mathbb{P}(B)} = \mathbb{P}(C^c)$, ali to su očigledne posljedice nezavisnosti od B i C:

$$\mathbb{P}(B \cap C) = \mathbb{P}(B)\mathbb{P}(C), \quad \mathbb{P}(B \cap C^c) = \mathbb{P}(B) - \mathbb{P}(B \cap C) = \mathbb{P}(B) - \mathbb{P}(B)\mathbb{P}(C) = \mathbb{P}(B)\mathbb{P}(C^c).$$

Time je završen dokaz formule (2.1). U slučaju $B = \emptyset$ formulu (2.1) možemo interpretirati kao

$$\mathbb{P}(A) = \mathbb{P}(C)\mathbb{P}(A|C) + \mathbb{P}(C^c)\mathbb{P}(A|C^c),$$

što je upravo formula potpune vjerojatnosti.

Osim toga, (2.1) se direktno proširuje i na uvjetno matematičko očekivanje, tj. za bilo koju slučajnu varijablu X vrijedi

$$\mathbb{E}(X|B) = \mathbb{P}(C)\mathbb{E}(X|B, C) + \mathbb{P}(C^c)\mathbb{E}(X|B, C^c), \tag{2.2}$$

Naime, prisjetimo se da je uvjetno očekivanje $\mathbb{E}(X|B)$ definirano kao očekivanje od X obzirom na vjerojatnosnu mjeru $A \mapsto \mathbb{P}(A|B)$. Ako je prostor elementarnih događaja konačan pa X poprima samo konačno mnogo vrijednosti $x_1, \ldots, x_n$, što je kod nas uvijek slučaj, tada je

$$\mathbb{E}(X|B) = \sum_{k=1}^{n} x_k \mathbb{P}(\{X = x_k\}|B).$$

Prema tome, formula (2.2) slijedi primjenom formule (2.1) na događaje $A = \{X = x_k\}$, i to množenjem s x_k i sumiranjem dobivenog.

Jednostavna primjena osnovne vjerojatnosne metode daje sljedeću tvrdnju:

Teorem 2.1.1. *Za svaki prirodan broj n postoji bojenje bridova potpunog grafa K_n u dvije boje takvo da je ukupan broj jednobojnih kopija grafa K_4 najviše $\binom{n}{4} \cdot 2^{-5}$.*

Dokaz. Promatrajmo slučajno bojenje bridova potpunog grafa K_n u dvije boje (crvenu i plavu) pri čemu je odabir obje boje jednako vjerojatan. Prostor elementarnih događaja je $\Omega = \{c, p\}^{\mathcal{E}(K_n)}$ pa ima $2^{\binom{n}{2}}$ točaka. Za svaki fiksan skup R od 4 vrha, neka je A_R događaj da je inducirani podgraf K_4 od K_n na skupu R jednobojan (drugim riječima, svi njegovi bridovi su ili crveni ili plavi). Tada je

$$\mathbb{P}(A_R) = 2 \cdot \frac{2^{\binom{n}{2}-\binom{4}{2}}}{2^{\binom{n}{2}}} = 2^{-5}.$$

Budući da postoji $\binom{n}{4}$ mogućih izbora za skup R, očekivani broj jednobojnih kopija grafa K_4 u bojenju potpunog grafa K_n je $\binom{n}{4} \cdot 2^{-5}$. Prema tome, postoji neko bojenje takvo da je ukupan broj jednobojnih kopija grafa K_4 najviše $\binom{n}{4} \cdot 2^{-5}$. □

Možemo li zapravo deterministički pronaći takvo bojenje u vremenu koje je polinomijalno u odnosu na n? Opisat ćemo postupak koji to čini i koji je specijalan slučaj općenite tehnike zvane *metoda uvjetnih vjerojatnosti*.

Najprije moramo definirati težinsku funkciju za svaki djelomično obojen potpun graf K_n. Za dano bojenje nekih bridova od K_n u crvenu i plavu boju, za svaku kopiju K od K_4 u K_n definiramo težinu $w(K)$ na sljedeći način:

- ako je najmanje jedan brid od K obojen crveno i najmanje jedan brid od K obojen plavo, onda je $w(K) = 0$;
- ako niti jedan brid od K nije obojen, onda je $w(K) = 2^{-5}$;
- ako je $r \geq 1$ bridova od K obojeno, i to u istu boju, onda je $w(K) = 2^{r-6}$.

Također, definiramo totalnu težinu W djelomično obojenog potpunog grafa K_n kao zbroj $\sum w(K)$, pri čemu K prolazi svim kopijama od K_4 u K_n. Ako će svi trenutno neobojeni bridovi od K_n biti nezavisno i slučajno obojeni u jednu od dvije boje, crvenu ili plavu, primjetimo da će tada težina svake kopije K od K_4 biti točno vjerojatnost da će ta kopija biti jednobojna. Stoga, zbog linearnosti očekivanja, ukupna težina W je jednostavno očekivani broj jednobojnih kopija od K_4 u takvom slučajnom proširenju djelomičnog bojenja od K_n do potpunog bojenja.

Sada možemo opisati postupak za pronalazak bojenja iz teorema 2.1.1 . Poredajmo $\binom{n}{2}$ bridova od K_n proizvoljno i konstruirajmo željeno bojenje u dvije boje bojenjem svakog brida redom ili u crveno ili u plavo. Pretpostavimo da su bridovi $e_1, \ldots, e_{i-1}$ već obojeni i da sada moramo obojiti brid e_i. Neka je W težina od K_n s obzirom na dano djelomično bojenje b bridova $e_1, \ldots, e_{i-1}$. Slično, neka je W_c težina od K_n s obzirom na djelomično bojenje dobiveno iz b bojenjem brida e_i u crvenu boju, i neka je W_p težina od K_n s obzirom na djelomično bojenje dobiveno iz b bojenjem brida e_i u plavu boju. Po definiciji od W i zahvaljujući formuli (2.2) (zbog interpretacije totalne težine kao očekivane vrijednosti) imamo

$$\begin{aligned}
&\mathbb{E}(\text{broj kopija od } K_4 | e_1, \ldots, e_{i-1} \text{ obojeni prema } b) = \\
&\mathbb{P}(e_i \text{ obojen crveno}) \cdot \mathbb{E}(\text{broj kopija od } K_4 | e_1, \ldots, e_{i-1} \text{ obojeni prema } b, e_i \text{ obojen crveno}) \\
&+ \mathbb{P}(e_i \text{ obojen plavo}) \cdot \mathbb{E}(\text{broj kopija od } K_4 | e_1, \ldots, e_{i-1} \text{ obojeni prema } b, e_i \text{ obojen plavo})
\end{aligned}$$

tj. jednostavno

$$W = \frac{W_c + W_p}{2}.$$

Boja od e_i će biti odabrana tako da minimizira ukupnu težinu. Drugim riječima, ako je $W_c \leq W_p$, obojimo brid e_i u crvenu boju, a ako je $W_p \leq W_c$, obojimo brid e_i u plavu boju. Zbog gornje nejednakosti težinska funkcija se nikad ne povećava tijekom provođenja

algoritma. Budući da je na početku njezina vrijednost točno $\binom{n}{4} \cdot 2^{-5}$, na kraju njezina vrijednost može biti najviše jednaka tom izrazu. Međutim, na kraju su svi bridovi obojeni i težina je točno jednaka broju jednobojnih kopija od K_4. Prema tome, gornji postupak, koji je deterministički i izvršava se u polinomijalnom vremenu, daje bojenje bridova potpunog grafa K_n u dvije boje, zadovoljavajući uz to zaključak teorema 2.1.1 . Pokažimo još da se postupak zaista izvršava u polinomijalnom vremenu. Bojimo $\binom{n}{2}$ bridova grafa K_n za što nam je potrebno $\binom{n}{2}$ koraka. U svakom koraku računamo težine za što je potrebno proći kroz sve kopije K od K_4, kojih ima $\binom{n}{4}$. Prema tome složenost je najviše reda veličine n^6, tj. $O(n^6)$. To je polinomijalno vrijeme i puno je bolje nego prolaziti kroz sva bojenja, kojih ima $2^{\binom{n}{2}}$.

2.2 Metoda uvjetnih vjerojatnosti

Opišimo sada metodu uvjetnih vjerojatnosti s općenitijim pretpostavkama. Pretpostavimo da imamo vjerojatnosni prostor i pretpostavimo zbog jednostavnosti da je pripadni skup elementarnih događaja $\Omega = \{-1, 1\}^l$, što posebno znači da ima 2^l točaka. Dakle, njegovi elementi su binarni vektori duljine l. Pretpostavljamo da je na Ω dana vjerojatnosna mjera $\mathbb{P}$ koja je jednaka l-toj potenciji neke vjerojatnosne mjere $\mathbb{P}_1$ na $\{-1, 1\}$, tj. eksplicitno

$$\mathbb{P}(\{(\epsilon_1, \ldots, \epsilon_l)\}) = \mathbb{P}_1(\{\epsilon_1\}) \cdots \mathbb{P}_1(\{\epsilon_l\}),$$

pri čemu je $\mathbb{P}_1(\{1\}) = p$ i $\mathbb{P}_1(\{-1\}) = 1 - p$ za neki $p \in [0, 1]$. Neka je $A_1, \ldots, A_s$ kolekcija događaja i pretpostavimo da je $\sum_{i=1}^{s} \mathbb{P}(A_i) = k$. Prema tome,

$$\mathbb{E} \sum_{i=1}^{s} \mathbb{1}_{A_i} = k,$$

odakle vidimo da je k očekivani broj događaja A_i koji su ispunjeni, pa stoga postoji točka $(\epsilon_1, \ldots, \epsilon_l)$ u tom prostoru u kojoj je ispunjeno najviše k događaja. Naš cilj je pronaći takvu točku deterministički.

Neka su X_j, $j = 1, \ldots, l$ koordinatne slučajne varijable, tj. $X_j \colon \Omega \to \{-1, 1\}$ je definirana sa

$$X_j(\epsilon_1, \ldots, \epsilon_l) := \epsilon_j.$$

Iz naše pretpostavke o vjerojatnosnoj mjeri $\mathbb{P}$ direktno slijedi da su slučajne varijable $X_1, \ldots, X_l$ nezavisne i jednako distribuirane, tj. preciznije

$$\mathbb{P}(X_j = 1) = p, \quad \mathbb{P}(X_j = -1) = 1 - p, \quad j = 1, \ldots, l.$$

za neki $p \in [0, 1]$. Za indekse $1 \leq i \leq s$, $1 \leq j \leq l$ i bilo koji izbor od $\epsilon_1, \ldots, \epsilon_j \in \{-1, 1\}$ kratko ćemo pisati

$$\mathbb{P}(A_i | \epsilon_1, \ldots, \epsilon_j)$$

umjesto

$$\mathbb{P}(A_i|X_1 = \epsilon_1, \ldots, X_j = \epsilon_j).$$

U slučaju $j = 0$ taj izraz interpetiramo naprosto kao $\mathbb{P}(A_i)$.

Za svaki izbor točke $\left(\epsilon_1, \ldots, \epsilon_{j-1}\right)$ i za svaki događaj A_i, uvjetna vjerojatnost događaja A_i uz dane vrijednosti $\epsilon_1, \ldots, \epsilon_{j-1}$

$$\mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}\right)$$

je jednostavno „težinski"prosjek (s težinama p i $1 - p$) dviju uvjetnih vjerojatnosti koje odgovaraju dvama mogućim izborima za ϵ_j. Drugim riječima, po formuli (2.1) imamo

$$\mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}\right) = \mathbb{P}\left(X_j = -1\right) \cdot \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}, -1\right) + \mathbb{P}\left(X_j = 1\right) \cdot \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}, 1\right).$$

Stoga,

$$\begin{aligned}\sum_{i=1}^{s} \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}\right) &= (1-p) \cdot \sum_{i=1}^{s} \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}, -1\right) + p \cdot \sum_{i=1}^{s} \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}, 1\right) \\ &\geq \min\left\{\sum_{i=1}^{s} \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}, -1\right), \sum_{i=1}^{s} \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_{j-1}, 1\right)\right\}.\end{aligned}$$

Dakle, ako su vrijednosti od ϵ_j redom izabrane tako da minimiziraju vrijednost sume $\sum_{i=1}^{s} \mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_j\right)$, onda se vrijednost ove sume ne može povećati. Kako je ta suma jednaka k na početku, slijedi da je na kraju najviše k. Ali na kraju je svaki ϵ_j fiksiran pa je stoga vrijednost ove sume točno broj događaja A_i koji su ispunjeni u točki $(\epsilon_1, \ldots, \epsilon_l)$, što pokazuje da naš postupak radi.

Gornji postupak je učinkovit pod pretpostavkom da l nije prevelik (što je obično slučaj u kombinatornim primjerima), i još važnije, pod pretpostavkom da uvjetne vjerojatnosti $\mathbb{P}\left(A_i|\epsilon_1, \ldots, \epsilon_j\right)$ mogu biti efikasno izračunate za svaki događaj A_i i za svaku moguću vrijednost $\epsilon_1, \ldots, \epsilon_j$. To je doista slučaj u primjeru razmatranom u teoremu 2.1.1 . Međutim, postoji mnogo zanimljivih primjera gdje nije tako. Trik koji može biti koristan u takvim situacijama je uvođenje *pesimističnih procjenitelja*.

2.3 Metoda pesimističnih procjenitelja

Pesimistične procjenitelje je 1988. godine predstavio Raghavan. Ponovno razmotrimo ranije opisani vjerojatnosni prostor i događaje $A_1, \ldots, A_s$ u njemu. Pretpostavimo da za svaki događaj A_i i za svaki $0 \leq j \leq l$ imamo funkciju $f_j^i \colon \{-1, 1\}^j \to \mathbb{R}$ koja može biti efikasno

izračunata. U slučaju $j = 0$ pak f_0^i intepretiramo naprosto kao realni broj. Također pretpostavimo da za svaki $1 \leq j \leq l$ i za svaki izbor $\epsilon_1, \ldots, \epsilon_{j-1} \in \{-1, 1\}$ postoji broj $q \in [0, 1]$ (koji smije ovisiti o njima) takav da za svaki $1 \leq i \leq s$ vrijedi

$$f_{j-1}^i(\epsilon_1, \ldots, \epsilon_{j-1}) \geq (1-q) f_j^i(\epsilon_1, \ldots, \epsilon_{j-1}, -1) + q f_j^i(\epsilon_1, \ldots, \epsilon_{j-1}, 1) \tag{2.3}$$

i da je f_j^i gornja granica za uvjetne vjerojatnosti događaja A_i, odnosno da je za $1 \leq i \leq s$ i za sve $\epsilon_1, \ldots, \epsilon_j \in \{-1, 1\}$

$$f_j^i\left(\epsilon_1, \ldots, \epsilon_j\right) \geq \mathbb{P}\left(A_i | \epsilon_1, \ldots, \epsilon_j\right). \tag{2.4}$$

Kao posljedicu od (2.3) očigledno imamo

$$\sum_{i=1}^{s} f_{j-1}^i(\epsilon_1, \ldots, \epsilon_{j-1}) \geq \min\Big\{ \sum_{i=1}^{s} f_j^i(\epsilon_1, \ldots, \epsilon_{j-1}, -1), \sum_{i=1}^{s} f_j^i(\epsilon_1, \ldots, \epsilon_{j-1}, 1)\Big\}.$$

U ovom slučaju, ako je na početku $\sum_{i=1}^{s} f_0^i \leq t$ i izaberemo vrijednosti od ϵ_j tako da u svakom koraku minimiziramo sumu $\sum_{i=1}^{s} f_j^i\left(\epsilon_1, \ldots, \epsilon_j\right)$, na kraju dobijemo točku $(\epsilon_1, \ldots, \epsilon_l)$ za koju je $\sum_{i=1}^{s} f_l^i(\epsilon_1, \ldots, \epsilon_l) \leq t$. Broj događaja A_i koji su ispunjeni u ovoj točki je najviše t. Funkcije f_j^i u gornjem izrazu zovemo pesimistični procjenitelji.

To nam omogućava da dobijemo učinkovite algoritme u nekim slučajevima u kojima ne postoji poznati učinkoviti način računanja traženih uvjetnih vjerojatnosti. Takav primjer nam daje sljedeći teorem, a dokaz tog teorema je varijanta dokaza iz [1].

Teorem 2.3.1. *Neka je $(a_{ij})_{i,j=1}^n$ $n \times n$ matrica realnih brojeva, gdje je $-1 \leq a_{ij} \leq 1$ za sve i, j. Tada u polinomijalnom vremenu možemo pronaći $\epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}$ takve da je za svako i, $1 \leq i \leq n$, ispunjena nejednakost $|\sum_{j=1}^n \epsilon_j a_{ij}| \leq \sqrt{2n \ln(2n)}$.*

Dokaz. Razmotrimo simetričan vjerojatnosni prostor na 2^n točaka koji je određen s 2^n mogućih vektora $(\epsilon_1, \ldots, \epsilon_n) \in \{-1, 1\}^n$. To znači da se svaki od tih vektora odabire s vjerojatnošću 2^{-n}. Definirajmo $\beta = \sqrt{2n \ln(2n)}$ i neka je A_i događaj

$$A_i = \left\{ \left| \sum_{j=1}^{n} X_j a_{ij} \right| > \beta \right\} = \left\{ (\epsilon_1, \ldots, \epsilon_n) : \left| \sum_{j=1}^{n} \epsilon_j a_{ij} \right| > \beta \right\}.$$

Pokazat ćemo da nam metoda uvjetnih vjerojatnosti s prikladnim pesimističnim procjeniteljima omogućava da efikasno pronađemo točku u prostoru u kojoj nije ispunjen niti jedan događaj A_i.

Definirajmo $\alpha = \frac{\beta}{n}$ i neka je $G(x)$ funkcija

$$G(x) = \operatorname{ch}(\alpha x) = \frac{e^{\alpha x} + e^{-\alpha x}}{2}.$$

Lema 2.3.2. *Za svaki realni broj x vrijedi*

$$G(x) \leq e^{\frac{\alpha^2 x^2}{2}},$$

sa strogom nejednakosti ako su i x i α različiti od 0*.*

Dokaz. Doista, budući da za sve realne brojeve x vrijedi

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots,$$

iz navedenog i definicije od $G(x)$ slijedi:

$$\begin{aligned} G(x) &= \frac{e^{\alpha x} + e^{-\alpha x}}{2} \\ &= \frac{1}{2}\left[\left(1 + \alpha x + \frac{\alpha^2 x^2}{2!} + \frac{\alpha^3 x^3}{3!} + \cdots\right) + \left(1 - \alpha x + \frac{\alpha^2 x^2}{2!} - \frac{\alpha^3 x^3}{3!} + \cdots\right)\right] \\ &= 1 + \frac{\alpha^2 x^2}{2!} + \frac{\alpha^4 x^4}{4!} + \cdots \\ &= \sum_{k=0}^{\infty} \frac{\alpha^{2k} x^{2k}}{(2k)!}. \end{aligned}$$

S druge strane,

$$\begin{aligned} e^{\frac{\alpha^2 x^2}{2}} &= 1 + \frac{\alpha^2 x^2}{2} + \frac{\alpha^4 x^4}{2^2 \cdot 2!} + \frac{\alpha^6 x^6}{2^3 \cdot 3!} + \cdots \\ &= \sum_{k=0}^{\infty} \frac{\alpha^{2k} x^{2k}}{2^k \cdot k!}. \end{aligned}$$

Trebamo dokazati da je

$$\frac{\alpha^{2k} x^{2k}}{(2k)!} \leq \frac{\alpha^{2k} x^{2k}}{2^k k!},$$

tj.

$$\frac{(2k)!}{k!} \geq 2^k.$$

Zapišimo prethodni izraz kao

$$(k+1)(k+2)\ldots(2k) \geq 2^k$$

pa nejednakost očigledno vrijedi za $k \geq 1$. Prema tome, dobivamo

$$G(x) \leq e^{\frac{\alpha^2 x^2}{2}},$$

što smo i trebali pokazati. Očito je da jednakost vrijedi jedino ako je barem jedan od argumenata x i α jednak nuli jer inače već u $\frac{\alpha^4 x^4}{24} \leq \frac{\alpha^4 x^4}{8}$ imamo strogu nejednakost. □

Lema 2.3.3. *Za sve realne brojeve x i y vrijedi sljedeća jednakost*

$$G(x)\,G(y) = \frac{G(x+y) + G(x-y)}{2}.$$

Dokaz. Tvrdnja slijedi direktno iz definicije funkcije G. S lijeve strane imamo

$$\begin{aligned} G(x)\,G(y) &= \frac{e^{\alpha x} + e^{-\alpha x}}{2} \cdot \frac{e^{\alpha y} + e^{-\alpha y}}{2} \\ &= \frac{e^{\alpha x}e^{\alpha y} + e^{\alpha x}e^{-\alpha y} + e^{-\alpha x}e^{\alpha y} + e^{-\alpha x}e^{-\alpha y}}{4} \\ &= \frac{e^{\alpha(x+y)} + e^{\alpha(x-y)} + e^{-\alpha(x-y)} + e^{-\alpha(x+y)}}{4}, \end{aligned}$$

a s desne strane

$$\begin{aligned} \frac{G(x+y) + G(x-y)}{2} &= \frac{1}{2}\left(\frac{e^{\alpha(x+y)} + e^{-\alpha(x+y)}}{2} + \frac{e^{\alpha(x-y)} + e^{-\alpha(x-y)}}{2}\right) \\ &= \frac{e^{\alpha(x+y)} + e^{\alpha(x-y)} + e^{-\alpha(x-y)} + e^{-\alpha(x+y)}}{4}. \end{aligned}$$

Dakle, tvrdnja vrijedi. □

Sada možemo definirati funkcije f_p^i koje će formirati naše pesimistične procjenitelje. Za svako $1 \le i \le n$ i za svako $\epsilon_1, \ldots, \epsilon_p \in \{-1, 1\}$ definiramo

$$f_p^i\left(\epsilon_1, \ldots, \epsilon_p\right) = 2e^{-\alpha\beta} G\left(\sum_{j=1}^{p} \epsilon_j a_{ij}\right) \prod_{j=p+1}^{n} G\left(a_{ij}\right).$$

Očito ove funkcije mogu biti efikasno izračunate. Ostaje provjeriti da one zadovoljavaju uvjete opisane jednadžbama (2.3) i (2.4) uz $q = \frac{1}{2}$ i da je suma $\sum_{i=1}^{n} f_0^i$ manja od 1. To je dokazano sljedećim tvrdnjama.

Lema 2.3.4. *Za svako* $1 \le i \le n$ *i za sve* $\epsilon_1, \ldots, \epsilon_{p-1} \in \{-1, 1\}$ *vrijedi*

$$f_{p-1}^i\left(\epsilon_1, \ldots, \epsilon_{p-1}\right) = \frac{f_p^i\left(\epsilon_1, \ldots, \epsilon_{p-1}, -1\right) + f_p^i\left(\epsilon_1, \ldots, \epsilon_{p-1}, 1\right)}{2}.$$

Dokaz. Stavimo $v = \sum_{j=1}^{p-1} \epsilon_j a_{ij}$. Prema definiciji od f_p^i i prema svojstvima od G vrijedi:

$$\begin{aligned} f_{p-1}^i\left(\epsilon_1, \ldots, \epsilon_{p-1}\right) &= 2e^{-\alpha\beta} G\left(\sum_{j=1}^{p-1} \epsilon_j a_{ij}\right) \prod_{j=p}^{n} G\left(a_{ij}\right) \\ &= 2e^{-\alpha\beta} G\left(v\right) G\left(a_{ip}\right) \prod_{j=p+1}^{n} G\left(a_{ij}\right) \\ &= 2e^{-\alpha\beta} \frac{G\left(v - a_{ip}\right) + G\left(v + a_{ip}\right)}{2} \prod_{j=p+1}^{n} G\left(a_{ij}\right) \\ &= \frac{2e^{-\alpha\beta} G\left(v - a_{ip}\right) \prod_{j=p+1}^{n} G\left(a_{ij}\right) + 2e^{-\alpha\beta} G\left(v + a_{ip}\right) \prod_{j=p+1}^{n} G\left(a_{ij}\right)}{2} \\ &= \frac{f_p^i\left(\epsilon_1, \ldots, \epsilon_{p-1}, -1\right) + f_p^i\left(\epsilon_1, \ldots, \epsilon_{p-1}, 1\right)}{2}, \end{aligned}$$

čime je dokazana tvrdnja. □

Lema 2.3.5. *(Markovljeva nejednakost) Neka je X neka nenegativna integrabilna slučajna varijabla i neka je $a > 0$ proizvoljan. Tada je*

$$P\left(X \geq a\right) \leq \frac{\mathbb{E}X}{a}.$$

Dokaz. Za proizvoljan događaj E, neka je $\mathbb{1}_E$ indikatorska slučajna varijabla tog događaja, tj.

$$\mathbb{1}_E = \begin{cases} 1\,, & \text{ako se dogodio događaj } E, \\ 0\,, & \text{inače .} \end{cases}$$

Analogno, koristeći ovu notaciju, imamo

$$\mathbb{1}_{\{X \geq a\}} = \begin{cases} 1\,, & \text{ako se dogodio događaj } \{X \geq a\}, \\ 0\,, & \text{ako se dogodio događaj } \{X < a\}. \end{cases}$$

Tada, za dano $a > 0$, vrijedi sljedeće:

- Ako je $X < a$, onda je $\mathbb{1}_{\{X \geq a\}} = 0$ pa vrijedi $a \cdot \mathbb{1}_{\{X \geq a\}} = 0 \leq X$.
- Obratno, ako je $X \geq a$, onda je $\mathbb{1}_{\{X \geq a\}} = 1$ pa vrijedi $a \cdot \mathbb{1}_{\{X \geq a\}} = a \leq X$.

Prema tome, za dano $a > 0$, vrijedi

$$a \cdot \mathbb{1}_{\{X \geq a\}} \leq X.$$

Budući da je očekivanje monotono rastuća funkcija iz prethodne nejednakosti slijedi

$$\mathbb{E}\left[a \cdot \mathbb{1}_{\{X \geq a\}}\right] \leq \mathbb{E}X.$$

Koristeći linearnost matematičkog očekivanja dobivamo

$$\begin{aligned}\mathbb{E}\left[a \cdot \mathbb{1}_{\{X \geq a\}}\right] &= a \cdot \mathbb{E}\left[\mathbb{1}_{\{X \geq a\}}\right] \\ &= a \cdot (1 \cdot \mathbb{P}(X \geq a) + 0 \cdot \mathbb{P}(X < a)) \\ &= a \cdot \mathbb{P}(X \geq a).\end{aligned}$$

Odavde slijedi da je

$$a \cdot \mathbb{P}(X \geq a) \leq \mathbb{E}X,$$

a budući da je $a > 0$ obje strane nejednakosti možemo podijeliti s a pa dobivamo

$$\mathbb{P}(X \geq a) \leq \frac{\mathbb{E}X}{a}$$

i time je tvrdnja leme dokazana. □

Dokaz prethodne leme preuzet je iz [6].

Lema 2.3.6. *Za svako* $1 \leq i \leq n$ *i za sve* $\epsilon_1, \ldots, \epsilon_p \in \{-1, 1\}$ *vrijedi*

$$f_p^i\left(\epsilon_1, \ldots, \epsilon_p\right) \geq \mathbb{P}\left(A_i | \epsilon_1, \ldots, \epsilon_p\right).$$

Prije nego što dokažemo ovu lemu, iskažimo još dvije pomoćne tvrdnje koje su nam potrebne za dokaz leme. Dokazi tih dviju tvrdnji mogu se pronaći u opsežnoj monografiji [3].

Tvrdnja 2.3.7. *Neka je* $\{X_i, i \in I\}$ *familija nezavisnih slučajnih varijabli i neka su* $g_i : \mathbb{R} \to \mathbb{R}$ $(i \in I)$ *Borelove funkcije. Tada je* $\{g_i(X_i), i \in I\}$ *familija nezavisnih slučajnih varijabli.*

Tvrdnja 2.3.8. *Neka su* $X_1, \ldots, X_n$ *nezavisne slučajne varijable. Ako su sve* X_i *nenegativne ili ako je* $\mathbb{E}X_i$ *konačno za sve i, tada postoji* $\mathbb{E}\left(\prod_{i=1}^n X_i\right)$ *i vrijedi*

$$\mathbb{E}\left(\prod_{i=1}^{n} X_i\right) = \prod_{i=1}^{n} \mathbb{E}X_i.$$

Dokaz (Lema 2.3.6). Neka je $v = \sum_{j=1}^{p} \epsilon_j a_{ij}$. Tada je zbog leme 2.3.5 i tvrdnji 2.3.7 i 2.3.8

$$\begin{aligned}
\mathbb{P}\left(A_i|\epsilon_1,\ldots,\epsilon_p\right) &\leq \mathbb{P}\left(v + \sum_{j>p} X_j a_{ij} > \beta\right) + \mathbb{P}\left(-v - \sum_{j>p} X_j a_{ij} > \beta\right) \\
&= \mathbb{P}\left(e^{\alpha(v+\sum_{j>p} X_j a_{ij})} > e^{\alpha\beta}\right) + \mathbb{P}\left(e^{-\alpha(v+\sum_{j>p} X_j a_{ij})} > e^{\alpha\beta}\right) \\
&\leq e^{\alpha v}e^{-\alpha\beta}\mathbb{E}\left(e^{\alpha(\sum_{j>p} X_j a_{ij})}\right) + e^{-\alpha v}e^{-\alpha\beta}\mathbb{E}\left(e^{-\alpha(\sum_{j>p} X_j a_{ij})}\right) \\
&= e^{\alpha v}e^{-\alpha\beta}\mathbb{E}\left(\prod_{j>p} e^{\alpha X_j a_{ij}}\right) + e^{-\alpha v}e^{-\alpha\beta}\mathbb{E}\left(\prod_{j>p} e^{-\alpha X_j a_{ij}}\right) \\
&= e^{-\alpha\beta}\left(e^{\alpha v}\prod_{j>p}\mathbb{E}\left(e^{\alpha X_j a_{ij}}\right) + e^{-\alpha v}\prod_{j>p}\mathbb{E}\left(e^{-\alpha X_j a_{ij}}\right)\right) \\
&= \left\{\begin{array}{l}\mathbb{E}\left(e^{\alpha X_j a_{ij}}\right) = \mathbb{P}(X_j = 1)\cdot e^{\alpha a_{ij}} + \mathbb{P}(X_j = -1)\cdot e^{-\alpha a_{ij}} \\ \qquad\qquad = \dfrac{e^{\alpha a_{ij}} + e^{-\alpha a_{ij}}}{2} = G(a_{ij}) = \cdots = \mathbb{E}\left(e^{-\alpha X_j a_{ij}}\right)\end{array}\right\} \\
&= e^{-\alpha\beta}\left(e^{\alpha v}\prod_{j>p} G(a_{ij}) + e^{-\alpha v}\prod_{j>p} G(a_{ij})\right) \\
&= 2e^{-\alpha\beta}G\left(v\right)\prod_{j>p} G\left(a_{ij}\right) \\
&= f_p^i\left(\epsilon_1,\ldots,\epsilon_p\right).
\end{aligned}$$

Time je dokazana tvrdnja 2.3.6 . □

Da bismo dokazali teorem još preostaje pokazati da vrijedi $\sum_{i=1}^{n} f_0^i < 1$. Zaista, prema svojstvima od G i zbog izbora α i β vrijedi:

$$\begin{aligned}
\sum_{i=1}^{n} f_0^i &= \sum_{i=1}^{n} 2e^{-\alpha\beta}\prod_{j=1}^{n} G\left(a_{ij}\right) \\
&\leq \sum_{i=1}^{n} 2e^{-\alpha\beta}\prod_{j=1}^{n} e^{\frac{\alpha^2 a_{ij}^2}{2}} \leq \sum_{i=1}^{n} 2e^{-\alpha\beta}e^{\frac{\alpha^2 n}{2}} \\
&= 2ne^{\frac{\alpha^2 n}{2}-\alpha\beta} = 2ne^{\frac{\alpha^2 n}{2}-\alpha^2 n} = 2ne^{\frac{-\alpha^2 n}{2}} \\
&= 2ne^{\frac{-\beta^2}{2n}} = 2ne^{\frac{-2n\ln(2n)}{2n}} = 2ne^{\ln\left(\frac{1}{2n}\right)} \\
&= 1.
\end{aligned}$$

Štoviše, prva nejednakost je stroga nejednakost osim ako je $a_{ij} = 0$ za sve i,j, a druga nejednakost je stroga osim ako je $a_{ij}^2 = 1$ za sve i,j. Time je dokazan teorem 2.3.1 . □

Poglavlje 3

Analiza triju igara

U ovom poglavlju analizirat ćemo tri primjera deterministčkih igara: igru sigurnosti, igru uravnoteženih vektora i igru lažova. To su igre za dva igrača (nazovimo ih Paul i Carole) s nesimetričnim pravilima, kod kojih se vjerojatnosnom metodom može dokazati postojanje pobjedničke strategije za jednog od igrača, uz odgovorajuće vrijednosti danih parametara. Zatim ćemo na primjerima gore spomenutih igara pronaći eksplicitne strategije, tj. provest ćemo postupak derandomizacije i antirandomizacije.

Sve tri igre imaju slična pravila. Paul u svakom krugu napravi potez, a zatim Carole bira između dvije opcije. Za svaku od igara provest ćemo sljedeća tri koraka:

- *Randomizacija:* Najprije analiziramo slučajnu strategiju za Carole. Budući da igre ne mogu završiti neriješenim rezultatom, ako možemo pokazati da njezina strategija pobjeđuje s pozitivnom vjerojatnosti, odmah slijedi da Carole uvijek može pobijediti.

- *Derandomizacija:* Definiramo težinsku funkciju poteza kao očekivani broj loših ishoda koji će se dogoditi ako će Carole igrati slučajno (i zbog kojih će izgubiti). Zatim kreiramo deterministčku strategiju koju Carole mora uvijek igrati kako bi minimizirala tu težinsku funkciju.

- *Antirandomizacija:* Paul koristi tu težinsku funkciju za efektivnu kontra-strategiju. Za svaki Paulov potez prosječna težina mogućih sljedećih poteza jednaka je težini prethodnog poteza. Paul igra tako da su težine ta dva nova moguća poteza što je moguće bliže jedna drugoj. Tada Carole ne može mnogo smanjiti težinu pa ako je početna težina dovoljno velika, ona mora biti takva i na kraju igre i time je Carole izgubila.

U ovim igrama specifična imena Paul i Carole nisu slučajno odabrana. Inicijali P i C se odnose na „Pusher-Chooser“ igre. Također Paulom možemo smatrati velikog matematičara Paula Erdősa, a ime Carole je smišljeno zbog njegovog akronima - Oracle (eng. prorok).

Budući da igre koje ćemo analizirati pripadaju klasi igara sa savršenom informacijom, objasnimo još što su igre sa savršenom informacijom i zašto u tim igrama mora postojati pobjednik. Kao što smo rekli, radi se o igrama za dva igrača pri čemu je cilj svakog igrača pobijediti u igri. Pretpostavljamo da igrači imaju konačan broj poteza i da oba igrača prije svakog poteza imaju informacije o svim prethodnim potezima u igri. Takve igre zovemo *igre sa savršenom informacijom i sumom nula* i one su strogo određene, odnosno uvijek postoji pobjednička strategija za jednog od igrača što ćemo i dokazati.

Tvrdnja 3.0.9. *Svaka igra za dva igrača sa savršenom informacijom koja ima sumu nula i konačan broj poteza je strogo određena.*

Dokaz. Pretpostavimo da imamo dva igrača (nazovimo ih Paul i Carole) i pretpostavimo da ishod igre nije određen prije početka igre (prije prvog poteza). To znači da niti jedan od igrača nema pobjedničku strategiju prije početka igre. Nadalje, pretpostavimo da postoji konačan broj poteza koje igrači mogu odigrati kako bi pobijedili. Prvi Paulov potez ne može biti dio njegove pobjedničke strategije jer bi to značilo da je ishod igre određen prije početka igre. Slično, taj prvi potez ne može biti niti dio pobjedničke strategije za Carole. Prema tome, prvi potez je nedeterministički. To povlači da niti jedan od sljedećih poteza u igri ne može biti dio pobjedničke strategije jer uvijek možemo promatrati igru koja je započela u poziciji dobivenoj kao rezultat prvog poteza, reduciranu za jedan potez. Dakle, igra je beskonačna jer niti jedan potez ne može biti deterministički. No, to je u kontradikciji s pretpostavkom da je igra konačna. Prema tome, igra je strogo određena odnosno postoji pobjednička strategija za jednog od igrača. □

Primjetimo da iako pobjednička strategija za jednog od igrača postoji, nema garancije da će je igrač pronaći tijekom igre i iskoristiti.

3.1 Igra sigurnosti

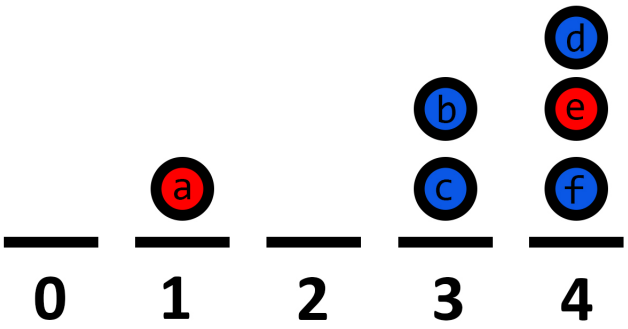
3.1.1 Opis i pravila

Paul, predsjednik odjela nekog fakulteta, pokušava promovirati jednog od svojih zaposlenika do stalnog (sigurnog) mjesta, no na putu mu stoji tvrdoglava rektorica Carole. Postoji k nivoa zaposlenja prije dobivanja stalnog mjesta. Označimo te nivoe s $1, \ldots, k$ pri čemu je nivo 1 najviši te označimo s 0 nivo stalnog zaposlenja. Za naše potrebe, svakog zaposlenika označit ćemo žetonom. $(x_1, \ldots, x_k)$ - igra sigurnosti počinje s x_i žetona na nivou i za sve $1 \leq i \leq k$ i bez ijednog žetona na nivou 0. Svake godine Paul predstavlja Carole skup S izabranih žetona (zaposlenika) koje želi promovirati. Carole može izabrati jednu od dvije opcije:

- promovirati sve žetone iz S i otpustiti sve ostale, ili
- promovirati sve žetone koji nisu u S i otpustiti sve one iz S.

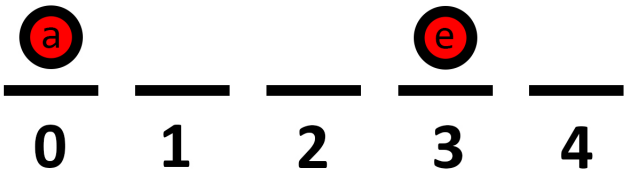
Promovirati zapravo znači pomaknuti s nivoa i na nivo $i - 1$, a otpustiti znači maknuti žetone iz igre. Ako neki od žetona dođe na nivo 0 (zaposlenik je dobio stalno zaposlenje), Paul je pobijedio, a inače je pobijedila Carole.

Ilustrirajmo sada primjerom prethodno objašnjenu igru uz $k = 4$ (postoje 4 nivoa prije nivoa stalnog zaposlenja). Označimo žetone (zaposlenike) slovima $a, b, c, \ldots, f$. Slika 3.1 prikazuje stanje na ploči na početku $(1, 0, 2, 3)$ - igre sigurnosti. Paul je prvi na potezu i pretpostavimo da je izabrao $S = \{a, e\}$ (na slici skup S čine crveni žetoni).



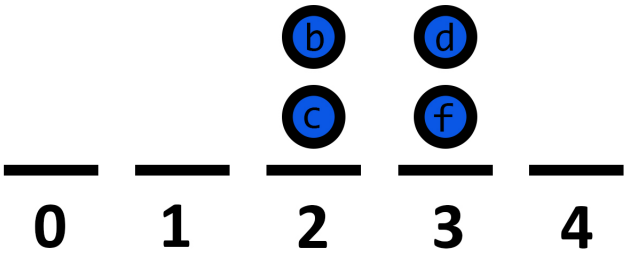
Slika 3.1: Početna situacija

Nakon toga, na potezu je Carole koja ima dvije opcije. Ako Carole izabere prvu opciju dolazimo do situacije na slici 3.2.



Slika 3.2: Carole je izabrala prvu opciju

U tom slučaju žeton a je dobio stalno zaposlenje pa je Paul pobjedio. Zato će Carole odabrati drugu opciju, odnosno otpustiti žetone iz S, a promovirati sve ostale. Tim potezom završen je prvi krug igre i situacija na ploči je prikazana slikom 3.3.



Slika 3.3: Carole je izabrala drugu opciju

U sljedećem krugu Paul ponovno izabire novi skup S, a Carole se odlučuje za jednu od dvije opcije. Okrutno pravilo igre prema kojem su jedine alternative promocija ili otkaz osigurava da igra završava unutar k godina, ili Paulovom pobjedom, ili tako da Carole uspješno eliminira sve žetone.

3.1.2 Randomizacija

Teorem 3.1.1. *Ako je*

$$\sum_i x_i 2^{-i} < 1\,,$$

onda Carole pobjeđuje u $(x_1, \ldots, x_k)$ *- igri sigurnosti.*

Dokaz. Fiksirajmo Paulovu strategiju. Tada Carole igra slučajno. To znači, da u svakom krugu nakon što Paul izabere skup žetona S, Carole baca simetričan novčić kako bi odlučila koju će opciju izabrati. Ako padne glava ona pomiče sve žetone koji nisu u S za jedno mjesto ulijevo, a ako padne pismo pomiče sve žetone iz S za jedno mjesto ulijevo. Neka je za svaki žeton c I_c indikatorska slučajna varijabla, odnosno

$$I_c = \begin{cases} 1\,, & \text{ako je } c \text{ dosegnuo nivo 0,} \\ 0\,, & \text{ako } c \text{ nije dosegnuo nivo 0.} \end{cases}$$

Neka je $X = \sum I_c$ broj žetona na kraju igre koji su dosegnuli nivo 0. Razmotrimo jedan žeton i označimo ga s c. U svakom krugu Paul može izabrati podskup S tako da vrijedi $c \in S$ ili $c \notin S$, ali u oba slučaja vjerojatnost da se c pomakne ulijevo je $\frac{1}{2}$. Pretpostavimo da se žeton c na početku nalazi na mjestu i. Taj žeton će na kraju igre ostati na ploči ako i samo ako je prvih i bacanja novčića dovelo do promoviranja žetona c. Tada je vjerojatnost ovog događaja $\mathbb{E}I_c$ jednaka upravo 2^{-i}. Zbog linearnosti očekivanja slijedi $\mathbb{E}X = \sum \mathbb{E}I_c = \sum_{i=1}^{k} x_i 2^{-i}$. Primjetimo da će Carole pobijediti ako i samo ako je $X = 0$. Pretpostavka teorema daje $\mathbb{E}X < 1$, a to znači da se događaj $\{X < 1\}$ mora dogoditi s pozitivnom vjerojatnosti. To zapravo znači da Carole mora pobijediti s pozitivnom vjerojatnosti. Paul nema strategiju koja bi mu uvijek omogućila pobjedu (kada bi je imao, tada bi vjerojatnost da Carole pobijedi morala biti nula, što nije slučaj), no kako se radi o igri sa savršenom informacijom u kojoj nema neriješenih rezultata netko mora imati savršenu strategiju koja uvijek pobjeđuje. Budući da to nije Paul, zaključujemo da Carole mora imati savršenu pobjedničku strategiju. □

Gornji dokaz daje lijep primjer korištenja vjerojatnosne metode, odnosno korištenja vjerojatnosne analize kako bismo dokazali neki deterministički rezultat. Kao što je i obično problem kod dokazivanja vjerojatnosnom metodom, ostaje otvoreno pitanje pronalaska koja je to točno pobjednička strategija. Gornji argument možemo derandomizirati kako bismo dali eksplicitnu strategiju za Carole.

3.1.3 Derandomizacija

Za poziciju $(y_1, \ldots, y_k)$, kod koje se na nivou i nalazi y_i žetona, definiramo težinu pozicije (igre) kao $\sum_i y_i 2^{-i}$. Primjetimo da je to zapravo $\mathbb{E}Y$, gdje je Y broj žetona koji bi dosegnuli nivo 0 kada bi Carole do kraja igre igrala na slučajan način. Razmotrimo bilo koju poziciju s težinom W i bilo koji Paulov odabir skupa S. Neka je W_1 nova težina nastala ako Carole pomakne sve žetone koji su u S za jedno mjesto ulijevo (odigra prvu opciju) i neka je W_2 nova težina nastala ako Carole pomakne sve žetone koji nisu u S za jedno mjesto ulijevo (odigra drugu opciju). Njezina strategija je da uvijek pomiče žetone tako da minimizira težinu, odnosno izabrat će prvu opciju ako je $W_1 < W_2$ i obratno. Tvrdimo da tada vrijedi $W = \frac{1}{2}(W_1 + W_2)$. Zaista, njezinu igru na slučajan način možemo shvatiti na sljedeći način: Carole najprije baca novčić kako bi donijela odluku o prvom potezu, a zatim igra slučajno tako da je, prema formuli (2.2), W prosjek dvaju uvjetnih očekivanja W_1 i W_2. Prema pretpostavci, na početku igre težina je manja od jedan. Eksplicitna strategija kojom igra Carole osigurava da se težina tijekom igre ne povećava pa je tijekom cijele igre težina manja od jedan. Kada bi neki žeton dosegnuo nivo 0, težina bi se povećala za jedan pa zaključujemo da se to nikad neće dogoditi i prema tome Carole pobjeđuje u igri.

3.1.4 Antirandomizacija

Igra sigurnosti ima lijepo svojstvo da kada nisu zadovoljeni uvjeti potrebni da Carole pobijedi, tada Paul može iskoristiti tu istu težinsku funkciju da bi razvio svoju pobjedničku strategiju. Taj proces nazivamo antirandomizacija.

Lema 3.1.2. *(Lema podjele) Neka su $x_1 \geq x_2 \geq \cdots \geq x_r$ negativne potencije broja 2 i neka je $x_1 + \cdots + x_r = 1$. Tada postoji particija od $\{x_i : i = 1, 2, \ldots, r\}$ u dvije grupe takva da je suma elemenata svake grupe jednaka točno $\frac{1}{2}$.*

Dokaz. Elemente x_i, $1 \leq i \leq r$, uzimamo redom po veličini i raspoređujemo u dvije grupe tako da u svakom koraku element x_i stavimo u onu grupu čija je trenutna suma manja. Kažemo da smo zapeli u l ako je, nakon što smo u grupe rasporedili elemente $x_1, \ldots, x_l$, apsolutna razlika suma elemenata po grupama veća od sume preostalih, još neraspoređenih elemenata $x_{l+1} + \cdots + x_r$. Pokazat ćemo, indukcijom po l, $0 \leq l \leq r$, da nikad ne možemo zapeti. Trivijalno, u $l = 0$ nismo zapeli. Pretpostavimo (pretpostavka indukcije) da nismo zapeli u $l - 1$. Tada imamo dva slučaja:

- Dvije grupe trenutno imaju različite sume. Budući da su svi $x_1, \ldots, x_{l-1}$ višekratnici od x_l, tada i razlika suma tih dviju grupa mora biti višekratnik od x_l. Dakle, ta razlika je najmanje x_l pa smještanjem elementa x_l u grupu koja ima manju sumu ne možemo zapeti.

- Dvije grupe trenutno imaju jednake sume. Kao i u prvom slučaju, ta suma mora biti oblika Ax_l, pri čemu je A neki cijeli broj. Prema tome $x_1 + \cdots + x_l$ je oblika $(2A + 1)\, x_l$, stoga je

$$x_{l+1} + \cdots + x_r = 1 - (2A + 1)\, x_l \geq x_l$$

  pa nakon smještanja elementa x_l u bilo koju od grupa nismo zapeli.

Dakle, nećemo zapeti ni u $l = r$, što znači da su nakon razmještanja svih elemenata $x_1, \ldots, x_r$ sume točno jednake. □

Korolar 3.1.3. *Neka su $x_1 \geq x_2 \geq \cdots \geq x_l$ negativne potencije broja 2 i neka je $x_1 + \cdots + x_l \geq 1$. Tada postoji particija od $\{x_i : i = 1, 2, \ldots, l\}$ u dvije grupe takva da je suma elemenata svake grupe najmanje $\frac{1}{2}$.*

Dokaz. Ako je $x_1 + \cdots + x_l > 1$, onda je (budući da se radi o višekratniku od x_l) $x_1 + \cdots + x_{l-1} \geq 1$. Redom maknimo $x_l, x_{l-1}, \ldots$ dok ne dobijemo $x_1 + \cdots + x_r = 1$. Tada tvrdnja slijedi primjenom leme 3.1.2 . □

Teorem 3.1.4. *Ako je*

$$\sum_i x_i 2^{-i} \geq 1\,,$$

onda Paul pobjeđuje u $(x_1, \ldots, x_k)$ - igri sigurnosti.

Dokaz. Početna težina je najmanje jedan. Prema korolaru 3.1.3 Paul može podijeliti žetone u dva dijela pri čemu svaki dio ima težinu najmanje $\frac{1}{2}$. Nakon podjele, Paul izabere jedan od ta dva dijela za skup S. Carole pomakne sve žetone iz jednog od ta dva dijela (ili žetone iz S, ili one koji nisu u S) za jedno mjesto ulijevo te tako udvostruči njihovu težinu i postavi težinu nove pozicije na najmanje jedan. Stoga, bez obzira za koji potez se Carole odluči, na kraju svakog kruga vrijednost težine nikad nije manja od jedan. Prema tome, igra ne može završiti bez ijednog žetona na ploči (jer bi to značilo da je na kraju težina nula) pa igra mora završiti Paulovom pobjedom. □

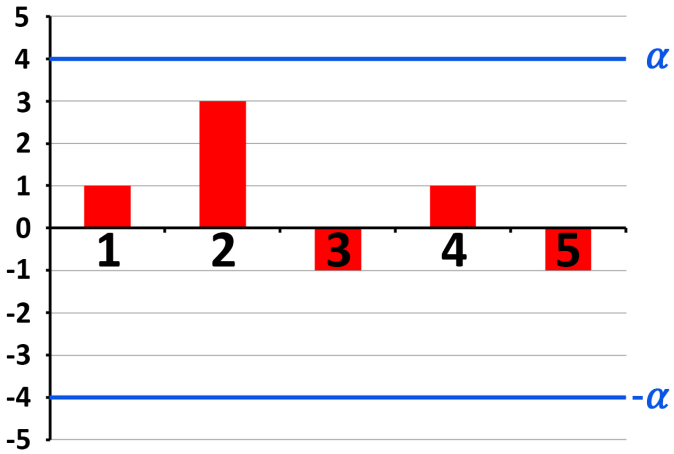
3.2 Igra uravnoteženih vektora

3.2.1 Opis i pravila

Igra uravnoteženih vektora je igra za dva igrača (u našem slučaju su to opet Paul i Carole) sa savršenom informacijom. Na početku igre zadan je parametar n koji označava broj krugova igre i vektor pozicije $P \in \mathbb{R}^n$ postavljen je na $\mathbf{0}$. Svaki krug igre sastoji se od dva dijela. Prvo Paul izabere $v \in \{-1, 1\}^n$, a zatim Carole postavi P ili na $P + v$ ili na $P - v$. Neka P^{kraj} označava vrijednost od P na kraju igre. Isplata koju Paul dobiva od Carole tada iznosi $|P^{\text{kraj}}|_\infty$, odnosno to je najveća apsolutna vrijednost od n koordinata vektora pozicije P^{kraj}.

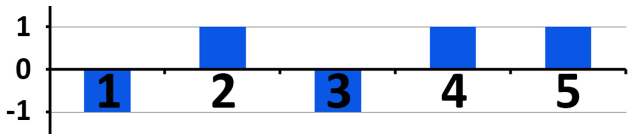
Za dani cjelobrojni parametar $\alpha \geq 0$ definirat ćemo (α, n) - igru uravnoteženih vektora na sljedeći način: kažemo da je pobijedio Paul ako je $|P^{\text{kraj}}|_\infty \geq \alpha$, a da je pobijedila Carole ako je $|P^{\text{kraj}}|_\infty < \alpha$. S $VAL(n)$ ćemo označiti vrijednost igre, tj. najveći parametar $\alpha \geq 0$ takav da Paul ima strategiju za pobjedu. To znači da Paul može pobijediti u (α, n) - igri uravnoteženih vektora čim je $\alpha \leq VAL(n)$, dok za $\alpha > VAL(n)$ pobjeđuje Carole. Prema tome, odluke o pobjedniku (α, n) - igre uravnoteženih vektora, za različite vrijednosti α, dat će ograde na vrijednost od $VAL(n)$.

Ilustrirajmo sada primjerom prethodno objašnjenu igru. Neka je npr. $n = 5$ i $\alpha = 4$. Tada promatramo $(4, 5)$ - igru uravnoteženih vektora koja se odvija u 5 krugova. Na početku igre vektor pozicije $P \in \mathbb{R}^5$ je $P = (0, 0, 0, 0, 0)$. Pretpostavimo da su već odigrana tri kruga igre i da je u tom trenutku vektor pozicije $P = (1, 3, -1, 1, -1)$. Ta situacija prikazana je na slici 3.4.



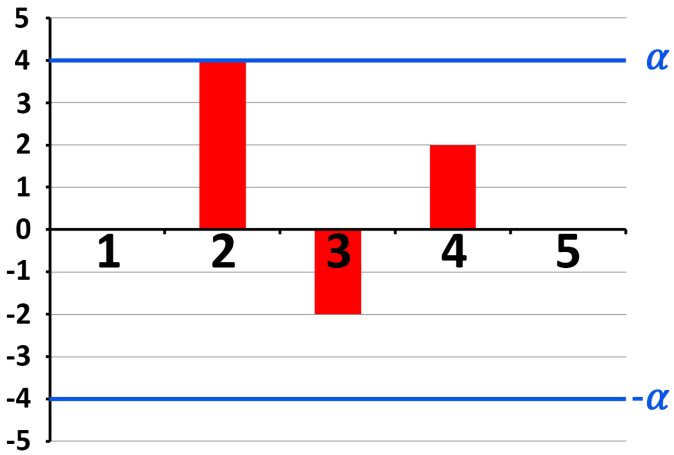
Slika 3.4: Početna situacija

Pretpostavimo da u sljedećem potezu Paul odabere vektor poteza $v = (-1, 1, -1, 1, 1)$ koji je prikazan na slici 3.5.



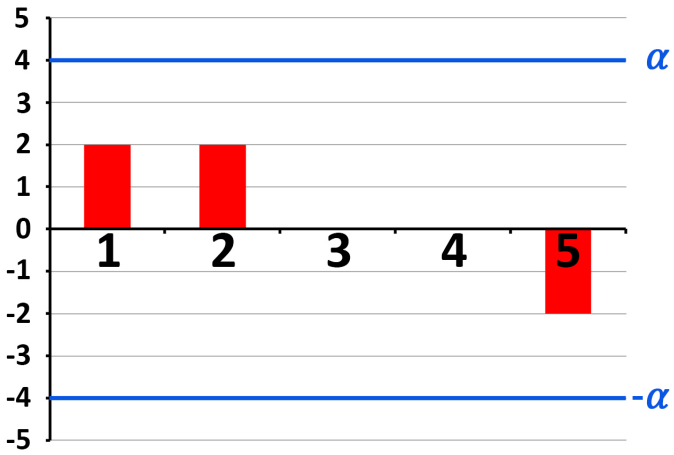
Slika 3.5: Paulov vektor poteza

Ako Carole odabere prvu opciju i postavi vektor pozicije na $P + v$, onda je novi vektor pozicije $P = (0, 4, -2, 2, 0)$ i ta situacija je prikazana na slici 3.6.



Slika 3.6: Carole je izabrala prvu opciju

Ako pak Carole odabere drugu opciju i postavi vektor pozicije na $P - v$, onda je novi vektor pozicije $P = (2, 2, 0, 0, -2)$ i ta situacija je prikazana na slici 3.7.



Slika 3.7: Carole je izabrala drugu opciju

Time je završen četvrti krug igre i u zadnjem krugu Paul ponovno odabire neki vektor poteza v, a Carole bira jednu od dvije opcije (pomiče P na $P + v$ ili $P - v$) i time određuje konačni vektor pozicije P^{kraj}. U tom trenutku igra završava i kažemo da je pobijedio Paul ako je $|P^{\text{kraj}}|_\infty \geq \alpha$, odnosno da je pobijedila Carole ako je $|P^{\text{kraj}}|_\infty < \alpha$.

3.2.2 Randomizacija

Napomena 3.2.1. *S_n je slučajna varijabla definirana sa*

$$S_n = X_1 + \cdots + X_n,$$

gdje je $\mathbb{P}(X_i = 1) = \mathbb{P}(X_i = -1) = \frac{1}{2}$ i slučajne varijable X_i su međusobno nezavisne. To je zapravo jednostavna simetrična slučajna šetnja na $\mathbb{Z}$.

Teorem 3.2.2. *Ako je*

$$\mathbb{P}(|S_n| \geq \alpha) < \frac{1}{n},$$

onda Carole pobjeđuje u (α, n) - igri uravnoteženih vektora.

Dokaz. Pretpostavimo da Carole igra slučajno, tj. u svakom krugu nakon što Paul odabere $v \in \mathbb{R}^n$, Carole baca simetričan novčić kako bi odlučila hoće li postaviti pozicijski vektor P na $P + v$ ili $P - v$. Fiksirajmo neku deterministčku strategiju za Paulovu igru. U tom slučaju, za svaku od koordinata promatramo vjerojatnost da ona na kraju igre ima apsolutnu vrijednost najmanje α. Primjetimo da je ta vjerojatnost jednaka $\mathbb{P}(|S_n| \geq \alpha)$ bez obzira na Paulovu strategiju. Razlog tome je što Paul može izabrati 1 ili -1 za koordinatu u v, ali

u oba slučaja se koordinata od P promijeni za $+1$ ili -1 s vjerojatnošću $\frac{1}{2}$. Prema tome, koordinate od P^{kraj} imaju istu distribuciju kao S_n. Neka je T broj koordinata od P^{kraj} čije su apsolutne vrijednosti najmanje α, tako da je T slučajna varijabla. Za svaku koordinatu $1 \leq i \leq n$ neka je I_i indikatorska slučajna varijabla koja govori ima li i-ta koordinata od P^{kraj} apsolutnu vrijednost najmanje α. Tada je $T = \sum I_i$. Zatim, prema linearnosti očekivanja slijedi

$$\mathbb{E}T = \sum_{i=1}^{n} \mathbb{E}I_i = n \cdot \mathbb{P}\left(|S_n| \geq \alpha\right).$$

Primjetimo da Paul pobjeđuje ako i samo ako je $T \geq 1$. Naša pretpostavka je da je $\mathbb{E}T < 1$ pa vrijedi

$$\mathbb{P}(\{\text{Paul pobjeđuje}\}) = \mathbb{P}(T \geq 1) < 1.$$

Budući da je (α, n) - igra uravnoteženih vektora igra sa savršenom informacijom u kojoj nema neriješenih rezultata jedan od igrača mora imati savršenu pobjedničku strategiju. Kada bi Paul imao savršenu pobjedničku strategiju, on bi mogao pobijediti sa vjerojatnošću jedan, što nije slučaj. Stoga, Carole mora imati savršenu pobjedničku strategiju. □

3.2.3 Derandomizacija

Kao i u igri sigurnosti, koristimo ovu randomiziranu strategiju kako bismo došli do težinske funkcije koja daje deterministička strategiju.

Definirajmo težinu pozicije kao očekivani broj $\mathbb{E}T$ koordinata od P^{kraj} koje imaju apsolutnu vrijednost najmanje α ukoliko Carole igra slučajno preostali dio igre. Eksplicitno, pretpostavimo da je $P = (x_1, \ldots, x_n)$ i da je preostalo još r krugova igre. Tada P ima težinu

$$w(P, r) = \sum_{i=1}^{n} \mathbb{P}(|x_i + S_r| \geq \alpha).$$

Za poziciju P Paul odabire $v \in \{-1, 1\}^n$. Carole tada odlučuje hoće li promijeniti P u $P + v$ ili $P - v$, ovisno o tome koji od ova dva izbora ima manju težinu. Ključna stvar ovdje je da je, prema formuli (2.2),

$$w(P, r+1) = \frac{1}{2}\left(w(P+v, r) + w(P-v, r)\right),$$

jer je slučajno igranje kroz cijelu igru jednako prosjeku od igranja $P+v$ u narednom potezu i dalje slučajno i igranja $P - v$ u narednom potezu i dalje slučajno. Početni vektor pozicije $P = \mathbf{0}$ ima težinu $w(\mathbf{0}, n) = n \cdot \mathbb{P}(|S_n| \geq \alpha) < 1$ prema pretpostavci. Ako je $w(P, r+1) < 1$, slijedi da je ili $w(P + v, r) < 1$ ili $w(P - v, r) < 1$ pa ova strategija osigurava Carole da će i za novi P vrijediti $w(P, r) < 1$. Ako Carole nastavi igrati na ovaj način, na kraju

igre dobivamo $w(P^{\text{kraj}}, 0) < 1$. No, na kraju igre $w(P^{\text{kraj}}, 0)$ predstavlja broj koordinata koje imaju apsolutnu vrijednost najmanje α. Prema tome, $w(P^{\text{kraj}}, 0) = 0$ pa je Carole pobijedila.

Primjetimo da su težine $w(P, r)$ sume binomnih koeficijenata pa se mogu efikasno izračunati i u svakom krugu igre Carole mora izračunati samo dvije takve težine.

Lema 3.2.3. *Za $k \in \mathbb{Z}$ vrijedi:*

$$\mathbb{P}(S_r = k) = \begin{cases} \frac{1}{2^r}\binom{r}{\frac{r-k}{2}}, & \text{ako su } r \text{ i } k \text{ iste parnosti}, \\ 0, & \text{inače}. \end{cases}$$

Pritom za binomne koeficijente podrazumijevamo

$$\binom{m}{l} = \begin{cases} \frac{m!}{l!(m-l)!}, & \text{za } l, m \in \mathbb{N}_0, 0 \leq l \leq m, \\ 0, & \text{inače}. \end{cases}$$

Dokaz. Prema napomeni 3.2.1 znamo da je $S_r = X_1 + \cdots + X_r$. Na skupu $\{S_r = k\}$ mora l varijabli X_j biti jednako -1, a d varijabli X_j jednako 1, pri čemu je:

$$\begin{cases} l \cdot (-1) + d \cdot 1 = k \\ l + d \quad\;\; = r. \end{cases}$$

Iz gornjeg sustava dobivamo $l = \frac{r-k}{2}$ i $d = \frac{r+k}{2}$. Prema tome,

$$\mathbb{P}(S_r = k) = \binom{r}{\frac{r-k}{2}} \cdot \left(\frac{1}{2}\right)^r, \text{ ako su } r \text{ i } k \text{ iste parnosti (tj. } 2 \mid r-k),$$
$$\mathbb{P}(S_r = k) = 0, \qquad \text{inače}$$

(ako su r i k različite parnosti, S_r ne može doći u poziciju k). □

Prema prethodnoj lemi zapravo imamo

$$w(P, r) = \sum_{i=1}^{n} \frac{1}{2^r} \sum_{\substack{k \in \mathbb{Z} \\ 2 \mid r-k \\ |x_i + k| \geq \alpha}} \binom{r}{\frac{r-k}{2}}.$$

3.2.4 Antirandomizacija

Provest ćemo proces antirandomizacije kako bismo dobili strategiju kojom Paul može igrati da bi pobijedio uz odgovarajuće vrijednosti polaznih parametara. Na početku, iskažimo i dokažimo lemu čiji ćemo rezultat kasnije koristiti.

Lema 3.2.4. *Među binomnim koeficijentima* $\binom{r}{l}$*, pri čemu je* $l = 0, 1, \ldots, r$ *najveći je upravo „srednji“* $\binom{r}{\lfloor r/2 \rfloor}$.

Dokaz.

$$\begin{aligned} & \binom{r}{l} \leq \binom{r}{l+1}, \qquad l \in \{0, \ldots, r-1\} \\ \Leftrightarrow \ & \frac{r!}{l!(r-l)!} \leq \frac{r!}{(l+1)!(r-l-1)!} \\ \Leftrightarrow \ & l+1 \leq r-l \\ \Leftrightarrow \ & l \leq \frac{r-1}{2} \end{aligned}$$

Za parne r imamo:

$$\binom{r}{0} \leq \ldots \leq \binom{r}{\frac{r-2}{2}} \leq \binom{r}{\frac{r}{2}} > \ldots > \binom{r}{r},$$

a za neparne:

$$\binom{r}{0} \leq \ldots \leq \binom{r}{\frac{r-1}{2}} = \binom{r}{\frac{r+1}{2}} > \ldots > \binom{r}{r}. \qquad \square$$

Neka je $P = (a_1, \ldots, a_n)$ vektor pozicije u trenutku kada je preostalo još $r+1$ krugova igre. Pretpostavimo da Paul tada odabire vektor $v = (\epsilon_1, \ldots, \epsilon_n)$. Tada je

$$\begin{aligned} w(P+v, r) - w(P-v, r) &= \sum_{i=1}^{n} \left[\mathbb{P}\left(|a_i + \epsilon_i + S_r| \geq \alpha\right) - \mathbb{P}\left(|a_i - \epsilon_i + S_r| \geq \alpha\right) \right] \\ &= \sum_{i=1}^{n} \epsilon_i z_i, \end{aligned}$$

gdje je

$$z_i = \mathbb{P}\left(|a_i + 1 + S_r| \geq \alpha\right) - \mathbb{P}\left(|a_i - 1 + S_r| \geq \alpha\right).$$

Primjetimo da sada možemo pisati

$$\begin{aligned} z_i &= \mathbb{P}\left(|a_i + 1 + S_r| \geq \alpha\right) - \mathbb{P}\left(|a_i - 1 + S_r| \geq \alpha\right) \\ &= \sum_{\substack{k \in \mathbb{Z} \text{ ima istu} \\ \text{parnost kao } r \\ k \geq -a_i - 1 + \alpha \text{ ili} \\ k \leq -a_i - 1 - \alpha}} \mathbb{P}(S_r = k) \quad - \sum_{\substack{k \in \mathbb{Z} \text{ ima istu} \\ \text{parnost kao } r \\ k \geq -a_i + 1 + \alpha \text{ ili} \\ k \leq -a_i + 1 - \alpha}} \mathbb{P}(S_r = k) \\ &= \begin{cases} \mathbb{P}(S_r = -a_i - 1 + \alpha) - \mathbb{P}(S_r = -a_i + 1 - \alpha), & \text{ako } 2 \,|\, a_i + 1 + \alpha + r \\ \mathbb{P}(S_r = -a_i + \alpha) - \mathbb{P}(S_r = -a_i - \alpha), & \text{ako } 2 \,|\, a_i + \alpha + r. \end{cases} \end{aligned}$$

Naime, svi osim dva člana u ovim sumama će se pokratiti prilikom oduzimanja. Pretpostavimo da je $\alpha \geq 1$, jer je inače to očigledno. Sada možemo preciznije reći da pribrojnici s pozitivnim predznakom ostaju jedino za

$$k \in [-a_i - 1 + \alpha, -a_i + 1 + \alpha\rangle,$$

dok preostali pribrojnici s negativnim predznakom odgovaraju

$$k \in \langle -a_i - 1 - \alpha, -a_i + 1 - \alpha].$$

Jasno je da u svakom od ta dva intervala duljine 2 postoji točno po jedan cijeli broj k iste parnosti kao r, ali ako želimo dobiti precizniji izraz kao u gornjoj formuli, onda razlikujemo slučajeve.

- *Slučaj 1.* r ima različitu parnost od $-a_i \pm \alpha$
  Preostali pribrojnici se dobiju upravo za

$$k = -a_i - 1 + \alpha \text{ i } k = -a_i + 1 - \alpha.$$

- *Slučaj 2.* r ima istu parnost kao $-a_i \pm \alpha$
  Preostali pribrojnici se dobiju upravo za

$$k = -a_i + \alpha \text{ i } k = -a_i - \alpha.$$

Dakle, z_i možemo ograničiti s

$$\begin{aligned} |z_i| &\leq \max_{k \in \mathbb{Z}} \mathbb{P}(S_r = k) \\ &\leq \max_{k \in \mathbb{Z}} \frac{1}{2^r} \binom{r}{\frac{r-k}{2}} \\ &= \binom{r}{\lfloor r/2 \rfloor} \cdot 2^{-r}. \end{aligned}$$

Budući da preciznu lemu podjele 3.1.2 iz igre sigurnosti ne možemo primijeniti u kontekstu igre uravnoteženih vektora, dat ćemo tzv. lemu približne podjele koja će nam još uvijek omogućiti koristan rezultat.

Lema 3.2.5. *(Lema približne podjele) U svakom od poteza u igri uravnoteženih vektora Paul može izabrati vektor $v = (\epsilon_1, \ldots, \epsilon_n)$ tako da u svakom trenutku vrijedi*

$$|w(P + v, r) - w(P - v, r)| \leq \binom{r}{\lfloor r/2 \rfloor} \cdot 2^{-r},$$

pri čemu r označava broj poteza do kraja igre.

Dokaz. Redom odabiremo ϵ_i tako da uvijek minimiziramo apsolutnu vrijednost parcijalne sume $\epsilon_1 z_1 + \cdots + \epsilon_l z_l$. Preciznije, ukoliko je prethodna suma $\epsilon_1 z_1 + \cdots + \epsilon_{l-1} z_{l-1}$ bila pozitivna (negativna), tada odabiremo ϵ_l koji smanjuje (povećava) sumu. Uz bilo koju ogradu K na $|z_i|$ ovaj pohlepni algoritam osigurava da će sve takve apsolutne vrijednosti biti najviše K. □

Teorem 3.2.6. *Ako je*

$$\mathbb{P}(|S_n| \geq \alpha) > \frac{1}{n} \sum_{r=0}^{n-1} \binom{r}{\lfloor r/2 \rfloor} \cdot 2^{-r-1},$$

onda Paul pobjeđuje u (α, n) *- igri uravnoteženih vektora.*

Dokaz. Paulova strategija je da uvijek odabire vektor v tako da su težine $w(P + v, r)$ i $w(P - v, r)$ što je moguće bliže jedna drugoj (preciznije, igra kao u lemi 3.2.5). Kako je $w(P, r + 1)$ uvijek prosjek od $w(P + v, r)$ i $w(P - v, r)$, vektor v iz leme 3.2.5 osigurava da je

$$w(P \pm v, r) \geq w(P, r + 1) - \frac{1}{2} \binom{r}{\lfloor r/2 \rfloor} \cdot 2^{-r},$$

u trenutku kada je preostalo još $r + 1$ poteza do kraja igre. Na početku igre je $w(\mathbf{0}, n) = n \cdot \mathbb{P}(|S_n| \geq \alpha)$ pa slijedi da je i na kraju igre

$$\begin{aligned} w(P^{\text{kraj}}, 0) &\geq w(\mathbf{0}, n) - \sum_{r=0}^{n-1} \binom{r}{\lfloor r/2 \rfloor} \cdot 2^{-r-1} \\ &= n \cdot \mathbb{P}(|S_n| \geq \alpha) - \sum_{r=0}^{n-1} \binom{r}{\lfloor r/2 \rfloor} \cdot 2^{-r-1} \ > 0. \end{aligned}$$

No, $w(P^{\text{kraj}}, 0)$ je broj koordinata koje imaju apsolutnu vrijednost najmanje α i kada je taj broj pozitivan Paul je pobijedio. Prema tome, zaključujemo da igrajući ovakvom strategijom, Paul pobjeđuje u (α, n) - igri uravnoteženih vektora. □

Uz zadani parametar n, za vrijednost igre $VAL(n)$ mogu se izračunati gornja i donja ograda. Asimptotika od $VAL(n)$ dana je sljedećim teoremom, kojeg nećemo dokazivati jer je njegov dokaz tehnički složen, a pronalazak odgovarajućih konstanti zahtijeva naporan račun. Više detalja o tome može se pronaći u knjizi [1] i članku [4].

Teorem 3.2.7.

$$VAL(n) = \Theta(\sqrt{n \ln n}),$$

tj. postoje $c, C > 0$ *takvi da je*

$$c\sqrt{n \ln n} \leq VAL(n) \leq C\sqrt{n \ln n}\,.$$

3.3 Igra lažova

3.3.1 Opis i pravila

Igra lažova je igra za dva igrača (Paul i Carole) zadana pomoću sljedeća tri parametra:

- n - veličina prostora pretraživanja,
- q - broj krugova igre, tj. broj pitanja koje Paul može postaviti Carole,
- k - broj laži koje Carole smije iskoristiti.

Oba igrača znaju vrijednosti ovih parametara. Carole zamisli cijeli broj x iz prostora pretraživanja (skupa $\{1, \ldots, n\}$), a Paulov zadatak je pogoditi taj broj x koristeći najviše q pitanja. Paul postavlja pitanja oblika „Je li $x \in L$?“, gdje je $L \subseteq \{1, \ldots, n\}$. U svakom krugu igre, Paul prije postavljanja novog pitanja može koristiti sve odgovore koje je dobio na prethodna pitanja. Carole može igrati protivničkom strategijom, tj. ona ne mora zamisliti cijeli broj x odmah na početku igre, ali mora igrati tako da na kraju igre zaista postoji barem jedan cijeli broj x kojeg je mogla izabrati iz prostora pretraživanja na početku igre. Uz to, ona čak smije najviše k puta slagati, tj. pogrešno odgovoriti na postavljeno pitanje. Budući da se radi o igri sa savršenom informacijom, možemo zaključiti da jedan od igrača mora pobijediti u ovoj igri. Paul će pobijediti ako uspije u q krugova igre utvrditi broj x koji je Carole zamislila, a u suprotnom pobjeđuje Carole. Ovakav tip igre poznat je pod nazivom $[n, q, k]$ - igra lažova.

Kako bismo lakše analizirali ovu igru, razmotrit ćemo njezinu općenitiju verziju u kojoj prostor pretraživanja zamjenjujemo konačnim nizom nenegativnih cijelih brojeva $x_0, x_1, \ldots, x_k$. Definirat ćemo A_i, $0 \leq i \leq k$, kao disjunktne skupove takve da je $|A_i| = x_i$ i igračima su ti skupovi poznati u svakom trenutku igre. Na početku igre Carole odabere cijeli broj $x \in A_0 \cup A_1 \cup \ldots \cup A_k$ i ako je $x \in A_i$ tada Carole smije lagati o vrijednosti broja x najviše $k - i$ puta za sljedeća pitanja. Takvu igru zvat ćemo $[(x_0, \ldots, x_k), q]$ - igra lažova.

Slično kao i u igri sigurnosti, objasnit ćemo ovu igru pomoću žetona. Zamislimo ploču s mjestima $0, 1, \ldots, k$. Svaki cijeli broj x reprezentiran je jednim žetonom. Ako je žeton koji predstavlja broj x smješten na mjestu i, gdje je $0 \leq i \leq k$, Carole može lagati još $k - i$ puta za taj žeton. Za svako mjesto i, označimo broj žetona na tom mjestu s x_i. Kao što smo i prije rekli, igra traje q krugova. U svakom krugu igre, Paul odabire skup žetona L i postavlja pitanje „Je li $x \in L$?“, a Carole ima dvije opcije:

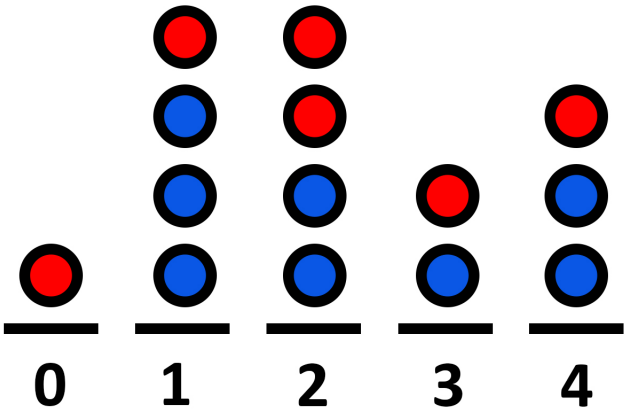
- može odgovoriti *Ne*, što je ekvivalentno pomicanju svih žetona iz L za jedno mjesto udesno.
- može odgovoriti *Da*, što je ekvivalentno pomicanju svih žetona koji nisu u L za jedno mjesto udesno.

U ovoj igri, za razliku od igre sigurnosti, na ploči ostaju i svi preostali žetoni koji se ne pomiču u tom krugu igre. Jedini žetoni koji se miču s ploče su oni žetoni koji su se prilikom pomicanja nalazili na mjestu k. Na kraju igre, nakon kruga q, preostali žetoni na ploči odgovaraju mogućim vrijednostima broja x. Ukoliko na kraju igre nema niti jednog žetona na ploči zaključujemo da je Carole varala. Pravila igre prilagodimo tako da dopustimo Carole da vara, ali inzistirajući na tome da izgubi igru ako je varala. S ovom modifikacijom, Paul pobjeđuje ako je na kraju igre na ploči preostao najviše jedan žeton.

Prikažimo ovu igru i u vektorskom zapisu kako bismo mogli koristiti dokaze i ideje iz prethodno opisane igre uravnoteženih vektora. Ako se na mjestu i nalazi b_i žetona, onda vektor $P = (b_0, \ldots, b_k)$ zovemo pozicijski vektor. Ako skup L na mjestu i sadrži c_i žetona, onda vektor $v = (c_0, \ldots, c_k)$ zovemo Paulov vektor poteza. Definiramo da je $P +^* v$ novi pozicijski vektor ukoliko Carole odigra prvu opciju i da je $P -^* v$ novi pozicijski vektor ukoliko Carole odigra drugu opciju. Eksplicitno zapisano,

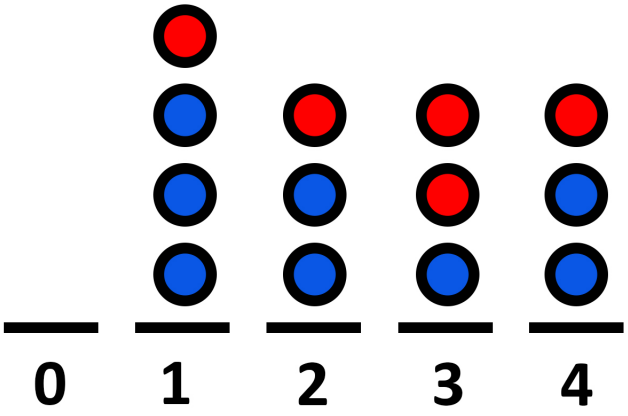
$$P +^* v = (b_0 - c_0, b_1 - c_1 + c_0, \ldots, b_i - c_i + c_{i-1}, \ldots, b_k - c_k + c_{k-1}) ,$$
$$P -^* v = (c_0, c_1 + b_0 - c_0, \ldots, c_i + b_{i-1} - c_{i-1}, \ldots, c_k + b_{k-1} - c_{k-1}) .$$

Ilustrirajmo sada primjerom prethodno objašnjenu igru uz $k = 4$ (Carole je dopušteno lagati najviše 4 puta). Slika 3.8 prikazuje stanje na ploči na početku $[(1, 4, 4, 2, 3), q]$ - igre lažova. Paul je prvi na potezu i pretpostavimo da je za skup L izabrao žetone koji su na slici označeni crvenom bojom te postavlja pitanje „Je li $x \in L$?“.



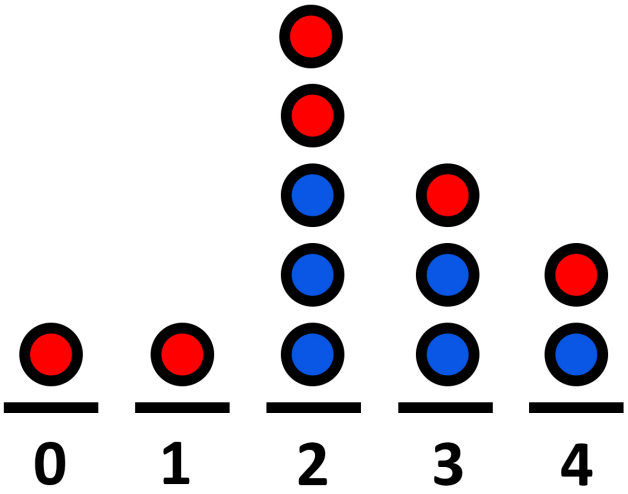
Slika 3.8: Početna situacija

U vektorskom zapisu to znači da je vektor pozicije $P = (1, 4, 4, 2, 3)$, a vektor poteza $v = (1, 1, 2, 1, 1)$. Nakon toga, na potezu je Carole, koja ima dvije opcije. Ako Carole izabere prvu opciju, odnosno odgovori *Ne*, pomičemo za jedno mjesto udesno sve žetone iz L i dolazimo do situacije na slici 3.9.



Slika 3.9: Carole je izabrala prvu opciju

U vektorskom zapisu tada imamo da je novi vektor pozicije $P +^* v = (0, 4, 3, 3, 3)$. Također, primjetimo da je žeton iz skupa L koji se nalazi na mjestu 4 maknut s ploče. Ako Carole izabere drugu opciju, odnosno odgovori *Da*, pomičemo za jedno mjesto udesno sve žetone koji nisu iz L i dolazimo do situacije na slici 3.10.



Slika 3.10: Carole je izabrala drugu opciju

U vektorskom zapisu tada imamo da je novi vektor pozicije $P-^{*}v = (1, 1, 5, 3, 2)$. Također, primjetimo da su s ploče maknuta dva žetona koja nisu bila u skupu L, a nalazila su se na mjestu 4. Time je završen jedan krug igre i Paulu je sada preostalo $q - 1$ pitanje. U sljedećem krugu Paul ponovno izabire novi skup L, a Carole se odlučuje za jednu od dvije opcije. Igra se nastavlja na ovaj način i Paul će pobijediti ako nakon q postavljenih pitanja na ploči ostane najviše jedan žeton.

3.3.2 Randomizacija

Neka $B\left(s, \frac{1}{2}\right)$ označava uobičajenu binomnu distribuciju, odnosno broj glava dobivenih u s nezavisnih bacanja simetričnog novčića. U daljnjem će nam B_s biti neka slučajna varijabla koja ima upravo tu razdiobu.

Teorem 3.3.1. *Ako je*

$$\sum_{i=0}^{k} x_i \mathbb{P}\left(B_q \leq k - i\right) > 1\,,$$

onda Carole pobjeđuje u $[(x_0, \ldots, x_k), q]$ *- igri lažova.*

Dokaz. Fiksirajmo Paulovu strategiju. Zamislimo da Carole igra slučajno, tj. u svakom krugu igre nakon što Paul odabere skup L Carole baca simetričan novčić kako bi odlučila koju će od dvije opcije odigrati. Tada za svaki žeton možemo računati vjerojatnost da on

ostane na ploči. Primjetimo da je, bez obzira na Paulovu strategiju, za žeton koji se na početku igre nalazi na mjestu i ta vjerojatnost jednaka $\mathbb{P}\left(B_q \leq k-i\right) = 2^{-q}\sum_{j=0}^{k-i}\binom{q}{j}$. To vrijedi jer u svakom krugu, bez obzira smjesti li Paul taj žeton u skup L ili ne, taj žeton se s vjerojatnošću $\frac{1}{2}$ pomakne za jedno mjesto.

Neka je X broj žetona preostalih na ploči i neka je za svaki preostali žeton c indikatorska slučajna varijabla označena sa I_c, odnosno

$$I_c = \begin{cases} 1, & \text{ako je } c \text{ ostao na ploči,} \\ 0, & \text{ako } c \text{ nije ostao na ploči .} \end{cases}$$

Tada je $X = \sum I_c$ (gdje suma ide po svim žetonima) pa zbog linearnosti očekivanja slijedi

$$\mathbb{E}X = \sum \mathbb{E}I_c = \sum_{i=0}^{k} x_i \mathbb{P}\left(B_q \leq k-i\right) .$$

Primjetimo da će Paul pobijediti ako i samo ako je $X \leq 1$. Prema pretpostavci teorema je $\mathbb{E}X > 1$, a to znači da je vjerojatnost da Paul pobijedi jednaka $\mathbb{P}(X \leq 1) < 1$. Budući da je igra lažova igra sa savršenom informacijom u kojoj nema neriješenih rezultata, netko od njih dvoje mora imati savršenu strategiju koja uvijek pobjeđuje. Kada bi Paul imao savršenu strategiju, vjerojatnost za njegovu pobjedu bi morala biti 1, što nije slučaj. Prema tome, Carole mora imati savršenu pobjedničku strategiju. □

Korolar 3.3.2. *Ako je*

$$n > \frac{2^q}{\sum_{j=0}^{k}\binom{q}{j}},$$

onda Carole pobjeđuje u (n, q, k) *- igri lažova.*

Dokaz. U prethodnom teoremu treba uzeti $x_0 = n$ te $x_i = 0$ za $i \geq 1$. Osim toga, već smo bili primijetili da je

$$\mathbb{P}(B_q \leq k) = 2^{-q}\sum_{j=0}^{k}\binom{q}{j}.$$ □

3.3.3 Derandomizacija

Definirajmo težinu pozicije kao očekivani broj $\mathbb{E}X$ žetona na kraju igre, ako Carole preostali dio igre odigra na slučajan način. Eksplicitno, vektor pozicije $P = (b_0, \ldots, b_k)$ uz preostalih r poteza ima težinu

$$w(P) = \sum_{i=0}^{k} b_i \mathbb{P}\left(B_r \leq k-i\right) .$$

Paul sada predstavlja Carole vektor poteza v. Njezina strategija je da odabere onu opciju kojom će nova pozicija ($P +^* v$ ili $P -^* v$) imati veću težinu. Primjetimo da su, kao i u igri uravnoteženih vektora, težine zapravo sume binomnih koeficijenata pa se mogu efikasno izračunati i u svakom krugu Carole mora izračunati samo dvije takve težine. Ključna stvar ovdje je da je, prema formuli (2.2),

$$w(P) = \frac{1}{2}\left(w(P +^* v) + w(P -^* v)\right) .$$

To je zaista čak i očigledno jer je težina pozicije dobivena ako Carole igra na slučajan način kroz cijelu igru zapravo jednaka srednjoj vrijednosti dobivenih težina pozicije ako Carole odigra prvu opciju i dalje nastavi igrati slučajno i ako odigra drugu opciju i dalje nastavi igrati slučajno. Prema pretpostavci, početna pozicija imala je težinu

$$w(P) = \sum_{i=0}^{k} x_i \mathbb{P}\left(B_q \leq k - i\right) > 1 .$$

Budući da strategija kojom igra Carole osigurava da se težina pozicije ne smanjuje, zaključujemo da je konačna težina veća od jedan. Kako je konačna težina jednaka broju preostalih žetona na ploči, Carole je pobjedila.

3.3.4 Antirandomizacija

Pronađimo sada pobjedničku strategiju za Paula. Pokažimo najprije primjerom da u ovoj igri ne vrijedi obrat teorema 3.3.1, odnosno korolara 3.3.2 (za razliku od igre sigurnosti, gdje je vrijedio obrat teorema 3.1.1 iz randomizacije).

Primjer 3.3.3. Promotrimo igru lažova s parametrima $n = 5$, $q = 5$, $k = 1$. To znači da Carole bira jedan broj iz skupa $\{1, \ldots, 5\}$ i ima najviše jednu mogućnost laganja, a Paul može postaviti najviše 5 pitanja kako bi utvrdio broj koji je Carole zamislila. To je zapravo $[(5, 0), 5]$ - igra lažova, odnosno početni vektor pozicije je $P = (5, 0)$. Tada je težina početne pozicije

$$\begin{aligned} w(P) &= \sum_{i=0}^{1} x_i \cdot \mathbb{P}\left(B\left(5, \frac{1}{2}\right) \leq 1 - i\right) \\ &= x_0 \cdot \mathbb{P}\left(B\left(5, \frac{1}{2}\right) \leq 1\right) + x_1 \cdot \mathbb{P}\left(B\left(5, \frac{1}{2}\right) \leq 0\right) \\ &= 5 \cdot \left[\binom{5}{0} \cdot 2^{-5} + \binom{5}{1} \cdot 2^{-5}\right] + 0 \\ &= \frac{30}{32} < 1. \end{aligned}$$

Najbolja strategija kojom Paul može igrati je da podijeli prostor pretraživanja na dva jednaka dijela (ukoliko prostor pretraživanja ima neparan broj elemenata, učinit će to što je bolje moguće, odnosno u jednom dijelu će biti jedan element više nego u drugom). Pretpostavimo da Paul postavlja pitanje „Je li $x \leq 3$?“i da Carole odgovara *Da*. Tada je novi vektor pozicije $P = (3, 2)$ i težina te pozicije je

$$\begin{aligned} w(P) &= \sum_{i=0}^{1} x_i \cdot \mathbb{P}\left(B\left(4, \frac{1}{2}\right) \leq 1 - i\right) \\ &= x_0 \cdot \mathbb{P}\left(B\left(4, \frac{1}{2}\right) \leq 1\right) + x_1 \cdot \mathbb{P}\left(B\left(4, \frac{1}{2}\right) \leq 0\right) \\ &= 3 \cdot \left[\binom{4}{0} \cdot 2^{-4} + \binom{4}{1} \cdot 2^{-4}\right] + 2 \cdot \binom{4}{0} \cdot 2^{-4} \\ &= \frac{17}{16} > 1. \end{aligned}$$

Prema teoremu 3.3.1 odavde slijedi da Carole mora pobijediti u ovoj igri.

Lako je provjeriti da niti jedan od preostalih Paulovih poteza ne vodi do njegove pobjede. Problem je u tome što Paul nema dobar prvi potez. Na početku igre Paul je bio u poziciji čija je težina manja od jedan, ali nije mogao pronaći takav potez da su $w(P +^* v) \leq 1$ i $w(P -^* v) \leq 1$.

Pokazali smo da obrat teorema 3.3.1 općenito ne vrijedi i kako bismo pronašli strategiju za Paula potrebne su nam neke dodatne pretpostavke. U ovoj igri možemo primjeniti preciznu lemu o razdvajanju iz igre sigurnosti, ali uz neke dodatne pretpostavke. Potrebna nam je lema koja omogućava Paulu da odabere vektor savršene podjele u svakom od q krugova igre. Vektor savršene podjele je vektor poteza v takav da vrijedi $w(P +^* v) = w(P -^* v)$.

Lema 3.3.4. *Neka je $P = (b_0, \ldots, b_k)$ vektor pozicije s preostalih $r + 1$ poteza i težinom $w(P) = 1$. Pretpostavimo da je $b_k \geq \binom{r}{k}$ i da je $r \geq 2k$. Tada postoji vektor savršene podjele $v = (c_0, \ldots, c_k)$ takav da je*

$$c_i = \left\lceil \frac{b_i}{2} \right\rceil \quad ili \quad c_i = \left\lfloor \frac{b_i}{2} \right\rfloor \quad za\ 0 \leq i < k\,,$$

i

$$\left| c_k - \frac{b_k}{2} \right| < \frac{1}{2}\binom{r}{k}.$$

Dokaz. Definirat ćemo $\Delta = w(P -^* v) - w(P +^* v)$. Razmotrimo učinak na Δ, odnosno stavljanje jednog žetona koji se nalazi na mjestu i u Paulov skup L. Ako Carole odabere prvu opciju, žeton će se pomaknuti na mjesto $i + 1$ i imat će težinu $\mathbb{P}(B_r \leq k - i - 1)$, a

ako Carole odabere drugu opciju, žeton će ostati na mjestu i i imat će težinu $\mathbb{P}(B_r \leq k - i)$. Prema tome,

$$\begin{aligned}\Delta &= w(P -^* v) - w(P +^* v)\\ &= \mathbb{P}(B_r \leq k - i) - \mathbb{P}(B_r \leq k - i - 1)\\ &= \mathbb{P}(B_r = k - i)\\ &= \binom{r}{k-i} \cdot 2^{-r}.\end{aligned}$$

Ukoliko Paul nije stavio taj žeton u skup L, učinak na Δ je obrnut i Δ je umanjena za isti iznos. Kada je broj žetona b_i koji se nalaze na mjestu i paran, stavljanje $c_i = \frac{b_i}{2}$ žetona u skup L nema nikakav učinak na Δ. Za ona mjesta $0 \leq i < k$ na kojima je broj žetona b_i neparan, Paul naizmjenično stavlja i ne stavlja „neparan"žeton u skup L, a preostale žetone razdvaja na pola. Tada je učinak na Δ niz alternirajućih izraza. Budući da je $r \geq 2k$, vrijednosti $\binom{r}{k-i}$ se smanjuju za $0 \leq i < k$ pa se ovi izrazi smanjuju po apsolutnoj vrijednosti. Žetone koji se nalaze na mjestu k nazovimo k - žetoni. Nakon smještanja svih preostalih žetona (osim k - žetona) apsolutna vrijednost od Δ je najviše $\binom{r}{k} \cdot 2^{-r}$ i ima oblik $a \cdot 2^{-r}$, gdje je a neki cijeli broj. Paul sada uzima prvih a k - žetona (prema pretpostavci je $a \leq \binom{r}{k} \leq b_k$) i stavlja ih ili sve ili niti jednog u skup L kako bi dobio $\Delta = 0$. Ako je preostali broj k - žetona paran, Paul ih podijeli na dva jednaka dijela i time je podjela završena. Tvrdimo da je ovo jedini mogući slučaj. Kada bi broj preostalih k - žetona bio neparan, Paul bi ih mogao podijeliti sve osim jednog na dva jednaka dijela i time bi dobio da je $\Delta = 2^{-r}$ (ili $\Delta = -2^{-r}$ ako taj jedan k - žeton nije stavio u L). Budući da je

$$\frac{1}{2}\left(w(P -^* v) + w(P +^* v)\right) = w(P) = 1,$$

$$\Delta = w(P -^* v) - w(P +^* v)$$

slijedi

$$\begin{aligned}\frac{1}{2}\left(w(P -^* v) + w(P -^* v) - \Delta\right) &= 1\\ 2 \cdot w(P -^* v) \pm 2^{-r} &= 2\\ w(P -^* v) &= 1 \pm \frac{2^{-r}}{2}.\end{aligned}$$

Budući da su sve težine s preostalih r poteza višekratnici broja 2^{-r}, dolazimo do kontradikcije. □

Premda smo pokazali da obrat teorema 3.3.1 ne vrijedi, ipak je moguće dobiti svojevrsni parcijalni obrat, tj. strategiju za Paula ukoliko on postupa kao u lemi 3.3.4, a parametri

igre su odabrani njemu u prilog. Kvantitativni dovoljni uvjet na parametre uz koje Paul ima strategiju za pobjedu je sadržan u idućem teoremu. Njegov dokaz je tehnički nešto složeniji, ali kombinatorno nije posebno zanimljiv pa zainteresiranog čitatelja upućujemo na članak [4].

Teorem 3.3.5. *Za svako k postoji $q_0 = q_0(k)$ takav da za $q > q_0$ (q je broj krugova u igri lažova) vrijedi sljedeća tvrdnja: ako je $P = (x_0, \ldots, x_k)$ početni vektor pozicije s težinom jedan i vrijedi*

$$x_k \geq 2\binom{q-1}{k} + 2^2\binom{q-2}{k} + \cdots + 2^k\binom{q-k}{k},$$

onda Paul pobjeđuje u igri lažova.

Napomenimo da do danas nisu nađeni uvjeti na parametre igre koji su istovremeno nužni i dovoljni kako bi Paul ili Carole imali pobjedničku strategiju; štoviše, taj problem se smatra iznimno težak.

Poglavlje 4

Neke varijante i eksplicitne strategije

4.1 Generalizacija igre sigurnosti

Poopćit ćemo cilj igre sigurnosti. Neka je vrijednost igre za Paula jednaka broju zaposlenika koji su dobili stalno zaposlenje. Paul tada pokušava maksimizirati broj tih zaposlenika, a Carole pokušava minimizirati taj broj. Kao i u igri uravnoteženih vektora, definirajmo $[(x_1, \ldots, x_k), \alpha]$ - igru sigurnosti kao igru u kojoj pobjeđuje Paul ako je najmanje α zaposlenika dobilo stalno zaposlenje.

Teorem 4.1.1. *Neka je $w = \sum_i x_i 2^{-i}$ težina početne pozicije u generaliziranoj igri sigurnosti. Tada je vrijednost igre V (za Paula) jednaka $\lfloor w \rfloor$.*

Dokaz. Neka je a cijeli broj takav da je $w < a$ i razmotrimo $[(x_1, \ldots, x_k), a]$ - igru sigurnosti. Analogno kao i u odjeljku 3.1, kada Carole igra slučajno, kojom god strategijom Paul igra dobivamo da je očekivani broj zaposlenika koji će dobiti stalno zaposlenje jednak w. Odavde slijedi da je vjerojatnost da Paul pobijedi manja od 1 pa Carole mora imati pobjedničku strategiju. Prema tome $V < a$.

Neka je a cijeli broj takav da je $w \geq a$ i razmotrimo ponovno $[(x_1, \ldots, x_k), a]$ - igru sigurnosti. Jednostavna generalizacija korolara 3.1.3 leme podjele daje: ako su $x_1 \geq \cdots \geq x_l$ negativne potencije broja dva sa sumom najmanje a onda postoji particija od $\{x_i : i = 1, 2, \ldots, l\}$ u dvije grupe takva da je suma elemenata svake grupe najmanje $\frac{a}{2}$. Primjenom ove generalizacije Paul može uzastopno osigurati da je težina najmanje a. Na kraju igre, težina je broj zaposlenika koji su dobili stalno zaposlenje. Prema tome, $V \geq a$.

Iz dobivene dvije nejednakosti slijedi $V = \lfloor w \rfloor$. □

Sada ćemo definirati obratnu igru sigurnosti. Pravila su jednaka i vrijednost igre je opet broj zaposlenika koji su dobili stalno zaposlenje, ali ovaj put je to vrijednost igre (isplata) za Carole. Paul tada pokušava minimizirati broj zaposlenika koji će dobiti stalno

zaposlenje, dok Carole pokušava maksimizirati taj broj. Označimo s V^o vrijednost ove igre. Definirajmo $[(x_1, \ldots, x_k), \alpha]$ - igru sigurnosti kao igru u kojoj pobjeđuje Carole ako je najmanje α zaposlenika dobilo stalno zaposlenje.

Teorem 4.1.2. *Neka je $w = \sum_i x_i 2^{-i}$ težina početne pozicije u generaliziranoj obratnoj igri sigurnosti. Tada je vrijednost igre V^o (za Carole) jednaka $\lceil w \rceil$.*

Dokaz. Neka je a cijeli broj takav da je $w \geq a$ i razmotrimo $[(x_1, \ldots, x_k), a]$ - igru sigurnosti. Kada Carole igra slučajno, kojom god strategijom Paul igra dobivamo (na isti način kao u odjeljku 3.1) da je očekivani broj zaposlenika koji će dobiti stalno zaposlenje jednak w. Odavde slijedi da je vjerojatnost da Paul pobijedi manja od 1 pa Carole mora imati pobjedničku strategiju. Prema tome $V^o \geq a$.

Neka je $a = \lceil w \rceil$ i razmotrimo ponovno $[(x_1, \ldots, x_k), a]$ - igru sigurnosti. Slično kao i u korolaru 3.1.3 vrijedi sljedeća tvrdnja: ako su $x_1 \geq \cdots \geq x_l$ negativne potencije broja dva sa sumom najviše a onda postoji particija od $\{x_i : i = 1, 2, \ldots, l\}$ u dvije grupe takva da je suma elemenata svake grupe najviše $\frac{a}{2}$. Uz neznatne izmjene dokaza korolara 3.1.3 dobije se dokaz ove tvrdnje. Potrebno je dodati brojeve $x_{l+1}, \ldots$ dok se ne dobije da je suma jednaka točno a i tada tvrdnja slijedi primjenom leme podjele 3.1.2. Primjenom ove promijenjene leme Paul može uzastopno osigurati da je težina najviše a. Na kraju igre, težina je broj zaposlenika koji su dobili stalno zaposlenje. Prema tome, $V^o \leq a$, odnosno $V^o = \lceil w \rceil$. □

4.2 Strategije za igru lažova

Ovaj odjeljak služi prvenstveno kao ilustrativna specijalizacija općenitih rezultata i principa iz prethodnog poglavlja na sasvim konkretnim primjerima, kod kojih bi se strategija mogla proniknuti i sasvim primitivnim heurističkim rezoniranjem i isprobavanjem. Mi ćemo opisati strategiju za igru „20 pitanja“i tri strategije za igru lažova s parametrima $k = 1$ i $n = 10^6$. Više detalja o tim strategijama, kao i općenitu strategiju za igru lažova s parametrima $k = 1$ i $n = 2^l$ (gdje je l neki prirodni broj), može se pronaći u [5].

4.2.1 Strategija za igru „20 pitanja“

Igra „20 pitanja“je zapravo igra lažova s parametrima $k = 0$ i $n = 10^6$. Postoje dvije strategije kojima Paul može igrati kako bi utvrdio o kojem se cijelom broju x radi. Prva strategija uključuje podjelu prostora pretraživanja (skupa $\{1, \ldots, n\}$) asimetrično, a druga strategija uključuje simetričnu podjelu tog prostora. Paul želi koristiti strategiju koja smanjuje broj potrebnih pitanja da bi pronašao broj x.

Promotrimo prvo asimetričnu podjelu prostora pretraživanja. Paul podijeli, na primjer, taj prostor na dva skupa, $A_1 = \{1, \ldots, 250\,000\}$ i $A_2 = \{250\,001, \ldots, 10^6\}$ i postavi pitanje

obzirom na manji od ta dva skupa, tj. „Je li $x \in A_1$?“. Očito, ukoliko Carole odgovori *Da*, Paul u tom slučaju mora postaviti manje pitanja kako bi utvrdio broj x nego u slučaju da je Carole odgovorila *Ne*.

Promotrimo sada simetričnu podjelu prostora pretraživanja. Paul podijeli taj prostor na dva skupa $A_1 = \{1, \ldots, 500\,000\}$ i $A_2 = \{500\,001, \ldots, 10^6\}$ i postavi pitanje obzirom na jedan od ta dva skupa, npr. „Je li $x \in A_1$?“. Bez obzira na odgovor koji da Carole, Paul mora odrediti broj x iz skupova jednake veličine pa je jednak i broj pitanja potrebnih za utvrđivanje broja x iz jednog ili drugog skupa.

Usporedimo ove dvije strategije nakon što je Paul pitao prvo pitanje. Očito je da ukoliko on koristi asimetričnu strategiju i ako se broj x nalazi u manjem skupu, onda će biti potrebno manje pitanja kako bi utvrdio broj x nego kad bi koristio simetričnu strategiju. No, ako koristi asimetričnu strategiju i ako se x nalazi u većem skupu, onda će biti potrebno više pitanja kako bi utvrdio x nego kad bi koristio simetričnu strategiju. Budući da Paul igra tako da uvijek minimizira broj pitanja koja su potrebna kako bi utvrdio broj x, usvojit će simetričnu strategiju. Izračunajmo koliko je pitanja Paulu potrebno kako bi pogodio broj x u prostoru veličine 10^6. Paul postavlja pitanja oblika „Je li $x \in A_i$?“, a mogući odgovori su ili *Da* ili *Ne* pa slijedi

$$2^q = 1\,000\,000 \Leftrightarrow q = 19.93.$$

Prema tome, ako Paul koristi strategiju simetrične podjele prostora pretraživanja bit će mu potrebno najviše 20 pitanja kako bi utvrdio broj x. Simetrična strategija za rješavanje igre „20 pitanja“opisana je na sljedeći način: prostor pretraživanja $\{1, \ldots, 10^6\}$ Paul treba podijeliti u dva skupa jednake veličine, gdje je $A_1 = \{1, \ldots, 500\,000\}$ i $A_2 = \{500\,001, \ldots, 10^6\}$. Prvo pitanje koje Paul postavlja je oblika „Je li $x \in A_1$?“. Ako Carole odgovori *Da*, Paul uzima skup A_1, podijeli ga u dva skupa jednake veličine i postavlja pitanje oblika „Je li $x \in A_i$?“, gdje A_i predstavlja jedan od ova dva manja skupa sadržana u A_1. Ako Carole pak odgovori *Ne*, Paul uzima skup A_2, podijeli ga u dva skupa jednake veličine i slično postavlja sljedeće pitanje oblika „Je li $x \in A_i'$?“, gdje A_i' predstavlja jedan od ova dva manja skupa sadržana u A_2. Igra se nastavlja na ovaj način, tako da Paul u svakom krugu podijeli trenutni prostor pretraživanja na dva nova skupa čije su veličine jednake ako je to moguće, vodeći obzira o tome da broj elemenata u svakom skupu bude cijeli broj. Ako je broj elemenata skupa pretraživanja u nekom krugu igre neparan, onda Paul stavi jedan element više u jedan od skupova. Nakon 20 postavljenih pitanja Paul će suziti originalni prostor pretraživanja na samo jedan cijeli broj, upravo x. Stoga, Paul pobjeđuje u ovoj igri i igra završava jer je broj x pronađen.

4.2.2 Strategije za igru lažova s jednom laži

Iako je igra lažova slična prethodnoj igri „20 pitanja“, Paul će morati promijeniti strategiju. Promatrat ćemo igru lažova u kojoj je dopuštena najviše jedna laž i koja se odvija na

prostoru pretraživanja $\{1, \ldots, 10^6\}$, dakle zadani su parametri $k = 1$ i $n = 10^6$. Jasno je da Paulu neće biti dovoljno 20 pitanja kako bi pronašao cijeli broj x koji je zamislila Carole. Opisat ćemo tri strategije kojima Paul može igrati kako bi pogodio broj x. U usporedbi s ostale dvije, u prvoj strategiji će biti potreban relativno veći broj pitanja kako bi se utvrdio x. Na kraju, reći ćemo koliko je najmanje pitanja potrebno za otkrivanje broja x.

Prva strategija - 41 pitanje

Kao i u originalnoj igri „20 pitanja“Carole zamisli broj x iz prostora pretraživanja (skupa $\{1, \ldots, 10^6\}$). Paul sada mora koristiti neku strategiju kojom će identificirati broj x, ali mora imati na umu da Carole smije lagati i to najviše jednom. Kao i prije, Paul simetrično podijeli prostor pretraživanja na dva skupa i postavlja pitanje oblika „Je li $x \in A_i$?“, gdje je A_i particija prostora pretraživanja. Kako bi bio siguran da Carole nije lagala, Paul može svako pitanje postaviti dva puta. Ako su odgovori koje je Paul dobio konzistentni, odnosno na isto pitanje je dobio oba odgovora *Da* ili oba odgovora *Ne*, onda Paul zna da je Carole rekla istinu i da može lagati još jednom. Zatim, Paul taj trenutni prostor pretraživanja ponovno podijeli na dva manja skupa jednake veličine i nastavi postavljati pitanja oblika „Je li $x \in A_i$?“. Ako Paul pak dobije dva nekonzistentna odgovora, odnosno jedan odgovor *Da* i jedan odgovor *Ne*, znači da je Carole lagala pa Paul mora postaviti isto pitanje i treći put i uzeti taj zadnji (treći) odgovor kao točan. Nakon toga, Paul ponovno podijeli taj trenutni prostor pretraživanja u dva manja skupa jednake veličine i nastavlja postavljati pitanja oblika „Je li $x \in A_i$?“. No, od sada nadalje svako pitanje mora postaviti samo jednom jer Carole više nije dopušteno lagati. Za ovu strategiju potrebno je najviše 41 pitanje jer se može dogoditi da Carole laže tek u posljednjem pitanju. Primjetimo da je broj od 41-og pitanja poprilično velik u usporedbi s brojem pitanja potrebnih da bi se utvrdio x u igri „20 pitanja“.

Druga strategija - 26 pitanja

Kao i u prvoj strategiji, Paul mora pogoditi broj x uzimajući u obzir da Carole može lagati najviše jednom. Paul traži Carole da cijeli broj x zapiše u binarnom obliku. Budući da znamo da je $10^6 < 2^{20}$ $(= 1\,048\,576)$ znamo da će taj broj imati najviše 20 znamenki. U prvom krugu igre, Paul postavlja pitanje „Je li prva znamenka broja x u binarnom zapisu jednaka 1?“. Carole mu odgovara s *Da* ili *Ne*. U sljedećem krugu igre, Paul postavlja pitanje „Je li druga znamenka broja x u binarnom zapisu jednaka 1?“i zatim nastavlja postavljati pitanja ovog oblika sve dok ne dobije dvadeseteroznamenkasti broj koji se sastoji od nula i jedinica. Znamo da je Carole do ovog trenutka mogla lagati najviše jednom pa najviše jedna znamenka ovog dvadeseteroznamenkastog broja može biti pogrešna, odnosno postoji 21 cijeli broj koji bi x mogao biti. Moguće je utvrditi broj x koristeći binarno pretraživanje na tom dvadeseteroznamenkastom broju, tj. Paul mora podijeliti znamenke tog

broja u dva skupa i onda postavljati pitanja u odnosu na svaki skup. Paul posebno razmatra znamenke koje se nalaze na pozicijama od 1 do 10, a posebno znamenke na pozicijama od 11 do 20. On prebroji broj jedinica na prvih 10 znamenki, recimo da ih ima m, i zatim postavlja pitanje „Ima li m jedinica u prvih 10 znamenki ovog broja?“. Razmotrit ćemo dva odvojena slučaja ovisno o tome je li Carole odgovorila s *Da* ili *Ne*.

- **Prvi slučaj:** Promotrimo prvo slučaj u kojem Carole odgovara *Da*. Tada znamo da ona nije lagala za tih prvih 10 znamenki. Kada bi Carole lagala u tom trenutku to bi značilo da tada nema m jedinica u prvih 10 znamenki tog broja. No, to bi također značilo da je Carole lagala i za neku od prvih 10 znamenki što bi značilo da je Carole dvaput lagala, a to nije moguće. Prema tome, Paul može zapisati ovih 10 znamenki i smatrati ih točnima pa još mora razmotriti zadnjih 10 znamenki. Slično kao i prije, on mora prebrojiti broj jedinica koje se pojavljuju u tom deseteroznamenkastom broju i postaviti pitanje o broju jedinica koje se pojavljuju u tom broju. Ako Carole odgovori *Da* na to pitanje, onda je i ovih deset znamenki točno pa možemo zaključiti da Carole nije lagala. Ako pak Carole odgovori *Ne* preostala analiza ovog slučaja slična je drugom slučaju.

- **Drugi slučaj:** Promotrimo sada slučaj u kojem Carole odgovara *Ne* na početno pitanje (pitanje koje se odnosi na prvih deset znamenki dvadeseteroznamenkastog broja). Ne znamo je li taj odgovor laž, ali znamo da je Carole do tog trenutka iskoristila jedinu laž koju je mogla koristiti. Ako je Carole iskreno odgovorila na to pitanje to znači da je lagala prije, za neku od prvih deset znamenki tog broja. Alternativno, ako je Carole lagala prilikom odgovaranja baš na ovo pitanje, onda su sve znamenke ovog deseteroznamenkastog broja točne i znamo da Carole više nema pravo lagati. U obje situacije znamo da Carole na sva sljedeća pitanja mora odgovoriti iskreno. Prema tome, ako Carole odgovori *Ne* na to pitanje, Paul mora podijeliti taj deseteroznamenkasti broj na dva peteroznamenkasta broja. Za svaki od tih peteroznamenkastih brojeva Paul prebroji broj jedinica koje se nalaze u tom broju i zatim postavlja pitanje o broju jedinica u tim brojevima, kao i prije, imajući na umu da sada svaki odgovor koji dobije mora biti istinit budući da Carole više ne smije lagati. To znači da Paul mora nastaviti razdvajati brojeve u manje brojeve i postavljati pitanja o broju jedinica u svakom od tih brojeva sve dok ne pronađe znamenku za koju je Carole lagala. Kada razdvaja brojeve u manje brojeve (brojeve s manje znamenaka) pokušava ih uvijek razdvojiti tako da oba nova broja imaju jednak broj znamenaka. U slučaju kada broj koji mora razdvojiti na dva manja broja ima neparan broj znamenki, recimo n, onda će ih podijeliti tako da jedan manji broj sadrži $\frac{n+1}{2}$ znamenki, a drugi $\frac{n-1}{2}$ znamenki. U trenutku kada Paul nađe znamenku o kojoj je Carole lagala ukoliko je ta znamenka 1 promijeni je u 0 i obratno i time je utvrdio broj x.

Koristeći ovu strategiju za pogađanje broja x potrebno je najviše 26 pitanja. Do toga će doći zbog pretpostavke da u svakom koraku prilikom dijeljenja originalnog binarnog broja u dva manja broja Carole odgovara *Ne* za veći od tih brojeva dobivenih razdvajanjem originalnog broja. Objasnimo to na ovom konkretnom primjeru. Paul najprije dijeli originalni dvadeseteroznamenkasti broj na dva broja duljine 10 (znamenki), a zatim deseteroznamenkasti broj dijeli na dva peteroznamenkasta broja. U sljedećem koraku peteroznamenkasti broj dijeli na dva broja, tako da jedan sadrži tri znamenke, a drugi sadrži dvije znamenke. Zatim uzima onaj broj koji ima veću duljinu, dakle troznamenkasti broj i njega dijeli na dva broja, jedan dvoznamenkasti i jedan jednoznamenkasti te ponovno uzima veći od ta dva broja i ponavlja postupak. Dakle, dvoznamenkasti broj podijeli na dva jednoznamenkasta broja. To rezultira time da Paul mora postaviti još 6 dodatnih pitanja uz onih 20 pitanja koje je već postavio. No, primjetimo da je 26 pitanja značajno manji broj nego 41 pitanje potrebno za otkrivanje broja x koristeći prvu strategiju.

Treća strategija - 25 pitanja

Ova strategija, u kojoj je potrebno najviše 25 pitanja kako bi se utvrdio broj x slična je prethodnoj strategiji. Nakon što Carole zamisli cijeli broj iz skupa $\{1, \ldots, 10^6\}$, Paul ju traži da zapiše taj broj u binarnom obliku. Paul zatim postavlja pitanja oblika „Je li vrijednost znamenke na prvom mjestu jednaka 1?“i tako dalje redom po svim znamenkama. Odgovori koje Carole daje formiraju dvadeseteroznamenkasti broj koji se sastoji od nula i jedinica. Do tog trenutka Paul je iskoristio 20 pitanja i preostalo mu je još 5 pitanja. U sljedećem koraku, Paul razdvoji dvadeseteroznamenkasti broj na dva broja. No, pitanje je koliko znamenaka treba imati svaki od ta dva broja. Iz druge strategije znamo da će Paulu biti potrebno 26 pitanja kako bi utvrdio broj x ako će brojeve razdvajati na dva broja jednakih veličina (jednakog broja znamenaka). Zato ćemo pretpostaviti da će Paul razdvojiti taj dvadeseteroznamenkasti broj na dva broja tako da jedan broj sadrži veći broj znamenaka od drugog broja. Sada će Paul postaviti pitanje o broju jedinica za veći od ta dva broja. Prema tome, iskoristio je još jedno pitanje i preostala su mu još 4 pitanja. Pretpostavimo da veći broj sadrži 14 znamenki, a manji 6 znamenki. U najgorem mogućem slučaju Paul će morati primjeniti binarno pretraživanje na broju od 14 znamenki. Tada će razdvojiti taj broj na dva sedmeroznamenkasta broja. Kao što smo objasnili u drugoj strategiji, znamo da je do tog trenutka Carole morala iskoristiti svoju jedinu laž pa svi odgovori od ovog trenutka nadalje moraju biti istiniti. Paul nastavlja postavljati pitanja o broju jedinica u brojevima i u najgorem slučaju morat će postaviti još 4 pitanja od trenutka kada je pitao za broj jedinica u tom četrnaestoznamenkastom broju. Prema tome, potrebno mu je samo 25 pitanja kako bi utvrdio broj x. Primijetimo da ukoliko je četrnaestoznamenkasti broj sadržavao točan broj jedinica, tada Paul mora postaviti najviše tri pitanja s obzirom na broj jedinica u drugom (šesteroznamenkastom) broju. U tom slučaju Paul će iskoristiti najviše 24 pitanja kako bi pronašao broj x. Prema tome, pronašli smo strategiju u kojoj je Paulu

potrebno najviše 25 pitanja kako bi utvrdio broj x u igri lažova s parametrima $k = 1$ i $n = 10^6$.

Minimalan broj pitanja

Nakon što smo vidjeli tri strategije, s različitim brojem potrebnih pitanja q, kojima Paul može igrati kako bi pogodio broj x iz skupa $\{1, \ldots, 10^6\}$ uz jednu dopuštenu laž ($k = 1$), možemo se zapitati koji je najmanji broj potrebnih pitanja q da bi Paul otkrio taj broj. Je li to zaista 25 kao u trećoj strategiji ili postoji manji broj? Istu stvar pitao se i poljski matematičar Stanislaw Ulam 1976. godine pa je taj problem poznat pod nazivom *Ulamov problem*. Svoja parcijalna rješenja tog problema dali su 1980. godine američki kriptograf Rivest odnosno 1984. godine američki matematičar Spencer. Njihova rješenja davala su dvije mogućnosti, odnosno oni su pokazali da je potrebno najmanje 25 ili 26 pitanja. Konačno, 1986. godine poljski matematičar Pelc dokazao je u svom radu [2] da je odgovor $q = 25$. Prema tome, rješenje originalnog Ulamovog problema je sljedeće: najmanji broj q pitanja koje je potrebno postaviti kako bi se pogodio cijeli broj x između 1 i 1 000 000, ukoliko je dopušteno jednom lagati, je $q = 25$.

Bibliografija

[1] N. Alon, J. H. Spencer, *The Probabilistic Method*, John Wiley & Sons, Inc., USA, 2000.

[2] A. Pelc, *Solution of Ulam's problem on searching with a lie*, Journal of Combinatorial Theory, Series A, 44 (1987), 129-140.

[3] N. Sarapa, *Teorija vjerojatnosti*, Školska knjiga, Zagreb, 2002.

[4] J. H. Spencer, *Randomization, derandomization and antirandomization: three games*, Theoretical Computer Science 131 (1994), 415-429.

[5] R. Watkinson, *Liar Games and Coding Theory*, dostupno na `http://web.mat.bham.ac.uk/D.Osthus/liargame.pdf` , (prosinac 2014.).

[6] Wikipedia contributors, *Markov's inequality*, dostupno na `http://en.wikipedia.org/w/index.php?title=Markov%27s_inequality&oldid=619859384` , (prosinac 2014.).

Sažetak

U ovom radu je obrađena takozvana vjerojatnosna metoda, s naglaskom na njezine primjene u analizi deterministčkih igara. Obzirom da je sama metoda nekonstruktivna, izložen je i proces derandomizacije, koji producira učinkovite algoritme. U radu su opisane dvije najčešće korištene metode u procesu derandomizacije - metoda uvjetnih vjerojatnosti i metoda pesimističnih procjenitelja. Potom su na primjerima triju deterministčkih igara za dva igrača provedeni postupci randomizacije, derandomizacije i antirandomizacije, s ciljem pronalaska savršenih pobjedničkih strategija za igrače, uz odgovarajuće vrijednosti danih parametara. Na kraju rada izloženi su konkretni primjeri strategija za igru lažova u svrhu približavanja i ilustracije prethodno dobivenih općenitih rezultata.

Summary

This thesis deals with the so-called probabilistic method, with emphasis on applications to the analysis of deterministic games. Since the method itself is nonconstructive, the process of derandomization which produces efficient algorithms is also presented. This thesis describes the two most commonly used methods in the process of derandomization - the method of conditional probabilities and the method of pessimistic estimators. Furthermore, the procedures of randomization, derandomization, and antirandomization were carried out on the examples of three deterministic games for two players, aimed at finding the perfect winning strategies for the players, depending on the corresponding values of the given parameters. At the end of the thesis concrete examples of strategies for the Liar game are given in order to clarify and illustrate previously obtained general results.

Životopis

Rođena sam 22. svibnja 1990. godine u Zagrebu. Nakon završetka Osnovne škole Vukovina, 2005. godine upisala sam prirodoslovno-matematički smjer Gimnazije Velika Gorica u istoimenom gradu. Završetkom srednje škole, 2009. godine upisala sam Preddiplomski sveučilišni studij Matematika na Prirodoslovno - matematičkom fakultetu u Zagrebu, a zatim, stjecanjem prvostupničke diplome 2012. godine, upisala sam Diplomski sveučilišni studij Matematička statistika na istom fakultetu.