Primjena vjerojatnosne metode i Markovljevih lanaca u analizi algoritama

Kroflin, Matej

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Matej Kroflin

Primjena vjerojatnosne metode i Markovljevih lanaca u analizi algoritama

Završni rad

Osijek, 2018.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Matej Kroflin

Primjena vjerojatnosne metode i Markovljevih lanaca u analizi algoritama

Završni rad

Mentor: izv. prof. dr. sc. Domagoj Matijević

Osijek, 2018.

Sažetak

U ovom završnom radu bavit ćemo se vjerojatnosnom metodom i Markovljevim lancima. Pokazat ćemo kako se konstruiraju algoritmi korištenjem argumenata iz vjerojatnosti te analizirat randomizirane algoritame pomoću Markovljevih lanaca.

Ključne riječi

vjerojatnost, randomizirani algoritmi, Markovljevi lanci, maze problem, vjerojatnosna metoda

Application of the probability method and Markov chains in analysis of randomized algorithms

Summary

In this paper we will study the probability method and Markov chains. We will show how to construct algorithms using argument from probability theory and analyze randomized algorithms using Markov chains.

Keywords

probability, randomized algorithms, Markov chains, maze problem, probability method

Sadržaj

Uvod

Znanost je u posljednjem stoljeću pokazala da je slučajnost važna komponenta u modeliranju i analizi. U fizici, Newtonovi zakoni dali su naslutiti da je svemir determinističko mjesto; za dovoljno veliki kalkulator i prikladne početne uvjete, pojedinac bio mogao izračunati lokaciju svakog planeta godinama unaprijed. Razvoj kvantne teorije sugerira drugačiji pogled; svemir se ponaša u skladu nekih pravila, ali u pozadini ova pravila su slučajna. „Bog se ne kocka" je poznat Einsteinov anegdotalni prigovor na modernu kvantnu mehaniku. Štoviše, prevladavajuća teorija danas u fizici je bazirana na slučajnim i statističkim zakonima, i slučajnost ima važnu ulogu u svakom području znanosti. U ovom radu pokazat ćemo kako se koristi vjerojatnost za egzistenciju te konstrukciju i analizu algoritama pomoću vjerojatnosnih argumenata. Jedan od najvećih problema u konstrukciji i analizi algoritama jest klasifikacija problema. To jest, da li je problem P ili NP[1]. Randomizirani algoritmi se najviše koriste kako bi se aproksimirao NP - težak problem.

U prvim poglavljima ćemo predstaviti glavne alate koje ćemo koristiti prilikom analize algoritama. Neki od tih su argument očekivanja i Markovljevi lanci. Potom ćemo iskazati glavne teoreme u Markovljevim lancima i slučajnim šetnjama, a neke i dokazati. Na kraju rada pokazat ćemo jedan NP-težak problem te ga analizirati.

[1] $P \neq NP$ je još uvijek otvoreno pitanje

1 Vjerojatnosna metoda

Vjerojatnosna metoda je način dokazivanja egzistencije objekata. Pretpostavimo da želimo dokazati postojanje nekog *dobrog* objekta. Na skupu svih objekata definiramo vjerojatnosnu mjeru pa potom pokažemo da skup svih dobrih objekata ima pozitivnu mjeru, to jest, da je pozitivna vjerojatnost da će slučajno odabrati objekt biti dobar. Kao posljedicu dobivamo da postoji barem jedan dobar objekt, ali ne mora odmah biti jasno kako ih doista naći.

Pokazat ćemo nekoliko klasičnih primjena metode. Odlična i vrlo opsežna knjiga o vjerojatnosnoj metodi je [1].

U teoriji grafova bojenje grafova se odnosi na specifičan slučaj označavanja grafa odnosno dodjeljivanja oznaka (boja) elementima grafa uz neka ograničenja. U neusmjerenom grafu $G = (V, E)$ definiramo k-kliku kao skup od k vrhova takav da za svaka dva vrha $u, v \in V$ vrijedi da je $(u, v) \in E$.

Teorem 1. *Ako* $\binom{n}{k} 2^{-\binom{k}{2}+1} < 1$*, tada postoji bojenje bridova od* K_n *s dvije boje tako da nema monokromatski* K_k *podgraf.*

Dokaz. Definiramo prostor elementarnih događaja kao skup svih mogućih bojenja grafa K_n s dvije boje. Postoje $2^{\binom{n}{2}}$ takva bojenja te tada je vjerojatnost da je jedno takvo bojenje odabrano uniformno jednaka $2^{-\binom{n}{2}}$. Fiksiramo bilo koji poredak svih $\binom{n}{k}$ k-klika od K_n i za svaki $i = 1, \ldots, \binom{n}{k}$ neka je A_i događaj da je klika i monokromatska. Kada je prvi brid klika i obojen, preostala $\binom{k}{2} - 1$ brida moraju biti iste boje. Slijedi da je tada

$$\mathrm{P}(A_i) = 2^{-\binom{k}{2}+1}.$$

Iz σ - subaditivnosti vjerojatnosti slijedi

$$\mathrm{P}\Big(\bigcup_{i=1}^{\binom{n}{k}} A_i\Big) \leq \sum_{i=1}^{\binom{n}{k}} \mathrm{P}(A_i) = \binom{n}{k} 2^{-\binom{k}{2}+1} < 1.$$

gdje posljednja nejednakost slijedi iz pretpostavke. Nadalje,

$$\mathrm{P}\Big(\bigcap_{i=1}^{\binom{n}{k}} A_i^{\mathrm{c}}\Big) = 1 - \mathrm{P}\Big(\bigcup_{i=1}^{\binom{n}{k}} A_i\Big) > 0$$

Lijeva strana nejednakosti nam upravo govori da je vjerojatnost da odabir bojenja u kojemu nema monokromatskih k-klika veća od 0, prema tome postoji bojenje bez monokromatskih k-klika. □

Primjer 1. *Promotrimo može li se graf* K_{1000} *obojiti u 2 boje tako da ne postoji monokromatski podgraf* K_{20}*. Uočimo da ukoliko* $n \leq 2^{k/2}$ *i* $k \geq 3$*,*

$$\binom{n}{k} 2^{-\binom{k}{2}+1} \leq \frac{n^k}{k!} 2^{-(k(k-1)/2)+1} \leq \frac{2^{k/2+1}}{k!} < 1$$

U našem slučaju, $n = 1000 \leq 2^{10} = 2^{k/2}$ *te su uvjeti iz Teorema 1 ispunjeni pa znamo da postoji 2-bojenje bridova od* K_{1000} *takvo da ne postoji monokromatski podgraf* K_{20}*.*

Kako bismo nastavili s razmatranjima pokažimo prvo jednu korisnu lemu

Lema 1. *Neka je* $(\Omega, \mathcal{F}, \mathrm{P})$ *vjerojatnosni prostor i* X *diskretna slučajna varijabla definirana na tom prostoru t.d. je* $\mathbf{E}[X] = \mu < \infty$. *Tada* $\mathrm{P}(X \geq \mu) > 0$ *i* $\mathrm{P}(X \leq \mu) > 0$.

Dokaz. Prema definiciji

$$\mu = \sum_x x \ \mathrm{P}(X = x),$$

gdje suma ide po svim $x \in \mathcal{R}(X)$. Ako $\mathrm{P}(X \geq \mu) = 0$, tada

$$\mu = \sum_x x \ \mathrm{P}(X = x) = \sum_{x<\mu} x \ \mathrm{P}(X = x) < \sum_{x<\mu} \mu \ \mathrm{P}(X = x) = \mu,$$

što je kontradikcija. Analogno, ako $\mathrm{P}(X \leq \mu) = 0$, tada

$$\mu = \sum_x x \ \mathrm{P}(X = x) = \sum_{x>\mu} x \ \mathrm{P}(X = x) > \sum_{x>\mu} \mu \ \mathrm{P}(X = x) = \mu.$$

□

Prema tome, postoji događaj za koju je vrijednost slučajne varijable X barem μ te postoji događaj za koju vrijednost slučajne varijable nije veća od μ. Ubuduće ćemo se pozivati na ovu lemu kao *argument očekivanja.*

Promotrimo sada problem pronalaska maksimalnog reza u neusmjerenom grafu. $G = (V, E)$. Rez, u oznaci (A, B), je particija vrhova grafa u dva disjunktna skupa A i B te vrijednost reza je suma težina svih bridova koji spajaju vrh iz jednog skupa s vrhom iz drugog skupa. Razmotrit ćemo samo slučaj kada je težina svih bridova jednaka 1. Drugim riječima, tražimo particiju od V na skupove A, B koji maksimiziraju

$$|\{(u, v) \mid (u, v) \in E \cap (A \times B)\}|. \tag{1}$$

Problem pronalaska maksimalnog reza je NP - težak problem. Koristeći vjerojatnosnu metodu, pokazat ćemo da je vrijednost maksimalnog reza barem $1/2$ od ukupnog broja bridova u grafu.

Teorem 2. *Neka je* (V, E) *neusmjereni graf t.d.* $|V| = n$ *i* $|E| = m$. *Tada postoji particija od* V *na disjunktne skupove* A *i* B *t.d. barem* $m/2$ *bridova povezuje vrh iz* A *s vrhom u* B. *To jest, postoji rez čija je vrijednost barem* $m/2$.

Dokaz. Konstruiramo A i B tako da slučajno i nezavisno pridružujemo svaki vrh jednom od dva skupa. Neka su $e_1,\ e_2,\ \ldots,\ e_m$ bridovi u G. Za $i = 1, \ldots, m$, definiramo diskretne slučajne varijable

$$X_i = \begin{cases} 1, & \text{ako brid } e_i \text{ povezuje } A \text{ i } B \\ 0, & \text{inače} \end{cases}$$

Vjerojatnost da brid e_i povezuje vrh iz A s vrhom iz B je jednaka $1/2$ te prema tome

$$\mathbf{E}[X_i] = \frac{1}{2}.$$

Nadalje, neka je $C(A, B)$ slučajna varijabla koja modelira vrijednost reza koji pripada skupovima A i B. Tada

$$\mathbf{E}[C(A,B)] = \mathbf{E}\Big[\sum_{i=1}^{m} X_i\Big] = \sum_{i=1}^{m} \mathbf{E}[X_i] = \frac{m}{2}$$

Jer je očekivanje od $C(A, B)$ jednako $m/2$, prema argumentu očekivanja slijedi da postoji rez čija je vrijednost barem $m/2$. □

Postavlja se pitanje, može li se ovakva metoda koristiti za konstruiranje algoritama?

2 Randomizirani algoritmi

Razmotrit ćemo dvije najpoznatije vrste randomiziranih algoritama, Monte Carlo i Las Vegas algoritmi. Kako bismo nastavili dalje prvo je potrebno definirati randomizirani algoritam.

Definicija 1. *Za algoritam kažemo da je* ***randomiziran*** *ukoliko donosi slučajne (ili pseudoslučajne) odluke.*

Nadalje, slijede definicije dviju vrsta randomiziranih algoritama.

Definicija 2. *Randomizirani algoritam naziva se* ***Las Vegas*** *algoritam ukoliko uvijek vraća točan rezultat, ali vrijeme izvršavanja je očekivano polinomno, to jest, za skup podataka veličine n, postoji polinom p t.d. je prosječno vrijeme izvršavanja manje od $p(n)$.*

Vrijeme izvršavanja Las Vegas algoritama je uvijek konačno.

Definicija 3. *Randomizirani algoritam naziva se* ***Monte Carlo*** *algoritam ukoliko vraća točan ili netočan rezultat, ali vrijeme izvršavanja ne ovisi o slučajnosti.*

Iako se na prvu čini besmisleno koristiti Monte Carlo algoritme za rješavanje problema s obzirom na neizvjesnost rezultata, u većini slučajeva vjerojatnost vraćanja netočnog rezultata je vrlo mala. Ponekad će biti potrebno ponoviti Monte Carlo algoritam kako bi se vjerojatnost netočnosti smanjila. Lako vidimo da se Monte Carlo algoritam može dobiti iz Las Vegas algoritma tako da zaustavimo s izvršavanjem te odaberemo neki od dosad izračunatih rezultata.

Najjednostavniji primjer randomiziranog algoritma je odabir točke u jediničnoj kružnici. Na slučajan način odabiremo brojeve $x \in (-1, 1)$, $y \in (-1, 1)$ te provjerimo vrijedi li nejednakost

$$x^2 + y^2 < 1. \tag{2}$$

Ukoliko stanemo ovdje, dobili smo Monte Carlo algoritam. Lako možemo izračunati vjerojatnost da je algoritam vratio točan rezultat. Jer je površina kvadrata iz kojeg biramo parametre jednaka 4, a površina kruga u kojemu se nalaze povoljne točke (točan rezultat) jednaka je π, slijedi da je vjerojatnost da je rezultat točan jednaka $\pi/4$. Ukoliko postupak ponavljamo sve dok ne vrijedi (2), dobivamo Las Vegas algoritam čije očekivano vrijeme izvršavanja iznosi $4/\pi$. Slična metoda se koristi kako bi se izračunala vrijednost broja π.

3 Konstrukcija i analiza algoritama

Iz dokaza za teorem 1 željeli bismo konstruirati randomizirani algoritam kojim bismo odredili bojenje bridova tako da graf K_n nema monokromatski K_k podgraf. Prvo, zahtjevamo da efikasno možemo odabrati bojenje grafa iz prostora elementarnih događaja. U ovom slučaju, odabiranje je jednostavno jer možemo svaki brid, nezavisno jedan od drugog, obojiti u jednu od dviju boja. Općenito, prilikom konstrukcije algoritma, ne mora nužno biti jednostavan način za odabiranje elementa iz prostora elementarnih događaja. Sada je potrebno odrediti koliki je očekivani broj odabiranja iz prostora elementarnih događaja prije negoli dobijemo traženo bojenje. Ako je vjerojatnost odabira traženog bojenja jednaka p i ako odabiremo nezavisno svaki puta, onda je broj odabira potrebnih, prije pronalaska traženog bojenja, geometrijska slučajna varijabla s očekivanjem $1/p$. Stoga je potrebno da $1/p$ bude polinomno s obzirom na veličinu podataka kako bi se algoritam izvršavao u očekivanom polinomnom vremenu.

Ako $p = 1-o(p)$, tada slučajno odabiranje daje Monte Carlo algoritam čija je vjerojatnost netočnog rezultata jednaka $o(1)$. U primjeru nakon teorema 1, traženo je postojanje bojenja potpunog grafa s 1000 vrhova tako da ne postoji monokromatski podgraf K_{20}. Znamo da je vjerojatnost da slučajno odabrano bojenje ima monokromatski podgraf K_{20} iznosi najviše

$$\frac{20^{20/2+1}}{20!} < 8.5 \cdot 10^{-16}.$$

Stoga smo dobili Monte Carlo algoritam s malom vjerojatnošću neuspjeha.

Ukoliko želimo Las Vegas algoritam, zahtjevamo proceduru u polinomnom vremenu koja će provjeriti da li je slučajno odabrano bojenje zadovoljavajuće; tada možemo slučajno birati bojenja dok ne dobijemo ono koje je zadovoljavajuće. Gornju među na očekivano vrijeme izvršavanja možemo dobiti tako da pomnožimo očekivani broj uzoraka s gornjom međom na vrijeme izvršavanja procedure kojom provjeravamo svaki uzorak. Jednostavno za svaki od $\binom{n}{k}$ k-klika, provjerimo da li je monokromatski. Ovaj pristup ima polinomno vrijeme izvršavanja ukoliko je k konstanta.

Kao i prethodno, željeli bismo argument korišten u dokazu teorema 2 pretvoriti u efektivni algoritam za pronalaženje reza čija je vrijednost barem $m/2$.

Lako je slučajno odabrati particiju vrhova kao što je opisano u zadatku. Argument očekivanja nam ne daje donju među na vjerojatnost da je vrijednost slučajno odabranog reza barem $m/2$. Neka je

$$p = \mathrm{P}\Big(C(A,B) \geq \frac{m}{2}\Big),$$

te uočimo da je $C(A,B) \leq m$. Tada,

$$\begin{aligned}\frac{m}{2} &= \mathbf{E}[C(A,B)] = \sum_{i\geq 1} i\ \mathrm{P}(C(A,B)=i) = \sum_{i\geq 1} \mathrm{P}(C(A,B)\geq i) = \\ &= \sum_{i\leq m/2-1} \mathrm{P}(C(A,B)\geq i) + \sum_{i\geq m/2} \mathrm{P}(C(A,B)\geq i) \\ &= \sum_{i\leq m/2-1} \mathrm{P}(i\leq C(A,B)\leq m/2-1) + \sum_{i\leq m/2-1} \mathrm{P}(C(A,B)\geq m/2) + \sum_{i\geq m/2} \mathrm{P}(C(A,B)\geq i) \\ &\leq (1-p)\Big(\frac{m}{2}-1\Big) + \frac{pm}{2} + \frac{pm}{2}\end{aligned}$$

što implicira da je

$$p \geq \frac{1}{m/2+1}.$$

Očekivani broj biranja reza prije odabiranja reza, čija je vrijednost barem $m/2$, je dakle $m/2+1$. Provjera da li je vrijednost reza barem $m/2$ može se izvršiti u polinomnom vremenu tako da samo prebrojimo sve bridove koji spajaju skupove A i B. Prema tome, odredili smo Las Vegas algoritam za pronalaženje takvog reza.

Poput traženja maksimalnog reza, zanimljivo je traženje minimalnog (netrivijalnog) reza, odnosno, particiju skupa V na skupove A, B koji minimiziraju (1). Monte Carlo algoritam dao je Karger 1993. godine koji, s velikom vjerojatnošću pogreške, u $O(m)$ vremenu računa minimalni rez. Algoritam se bazira na takozvanoj *kontrakciji bridova.*

Definicija 4. *Neka je $G = (V,E)$ multi-graf i $(u,v) \in E$.* ***Kontrakcija brida*** *(u,v) je postupak pri čemu:*

- *Vrhovi u i v zamjenjeni su sa super-vrhom $w = \{u,v\}$*
- *Brid (u,v) zamijenjuje se s petljom (w,w). Svaki brid čiji je jedan od krajeva u ili v sada ima w za kraj.*

Rezultirajući graf može sadržavati višestruke bridove i petlje.

Kontrakcija brida može pojednostaviti graf prilikom čega je očuvan rez (A,B).

Napomena 1. *Neka je (A,B) rez u G te neka je $e = (u,v)$ brid pri čemu su $u,v \in A$ ili $u,v \in B$. Ako je G' nastali graf nakon kontrakcije brida e, tada je $|(A,B)|$ jednak i u G i u G'.*

Lema 2. *Neka je G' graf nastali nakon kontrakcije brida e iz G. Svaki rez u G' odgovara rezu jednake veličine u G nad istim super-vrhovima.*

Dokaz. Slijedi direktno iz napomene 1. Uočimo da obrnuta implikacija ne vrijedi: nije svaki rez u G', rez u G. Posebno, svaki rez u G koji uključuje e, iščezava u G'. □

Kontrakcija očuva veličinu reza ukoliko taj brid ne povezuje skupove koji čine taj rez. Intuitivno, kontrakcija ne uzrokuje postojanje manjih rezova u G', što znači da minimalni rez u G je minimalni rez u G'. Upravo to je invarijanta oko koje se bazira algoritam.

Korolar 1. *Neka je (A, B) minimalni rez u G i neka je G' graf koji nastaje kontrakcijom brida $e \notin (A, B)$. Tada je (A, B) minimalni rez u G' te je jednake veličine.*

Nadalje navodimo pseudokod za Kargerov algoritam:

Algoritam 1: (Karger 1993)

Ulaz: $G = (V, E)$
Izlaz: Rez reprezentiran s dva supervrha koja su preostala u G_2

```
1 G_n ← G
2 za i ← (n − 1) do 2 čini
3 |   G_i ← G_{i+1}
4 |   Kontraktiraj e ∈ E_i, uniformno odabran i obriši sve petlje
5 kraj
6 vrati G_2
```

Sada je potrebno analizirati uspješnost algoritma. Najprije, jedna relacija između veličine minimalnog reza i broja bridova u grafu.

Lema 3. *Neka je λ veličina minimalnog reza u grafu $G = (V, E)$. Tada vrijedi $|E| \geq \lambda|V|/2$.*

Dokaz. Neka je $deg(v)$ stupanj vrha $v \in V$. Sumiranjem po svim vrhovima u G dobivamo

$$\sum_{v \in V} deg(v) = 2|E|.$$

To je zbog dvostrukog brojanja svakog brida. Veličina minimalnog reza daje donju među za stupanj vrha (u suprotnom bi vrh s manjim stupnjem inducirao manji rez).

$$\sum_{v \in V} deg(v) \geq \lambda|V|$$

Premještanjem dobivamo:

$$|E| \geq \frac{\lambda}{2}|V|$$

□

Sada možemo izreći i dokazati teorem koji nam govori o vjerojatnosti uspjeha Kargerovog algoritma

Teorem 3. *Neka je $G = (V, E)$ graf. Kargerov algoritam daje točan minimalni rez (A, B) s vjerojatnošću $\binom{n}{2}^{-1}$.*

Dokaz. Neka je $C = (A, B)$ t.d. $|C| = \lambda$ te $n = |V|$. Kargerov algoritam će vratiti C ukoliko se ne dogodi kontrakcija brida u C. Posebno, vjerojatnost da će prva kontrakcija izbjeći brid u C iznosi $1 - \lambda/|E|$. Prema lemi 3 slijedi da vjerojatnost da će u algoritmu doći do kontrakcije brida u C iznosi

$$\frac{\lambda}{|E|} \leq \frac{2\lambda}{\lambda n} = \frac{2}{n}$$

Vjerojatnost p_n da će algoritam izbjeći kontrakciju brida iz C zadovoljava rekurzivnu relaciju $p_n \geq (1 - \frac{2}{n})p_{n-1}$, pri čemu $p_2 = 1$. Raspisivanjem dobivamo:

$$\begin{aligned} p_n &\geq \left(1 - \frac{2}{n}\right) \cdot \left(1 - \frac{2}{n-1}\right) \cdots \left(1 - \frac{2}{4}\right) \cdot \left(1 - \frac{2}{3}\right) \\ &= \frac{n-2}{n} \cdot \frac{n-3}{n-1} \cdots \frac{3}{5} \cdot \frac{2}{4} \cdot \frac{1}{3} \\ &= \frac{2}{n(n-1)} \\ &= \binom{n}{2}^{-1}. \end{aligned}$$

□

S obzirom da je vjerojatnost pronalaska točno reza Kargerovim algoritmom mala, postupak se ponavlja određeni broj puta. Ponavljanjem algoritma $T = \binom{n}{2} \ln n$ puta, slučajno i nezavisno, vjerojatnost da će algoritam dati netočan rezultat je

$$\left[1 - \binom{n}{2}^{-1}\right]^T \leq \frac{1}{e^{\ln n}} = \frac{1}{n}.$$

Tada ukupno vrijeme izvršavanja algoritma na grafu s n vrhova i m bridova iznosi $O(Tm) = O(n^2 m \ln n)$.

4 Markovljevi lanci

Markovljevi lanci pružaju moćan alat u modeliranju slučajnih procesa. Pokazat ćemo kako ih možemo koristiti u analizi jednostavnih randomiziranih algoritama konkretno za 2-SAT problem. Kako bismo definirali Markovljeve lance, prvo je potrebno definirati slučajni proces.

Definicija 5. *Slučajni proces je familija slučajnih varijabli* $\mathbf{X} = \{X(t) : t \in T\}$ *na istom vjerojatnosnom prostoru* $(\Omega, \mathcal{F}, P)$. *Index* t *općenito predstavlja vrijeme te u tom slučaju proces* $\mathbf{X}$ *modelira vrijednost slučajne varijable* X *kroz vrijeme.* $X(t)$ *nazivamo stanje procesa u trenutku* t.

U nastavku, $X(t)$ označavat ćemo s X_t. Ako, za svaki t, X_t poprima vrijednosti iz prebrojivo beskonačnog skupa, tada kažemo da je $\mathbf{X}$ slučajni proces na *diskretnom skupu stanja*. Ako X_t poprima vrijednosti iz konačnog skupa tada je proces *konačan*. Ako je

T prebrojivo beskonačan skup tada kažemo da je $\mathbf{X}$ slučajni proces u *diskretnom vremenu*. Bez daljneg naglašavanja, $\mathbf{X}$ će biti slučajni proces na diskretnom skupu stanja u diskretnom vremenu.

Definicija 6. *Slučajni proces* $\mathbf{X} = \{X_0,\ X_1,\ \dots\}$ *je* ***Markovljev lanac*** *ako vrijedi*

$$\mathrm{P}(X_t = a_t \mid X_{t-1} = a_{t-1},\ X_{t-2} = a_{t-2},\ \dots,\ X_0 = a_0) = \mathrm{P}(X_t = a_t \mid X_{t-1} = a_{t-1})$$

To svojstvo naziva se ***Markovljevo svojstvo****.*

Važno je naglasiti da Markovljevo svojstvo ne implicira da je X_t nezavisna od $X_0,\ X_1,\ \dots,\ X_{t-2}$ već da se sva zavisnost X_t o prethodnim stanjima nalazi u X_{t-1}.

Definicija 7. *Prijelazna vjerojatnost* $P_{i,j} = \mathrm{P}(X_t = j \mid X_{t-1} = i)$ *je vjerojatnost da se dogodio prijelaz iz stanja* i *u stanje* j*.*

Markovljevo svojstvo implicira da je Markovljev lanac jedinstveno definiran matricom $\mathbf{P} = [P_{i,j}] \in M_n(\mathbb{R})$ koju nazivamo **matricom tranzicije**.

Matrica tranzicije korisna je reprezentacija Markovljevog lanca jer nam omogućuje jednostavnu metodu računanja distribucija budućih stanja. Naime, neka je $p_i(t)$ vjerojatnost da je proces u stanju i u trenutku t. Neka je $\overline{p}(t) = (p_0(t),\ p_1(t),\ p_2(t), \dots)$ vektor distribucije stanja lanca u vremenu t. Sumiranjem po svim stanjima za vrijeme $t-1$ dobivamo

$$p_i(t) = \sum_{j \geq 1} p_j(t-1) P_{j,i}.$$

to jest:

$$\overline{p}(t) = \overline{p}(t-1)\mathbf{P}.$$

Distrubiciju prikazujemo kao vektor redak i množimo $\overline{p}\mathbf{P}$ umjesto $\mathbf{P}\overline{p}$ u skladu s interpretacijom da počevši s distribucijom $\overline{p}(t-1)$ i djelovanjem s operatorom $\mathbf{P}$, dobivamo distribuciju $\overline{p}(t)$.

Definicija 8. *Neka je* $m \geq 0$*, definiramo vjerojatnost* m *- step tranzicije*

$$P_{i,j}^m = \mathrm{P}(X_{t+m} = j \mid X_t = i)$$

kao vjerojatnost da lanac prijeđe iz stanja i *u stanje* j *u točno* m *koraka.*

Tranzicijom sa i-tog stanja imamo

$$P_{i,j}^m = \sum_{k \geq 0} P_{i,k} P_{k,j}^{m-1}.$$

Neka je $\mathbf{P^{(m)}}$ matrica čije su vrijednosti vjerojatnosti m - step tranzicije, to jest, u i-tom retku i j-tom stupcu se nalazi vrijednost $P_{i,j}^m$. Primjenom prethodne jednakosti dobivamo

$$\mathbf{P^{(m)}} = \mathbf{P} \cdot \mathbf{P^{(m-1)}}.$$

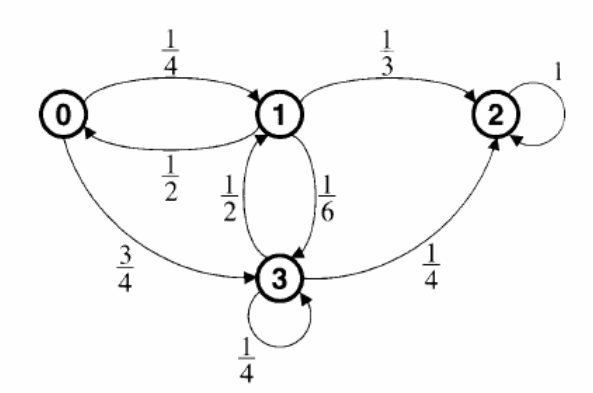
Induktivno po m slijedi da je

$$\mathbf{P^{(m)}} = \mathbf{P^m}.$$

Dakle, za svaki $t \geq 0$ i $m \geq 1$,

$$\overline{p}(t+m) = \overline{p}(t)\mathbf{P^m}.$$

Još jedna korisna reprezentacija Markovljevog lanca je s usmjerenim, težinskim grafom $G = (V, E, w)$. Skup vrhova predstavlja stanja lanca. Postoji usmjereni vrh $(i, j) \in E$ ako i samo ako $P_{i,j} > 0$ te u tom slučaju $w(i, j) = P_{i,j}$. Petlje su dopuštene. Ponovno, zahtjevamo da je $\sum_{(i,j)\in E} w(i, j) = 1$. Niz stanja kroz koje prođe proces reprezentiran je s usmjerenim putem na grafu.



$$\mathbf{P} = \begin{bmatrix} 0 & 1/4 & 0 & 3/4 \\ 1/2 & 0 & 1/3 & 1/6 \\ 0 & 0 & 1 & 0 \\ 0 & 1/2 & 1/4 & 1/4 \end{bmatrix}$$

Slika 1: Markovljev lanac (lijevo) i pripadna matrica tranzicije (desno)

Primjer 2. *Slika 1 nam daje primjer Markovljevog lanca i njegove dvije reprezentacije. Razmotrimo kako bismo izračunali, sa svakom reprezentacijom, vjerojatnost prelaska iz stanja 0 u stanje 3 u točno 3 koraka. Iz grafa možemo vidjeti da postoje samo 4 takva puta: 0-1-0-3, 0-1-3-3, 0-3-1-3 i 0-3-3-3. Vjerojatnost svakog puta računamo množenjem težina bridova na putu, a traženu vjerojatnost tako da sumiramo po svim putevima. Redom vjerojatnosti svakog puta su 3/32, 1/96, 1/16 i 3/64. Sumiranjem ovih vjerojatnosti dobivamo ukupnu vjerojatnost koja iznosi 41/192. Korištenjem matrice tranzicije, računamo*

$$\mathbf{P^3} = \begin{bmatrix} 3/16 & 7/48 & 29/64 & 41/192 \\ 5/48 & 5/24 & 79/144 & 5/36 \\ 0 & 0 & 1 & 0 \\ 1/16 & 13/96 & 107/192 & 47/192 \end{bmatrix}.$$

Element $P^3_{0,3} = 41/192$ *nam daje traženi rezultat. Matrica tranzicije je također korisna prilikom računanja vjerojatnosti da će se proces nalaziti u stanju 3 nakon 3 koraka ukoliko je početno stanje odabrano uniformno. To računamo*

$$[1/4,\ 1/4,\ 1/4,\ 1/4]\mathbf{P^3} = [17/192,\ 47/384,\ 737/1152,\ 43/288]$$

Ovdje, posljednji element, 43/288, je traženi rezultat.

4.1 Klasifikacija Markovljevih lanaca i stanja

Prvi korak u analiziraju dugoročnog ponašanja Markovljevih lanaca jest klasifikacija. U slučaju konačnog Markovljevog lanca, to je ekvivalentno analiziranju povezanosti usmjerenog grafa kojim je reprezentiran Markovljev lanac.

Definicija 9. *Kažemo da je stanje i dostupno iz stanja j, ako za neki $n \geq 0$ vrijedi $P^n_{i,j} > 0$. Ako su dva stanja i i j međusobno dostupna iz svakog, tada kažemo da oni komuniciraju i pišemo $i \leftrightarrow j$.*

Komunikacija definira relaciju ekvivalencije. Stoga, ta relacija particionira stanja u disjunktne klase ekvivalencije koje nazivamo komunikacijske klase. Moguće je posjetiti iz jedne klase drugu, ali nije moguće se vratiti (u suprotnom bi bile u istoj klasi).

Definicija 10. *Markovljev lanac je ireducibilan ako sva stanja pripadaju jednoj komunikacijskoj klasi.*

Drugim rječima, Markovljev lanac je ireducibilan ukoliko, za svaki par stanja, postoji nenul vjerojatnost da će se iz prvog stanja posjetiti drugo. Stoga imamo sljedeću lemu.

Lema 4. *Konačan Markovljev lanac je ireducibilan ako i samo ako je graf, koji ga reprezentira, strogo povezan graf.*

Nadalje, razlikujemo povratna i prolazna stanja. Neka je $r^t_{i,j}$ vjerojatnost da se, počevši u stanju i, prva tranzicija na stanje j dogodi u trenutku t; to jest,

$$r^t_{i,j} = \mathrm{P}(X_t = j \wedge \forall s,\ 1 \leq s \leq t-1 \implies X_s \neq j \mid X_0 = i).$$

Definicija 11. *Stanje je povratno ako $\sum_{t\geq 1} r^t_{i,i} = 1$, i ono je prolazno ako $\sum_{t\geq 1} r^t_{i,i} < 1$. Markovljev lanac je povratan ako su sva stanja lanca povratna.*

Ako je stanje i povratno, tada kada lanac jednom posjeti to stanje, ono će (s vjerojatnošću 1) se u nekom tenutku vratiti u to stanje. Stoga će lanac posjetiti to stanje beskonačno mnogo puta. Ukoliko je stanje prolazno, tada će lanac, počevši od i, posjetiti ponovno to stanje s vjerojatnošću < 1. U ovom slučaju, broj puta koji će lanac posjetiti i počevši od i biti dan geometrijskom slučajnom varijablom. Ako je jedno stanje komunikacijske klase prolazno (povratno), tada su sva ostala stanja te klase prolazna (povratna).

Za neko stanje i, označimo s $h_{i,i} = \sum_{t\geq 1} t \cdot r^t_{i,i}$ očekivano vrijeme povratka u stanje i. Slično za par stanja i, j s $h_{i,j} = \sum_{t\geq 1} t \cdot r^t_{i,j}$ označavamo očekivano vrijeme da se prvi puta posjeti j iz i. Za lanac koji je povratan čini se da za stanje i je, s obzirom da će se stanje i posjetiti beskonačno mnogo puta, $h_{i,i}$ konačan. Ovo nije slučaj, što motivira sljedeću definiciju.

Definicija 12. *Kažemo da povratno stanje i je pozitivno povratno ako $h_{i,i} < \infty$. U suprotnom kažemo da je nul povratno.*

Primjer 3. *Definiramo Markovljev lanac čija su stanja pozitivni cijeli brojevi. Neka od stanja i, vjerojatnost da će iduće posjećeno stanje biti $i+1$ iznosi $i/(i+1)$. S vjerojatnošću $1/(i+1)$, lanac se vraća u stanje 1. Počevši od 1, vjerojatnost da se neće lanac vratiti u stanje 1 u prvih t koraka iznosi dakle*

$$\prod_{j=1}^{t} \frac{j}{j+1} = \frac{1}{t+1}.$$

Stoga vjerojatnost da se nikada neće vratiti u stanje 1 iznosi 0, pa je stanje 1 povratno. Slijedi da je tada

$$r_{1,1}^{t} = \frac{1}{t(t+1)}.$$

Međutim, očekivani broj koraka da se vrati u stanje i iznosi

$$h_{1,1} = \sum_{t=1}^{\infty} t \cdot r_{1,1}^{t} = \sum_{t=1}^{\infty} \frac{1}{t+1},$$

što ne konvergira jer je posljednja suma harmonijski red.

Za kasnije razmatranje potrebno je definirati što znači da je Markovljev lanac aperiodičan. Primjer periodičnosti jest slučajna šetnja po cjelobrojnom brojevnom pravcu. Vjerojatnost da prelaska iz stanja i u stanja $i+1$ i $i-1$ su $1/2$. Ako lanac počinje u stanju 0, tada može biti na parnom stanju samo ako je prošao paran broj koraka.

Definicija 13. *Stanje j u Markovljevom lancu je periodično ako postoji $m \in \mathbb{N}$ t.d.*

$$m|s \implies \mathrm{P}(X_{t+s} = j \mid X_t = j) = 0.$$

Markovljev lanac je periodičan ako je bilo koje stanje periodično. Za stanje ili lanac koji nije periodičan kažemo da je aperiodičan.

Na kraju potpoglavlja navodimo, bez dokaza, važan korolar vezan za konačne Markovljeve lance.

Definicija 14. *Za aperiodično, pozitivno povratno stanje kažemo da je ergodično. Kažemo da je Markovljev lanac ergodičan ukoliko su mu sva stanja ergodična.*

Korolar 2. *Svaki konačan, ireducibilan i aperiodičan Markovljev lanac je ergodičan.*

4.2 Stacionarna distribucija

Posebna distrubicija od važnost je *stacionarna distribucija.*

Definicija 15. *Stacionarna distrubicija Markovljevog lanca je distribucija $\overline{\pi}$ takva da*

$$\overline{\pi} = \overline{\pi}\mathbf{P}.$$

Stacionarne distribucije su ključne u analizi Markovljevih lanaca. Fundementalni teorem o Markovljevim lancima karakterizira lance koji konvergiraju prema stacionarnoj distribuciji. Prije nego navedemo teorem o karakterizaciji, prvo lema koja će poslužiti u dokazu karakterizacije.

Lema 5. *Za svaki ireducibilan, ergodičan Markovljev lanac i za svako stanje i vrijedi*

$$\lim_{t\to\infty} P_{i,i}^t = \frac{1}{h_{i,i}}.$$

Teorem 4 (Fundementalni teorem Markovljevih lanaca)**.** *Svaki konačan, ireducibilan i ergodičan Markovljev lanac ima sljedeća svojstva:*

- *lanac ima jedinstvenu stacionarnu distribuciji $\overline{\pi} = (\pi_0, \pi_1, \ldots, \pi_n)$*
- *$\forall i, j,\ \lim_{t\to\infty} P_{j,i}^t$ postoji i ne ovisi o j*
- *$\pi_i = \lim_{t\to\infty} P_{j,i}^t = 1/h_{i,i}$.*

Dokaz. Iz činjenice da $\lim_{t\to\infty} P_{i,i}^t$ postoji, pokažimo da, za svaki i, j vrijedi

$$\lim_{t\to\infty} P_{j,i}^t = \lim_{t\to\infty} P_{i,i}^t = \frac{1}{h_{i,i}},$$

to jest, da ovi limesi postoje i nezavisni su o početnom stanju j. Kako je lanac ireducibilan znamo da $\sum_{t=1}^{\infty} r_{j,i}^t = 1$ i za svaki $\varepsilon > 0$ postoji konačan $t_1 = t_1(\varepsilon)$ takav da $\sum_{t=1}^{t_1} r_{j,i}^t \geq 1-\varepsilon$.

Za $j \neq i$,

$$P_{j,i}^t = \sum_{k=1}^{t} r_{j,i}^k P_{i,i}^{t-k}.$$

Za $t \geq t_1$,

$$\sum_{k=1}^{t_1} r_{j,i}^k P_{i,i}^{t-k} \leq \sum_{k}^{t} r_{j,i}^k P_{i,i}^{t-k} = P_{j,i}^t.$$

Iz činjenice da $\lim_{t\to\infty} P_{i,i}^t$ postoji i da je t_1 konačan, slijedi

$$\begin{aligned}
\lim_{t\to\infty} P_{j,i}^t &\geq \lim_{t\to\infty} \sum_{k=1}^{t_1} r_{j,i}^k P_{i,i}^{t-k} \\
&= \sum_{k=1}^{t_1} r_{j,i}^k \lim_{t\to\infty} P_{i,i}^t \\
&= \lim_{t\to\infty} P_{i,i}^t \sum_{k=1}^{t_1} r_{j,i}^k \\
&\geq (1-\varepsilon) \lim_{t\to\infty} P_{i,i}^t.
\end{aligned}$$

Slično,

$$\begin{aligned}
P_{j,i}^t &= \sum_{k=1}^{t} r_{j,i}^k P_{i,i}^{t-k} \\
&\leq \sum_{k=1}^{t_1} r_{j,i}^k P_{i,i}^{t-k} + \varepsilon
\end{aligned}$$

iz čega možemo zaključiti da je

$$\begin{aligned}\lim_{t\to\infty} P_{j,i}^t &\leq \lim_{t\to\infty}\left(\sum_{k=1}^{t_1} r_{j,i}^k P_{i,i}^{t-k} + \varepsilon\right)\\ &= \sum_{k=1}^{t_1} r_{j,i}^k \lim_{t\to\infty} P_{i,i}^{t-k} + \varepsilon\\ &\leq \lim_{t\to\infty} P_{i,i}^t + \varepsilon.\end{aligned}$$

Zbog proizvoljnosti ε, pokazali smo da za svaki par i i j,

$$\lim_{t\to\infty} P_{j,i}^t = \lim_{t\to\infty} P_{i,i}^t = \frac{1}{h_{i,i}}.$$

Sada neka je

$$\pi_i = \lim_{t\to\infty} P_{j,i}^t = \frac{1}{h_{i,i}}.$$

Pokažimo da je $\overline{\pi} = (\pi_0, \pi_1, \dots)$ stacionarna distribucija.

Za svaki $t \geq 0$, vrijedi da je $P_{i,i}^t \geq 0$ pa je $\pi_i \geq 0$. Za svaki $t \geq 0$, $\sum_{i=0}^n P_{j,i}^t = 1$ pa je

$$\lim_{t\to\infty} \sum_{i=0}^n P_{j,i}^t = \sum_{i=0}^n \lim_{t\to\infty} P_{j,i}^t = \sum_{i=0}^n \pi_i = 1$$

i $\overline{\pi}$ je dobro definirana distribucija. Sada,

$$P_{j,i}^{t+1} = \sum_{k=0}^n P_{j,k}^t P_{k,i}.$$

Za $t \to \infty$, slijedi

$$\pi_i = \sum_{k=0}^n \pi_k P_{k,i},$$

što pokazuje da je $\overline{\pi}$ stacionarna distribucija.

Pretpostavimo da postoji druga stacionarna distribucija $\overline{\phi} = (\phi_0, \phi_1, \dots)$. Tada vrijedi da

$$\phi_i = \sum_{k=0}^n \phi_k P_{k,i}^t,$$

i za $t \to \infty$ slijedi

$$\phi_i = \sum_{k=0}^n \phi_k \pi_i = \pi_i \sum_{k=0}^n \phi_k = \pi_i.$$

To vrijedi za svaki i pa prema tome $\overline{\phi} = \overline{\pi}$. □

4.3 Slučajne šetnje na neusmjerenim grafovima

Slučajna šetnja na neusmjerenom grafu posebna je vrsta Markovljevog lanca koja se često koristi u analizi algoritama. Neka je $G = (V, E)$ konačan, neusmjeren i povezan graf.

Definicija 16. *Slučajna šetnja na G je Markovljev lanac definiran nizom poteza čestice između vrhova od G. U ovom procesu, mjesto čestice u nekom trenutku je stanje sustava. Ako je čestica na vrhu i i ako $deg(i) > 0$, tada je vjerojatnost da će čestica ići bridom (i, j) do susjeda j jednaka $1/deg(i)$.*

Lema 6. *Slučajna šetnja na neusmjerenom grafu G je aperiodična ako i samo ako G nije bipartitan.*

Slučajna šetnja na konačnom, neusmjerenom i ne-bipartitnom grafu G zadovoljava svojstva 2 pa prema tome slučajna šetnja konvergira prema stacionarnoj distribuciji. Sljedeći teorem pokazuje da ova distribucija ovisi samo o nizu stupnjeva grafa.

Teorem 5. *Slučajna šetnja na G konvergira k stacionarnoj distribuciji $\overline{\pi}$, gdje*

$$\pi_v = \frac{d(v)}{2|E|}.$$

Dokaz. Kako $\sum_{v \in V} d(v) = 2|E|$, slijedi

$$\sum_{v \in V} \pi_v = \sum_{v \in V} \frac{d(v)}{2|E|} = 1,$$

i neka je $\overline{\pi}$ distribucija na $v \in V$.

Neka je $\mathbf{P}$ matrica tranzicije. Neka je $N(v)$ skup susjeda od v. Relacija $\overline{\pi} = \mathbf{P}\overline{\pi}$ ekvivalentna je

$$\pi_v = \sum_{u \in N(v)} \frac{d(u)}{2|E|} \frac{1}{d(u)} = \frac{d(v)}{2|E|}.$$

□

Kako je $h_{v,u}$ očekivani broj koraka od u do v, lako slijedi idući korolar.

Korolar 3. *Za svaki $u \in V$,*

$$h_{u,u} = \frac{2|E|}{d(u)}.$$

Za bilo koje $u, v \in V$, pokazujemo sljedeću gornju među.

Lema 7. *Ako $(u, v) \in E$, tada $h_{v,u} < 2|E|$.*

Dokaz. Neka je $N(u)$ skup svih susjeda od $u \in V$. $h_{u,u}$ računamo na dva različita načina:

$$\frac{2|E|}{d(u)} = h_{u,u} = \frac{1}{d(u)} \sum_{w \in N(u)} (1 + h_{w,u}).$$

Stoga,

$$2|E| = \sum_{w \in N(v)} (1 + h_{w,u}),$$

i zaključujemo da $h_{v,u} < 2|E|$. □

Definicija 17. *Vrijeme pokrivanja grafa $G = (V, E)$ je maksimum po svim vrhovima $v \in V$ od očekivanog vremena da se posjete svi vrhovi u grafu slučajnom šetnjom počevši od v.*

S obzirom da je graf povezan, jasno je da je taj broj konačan. Sljedeća lema pokazuje i gornju među na taj broj.

Lema 8. *Vrijeme pokrivanja grafa $G = (V, E)$ je omeđeno odozgo s $4|V| \cdot |E|$.*

Dokaz. Odaberemo bilo koje razapinjuće stablo od G. Tada postoji Eulerova tura tog razapinjućeg stabla koja svaki brid posjeti jednom u svakom smjeru. Takva tura se može konstruirati DFS-om(depth-first search). Neka s u $v_0, v_1, \ldots, v_{2|V|-2} = v_0$ niz vrhova u turi, počevši od v_0. Očito je očekivano vrijeme da se prođe kroz sve vrhove ture gornja međa na vrijeme pokrivanja. Stoga je gornja međa na vrijeme pokrivanja

$$\sum_{i=0}^{2|V|-3} h_{v_i,v_{i+1}} < (2|V| - 2)(2|E|) < 4|V| \cdot |E|,$$

gdje prva nejednakost slijedi iz 7. □

4.4 2-SAT

Promotrimo sada SAT (eng. satisfiability) problem. Booleova varijabla [2] zajedno sa svojom negacijom naziva se **literal**. Interpretacija je funkcija koja svakoj varijabli pridružuje vrijednosti **istina** ili **laž** (eng. True i False). Formulu oblika $A_1 \vee A_2 \vee \cdots \vee A_n$ nazivamo konjunkcija (A_i su proizvoljne formule). Formulu oblika $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ nazivamo disjunkcija. Elementarna konjunkcija je konjunkcija literala, a elementarna disjunkcija je disjunkcija literala. **Konjunktivna normalna forma** je konjunkcija elementarnih disjunkcija. SAT problem je dana konjuktivna normalna forma za koju je potrebno pronaći interpretaciju za koju je ona istinita (iznosi 1). Generalni SAT problem je NP - težak. Analizirat ćemo zato randomizirani algoritam za 2-SAT problem koji je rješiv u polinomnom vremenu. k-SAT problem je konjunktivna normalna forma pri čemu se u svakoj elementarnoj disjunkciji pojavljuje točno k literala. Dakle, 2-SAT problem ima točno 2 literala u svakoj elementarnoj disjunkciji. Sljedeći izraz je primjer 2-SAT:

$$(x_1 \vee \overline{x}_2) \wedge (\overline{x}_1 \vee \overline{x}_3) \wedge (x_1 \vee x_2) \wedge (x_4 \vee \overline{x}_3) \wedge (x_4 \vee \overline{x}_1).$$

Jedan prirodan način kojim pristupamo algoritmu jest da za 2-SAT formulu odaberemo neku interpretaciju, provjerimo koja od disjunkcija nije zadovoljena te promijenimo interpretaciju tako da ona disjunkcija bude istinita. Ako ima 2 literala u disjunkciji, onda postoje 2 načina na koji možemo pridružiti interpretaciju. Algoritam koji ćemo konstruirati na slučajan način će birati koju interpretaciju odabrati. U algoritmu, n označava broj varijabli u formuli i m je parametar koji opisuje vjerojatnost da algoritam završava s točnim rezultatom.

U primjeru iznad, ukoliko stavimo da interpretacija svake varijable bude 0, tada će disjunkcija $(x_1 \vee x_2)$ biti 0. Algoritam će tada možda promijeniti varijablu x_1 da bude 1. U

[2] u matematičkoj logici se još naziva **atomarna formula**

tom slučaju, disjunkcija $(x_4 \vee \overline{x}_1)$ će biti 0 i algoritam će tada moža promijeniti vrijednost varijable u toj disjunkciji itd.

Ukoliko algoritam završi s interpretacijom za koju je formula istinita, tada je očito vratio točan rezultat. Slučaj u kojemu algoritam ne pronađe dobru interpretaciju treba pažljivo razmotriti. Zasad, pretpostavimo da je formula ispunjiva i da će se algoritam izvršavati dok ne pronađe interpretaciju za koju je formula 1.

Zanima nas broj iteracija u while-petlji koji se izvrši. Kako 2-SAT formula ima $O(n^2)$ različitih disjunkcija, algoritmu je potrebno $O(n^2)$ da promijeni interpretaciju. Neka je S interpretacija za koju je 2-SAT formula s n varijabli ispunjiva i neka je A_i interpretacija u i-tom koraku algoritma. Neka je X_i broj varijabli koje se podudaraju u A_i i S. Kad je $X_i = n$, gotovi smo. Počevši s $X_i < n$, promatramo ponašanje X_i kroz vrijeme i posebno koliko vremena je potrebno prije nego $X_i = n$.

Najprije, ako $X_i = 0$ tada, za bilo koju promjenu $X_{i+1} = 1$. Dakle,

$$\mathrm{P}(X_{i+1} = 1 \mid X_i = 0) = 1.$$

Pretpostavimo sada da $1 \leq X_i \leq n - 1$. Na svakom koraku, odabiremo disjunkciju koja nije ispunjena. Kako je za S formula istinita, to znači da se A_i i S ne podudaraju u barem jednoj varijabli u toj disjunkciji. Jer disjunkcija nema više od dvije varijable, vjerojatnost da ćemo promijenom povećati broj podudaranja je barem $1/2$; vjerojatnost je 1 ukoliko se ne podudaraju u dvije varijable u danoj disjunkciji. Slijedi da je vjerojatnost da smanjimo broj podudaranja najviše $1/2$. Dakle, za $1 \leq i \leq n - 1$,

$$\begin{aligned}\mathrm{P}(X_{i+1} = j + 1 \mid X_i = j) &\geq 1/2\\ \mathrm{P}(X_{i+1} = j - 1 \mid X_i = j) &\leq 1/2.\end{aligned}$$

Slučajni proces $X_0, X_1, X_2, \ldots$ nije nužno Markovljev lanac, jer vjerojatnost povećanja X_i može ovisiti o tome da li se A_i i S ne podudaraju u jednoj ili dvije varijable u disjunkciji. To, naime, možda ovisi o prethodno razmatranim disjunkcijama. Međutim, razmotrimo sljedeći Markovljev lanac $Y_0, Y_1, Y_2, \ldots$:

$$\begin{aligned}Y_0 &= X_0\\ \mathrm{P}(Y_{i+1} = 1 \mid Y_i = 0) &= 1\\ \mathrm{P}(Y_{i+1} = j + 1 \mid Y_i = j) &= 1/2\\ \mathrm{P}(Y_{i+1} = j - 1 \mid Y_i = j) &= 1/2\end{aligned}$$

Markovljev lanac $Y_0, Y_1, Y_2, \ldots$ je pesimistična verzija slučajnog procesa $X_0, X_1, X_2, \ldots$ u tome što se X_i povećava na idućem koraku s vjerojatnošću koja iznosi barem $1/2$. Y_i se povećava s vjerojatnošću točno $1/2$. Jasno je da je očekivano vrijeme da proces dostigne n počevši od bilo kojeg stanja veća u Markovljevom lancu Y nego u procesu X. Markovljev lanac modelira slučajnu šetnju na neusmjerenom grafu G. Vrhovi grafa su brojevi $0, \ldots, n$

i, $1 \leq i \leq n-1$, vrh i je povezan s vrhovima $i-1$ i $i+1$. Neka je h_j očekivani broj koraka da se dođe do n počevši od j. Za 2-SAT algoritam, h_j je gornja međa za očekivani broj koraka da se S podudara u potpunosti s trenutnom interpretacijom koja se podudara s S na j mjesta.

Očino, $h_n = 0$ i $h_0 = h_1 + 1$ jer se od h_0 uvijek pomaknemo na h_1 za jedan korak. Koristimo linearnost očekivanja kako bismo pronašli opći izraz za h_j. Neka je Z_j slučajna varijabla koja predstavlja broj koraka da se iz stanja j dođe do n. Sada razmatramo početno stanje j, pri čemu $1 \leq j \leq n$. S vjerojatnošću $1/2$, slijedeće stanje je $j-1$ i u tom slučaju $Z_j = 1 + Z_{j-1}$. S vjerojatnošću $1/2$, slijedeće stanje je $j+1$ i u tom slučaju $Z_j = 1 + Z_{j+1}$. Stoga,

$$\mathbf{E}[Z_j] = \mathbf{E}\left[\frac{1}{2}(1 + Z_{j-1}) + \frac{1}{2}(1 + Z_{j+1})\right].$$

Ali $\mathbf{E}[Z_j] = h_j$ i tako, primjenom linearnosti očekivanja dobivamo

$$h_j = \frac{h_{j-1}}{2} + \frac{h_{j+1}}{2} + 1$$

Stoga imamo sljedeći sustav jednadžbi

$$\begin{aligned} h_n &= 0 \\ h_j &= \frac{h_{j-1}}{2} + \frac{h_{j+1}}{2} + 1 \\ h_0 &= h_1 + 1 \end{aligned}$$

Matematičkom indukcijom, lako se pokaže da za $0 \leq j \leq n-1$,

$$h_j = h_{j+1} + 2j + 1.$$

Induktivno zaključujemo da

$$h_0 = h_1 + 1 = h_2 + 1 + 3 = \cdots = \sum_{i=0}^{n-1} 2i + 1 = n^2.$$

Time smo pokazali sljedeću lemu

Lema 9. *Pretpostavimo da je 2-SAT formula s n varijabli ispunjiva i da je 2-SAT algoritmu dopušteno vrijeme izvršavanja dok ne pronađe ispunjivu interpretaciju. Tada je očekivani broj koraka algoritma najviše n^2.*

Prije dokazivanja teorema o uspješnosti 2-SAT algoritma, navodimo bez dokaza Markovljevu nejednakost koja je vrlo korisna u teoriji vjerojatnosti.

Teorem 6. *Neka je X slučajna varijabla i g nenegativna funkcija definirana na $\mathcal{R}(X)$ takva da postoji $\mathbf{E}[X]$. Tada za svaki $\varepsilon > 0$ vrijedi:*

$$P(g(X) \geq \varepsilon) \leq \frac{\mathbf{E}[g(X)]}{\varepsilon}.$$

Sada ćemo se posvetiti problemu ukoliko 2-SAT formula nije ispunjiva, to jest, ne postoji interpretacija za koju je formula istinita te vjerojatnosti uspjeha algoritma.

Teorem 7. *2-SAT algoritam uvijek vraća točan rezultat za formulu koja nije ispunjiva. Ako je formula ispunjiva, tada s vjerojatnošću barem* $1-2^{-m}$ *algoritam vraća točnu interpretaciju. U suprotnom, netočno vraća da je formula neispunjiva.*

Dokaz. Očito je da će, ukoliko ne postoji interpretacija za koju je formula istinita, algoritam vratiti da je formula neispunjiva. Pretpostavimo da je formula ispunjiva. Podijelimo izvršenje algoritma na segmente duljine $2n^2$ koraka. Ako nije pronađeno točna ispunjiva interpretacija u prvih $i-1$ segmenata, zanima nas uvjetna vjerojatnost da algoritam nije pronašao ispunjivu interpretaciju u i-tom segmentu. Prema prethodnoj lemi, očekivano vrijeme da se pronađe ispunjiva interpretacija je omeđena odozgo s n^2. Neka je Z broj koraka od početka segmenta i do trenutka kada algoritam pronađe ispunjivu interpretaciju. Primjenom Markovljeve nejednakosti,

$$\mathrm{P}(Z > 2n^2) \leq \frac{n^2}{2n^2} = \frac{1}{2}.$$

Tako je vjerojatnost da algoritam neuspijeva pronaći ispunjivu interpretaciju nakon m segmenata omeđena odozgo s $(1/2)^m$ □

Algoritam 2: (2-SAT)

Ulaz: F
Izlaz: $x_1, x_2, \ldots, x_n$
$A_0 \leftarrow$ slučajno odabrana početna interpretacija
$i \leftarrow 1$
dok $i < 2mn^2$ **čini**
  Slučajno odaberi disjunkciju koja nije istinita
  Uniformno slučajno odaberi varijablu u odabranoj disjunkciji i promijeni joj vrijednost
  $i \leftarrow i + 1$
kraj
ako *Interpretacija ispunjiva* **onda**
  vrati $x_1, \ldots, x_n$
inače
  vrati formula nije ispunjiva
kraj

5 Maze problem

Labirint je matrica čije su vrijednosti iz skupa $\{0, 1\}$ pri čemu 0 predstavlja prazno mjesto, a 1 predstavlja blokirano mjesto. Dopušteni potezi su *gore*, *dolje*, *lijevo* i *desno*. Ukoliko pokušamo izvršiti potez na blokirano mjesto, jednostavno ostanemo na mjestu. Riješiti labirint znači pronaći niz poteza kojim bismo počevši u $(0, 0)$ obišli (n, m) za labirint dimenzije $n \times m$. Za labirint kažemo da je rješiv ukoliko takav niz poteza postoji. Razmotrimo problem pronalaska najkraćeg takvog niza poteza koji rješava skup $n \times m$ rješivih labirinata $\mathcal{M}$ istovremeno. Za niz koji rješava skup $\mathcal{M}$ kažemo da je **savršen** ukoliko konačna pozicija u svakom labiritnu iz $\mathcal{M}$ je (n, m).

Rješenje problema istovremenog rješavanja nizova može se interpretirati kao hitan protokol za robota, čiji su senzori zatajili, koji omogućuje dolazak do izlaza sobe unatoč tome što nema nikakvo znanje o broju i poziciji potencijalnih prepreka. Pronalaženje rješenja u praksi izaziva potprobleme koji su zanimljivi sami po sebi. Ima više od $9 \cdot 10^9$ labirinta dimenzije 7×7 pa sama provjera točnosti niza je zahtjevna. Nadalje, čini se da je primjena bilo kojeg algoritma za pronalaženje rješenja problema osuđena na propast zbog eksponencijalnog rasta $|\mathcal{M}|$.

Uočimo da je konstruiranje algoritma koji pronalazi takav niz trivijalan. Odaberemo neki labirint $L_1 \in \mathcal{M}$. Pretraživajem u širinu lako možemo dobiti niz poteza kojim bi riješili L_1. Odaberemo sada neki drugi labirint u $L_2 \in \mathcal{M} \backslash \{L_1\}$. Izvršimo niz poteza koji smo dobili rješavanjem L_1. Ukoliko taj niz rješava L_2, nastavljamo dalje. Ako nismo došli do tražene pozicije u L_2, ponovnim pretraživanjem u širinu nadopunjujemo početni niz. Ponavljanjem ovog postupka dobit ćemo u konačnici niz koji rješava $\mathcal{M}$.

Poblem ovom pristupu je što redoslijed kojim odabiremo labirinte iz $\mathcal{M}$ znatno utječe na konačni niz poteza. Naravno da u praksi ovaj algoritam nije upotrebljiv te nas zanima postoji li algoritam koji će nam dati najkraći savršeni niz. Naime, dokaz postojanja savršenog niza se temelji na vjerojatnostnoj metodi i Markovljevim lancima, ali nije konstruktivan.

Teorem 8. *Za dane $n, m \in \mathbb{N}$, postoji savršeni niz za sve rješive labirinte dimenzije $n \times m$.*

Dokaz. Za $n < 2$ ili $m < 2$ tvrdnja je trivijalna. Označimo s $p_u,\ p_l,\ p_d$ i p_r redom vjerojatnosti da ćemo se kretati u smjeru gore, lijevo, dolje i desno. Neka su $p_u = p_l = c$, $p_d = p_r = \frac{1}{2} - c,\ c = (\frac{1}{4})^{nm} \leq \frac{1}{4}$. Ovime smo definirali Markovljev lanac. Tvrdimo da je stacionarna distribucija svakog Markovljevog lanca koji pripada labirintu iz $\mathcal{M}$ dana s $p_{i,j} \propto \left(\frac{\frac{1}{2}-c}{c}\right)^{i+j}$ gdje je $p_{i,j}$ vjerojatnost da se nalazimo na poziciji (i, j) ukoliko je do nje moguće doći. Treba imati na umu da ova se distribucija razlikuje do na konstantu u ovisnosti o labirintu - što je ukorporirano u proporcionalnosti.

Sada ćemo pokazati da to uistinu je stacionarna distribucija. Vjerojanosti očito u sumi daju 1. Pokažimo prvo da račun ne ovisi da li se trenutna pozicija nalazi pored zida ili

slobodnog mjesta:

$$p_{i,j-1} \cdot p_r = p_{i-1,j} \cdot p_d = \left(\frac{\frac{1}{2}-c}{c}\right)^{i+j-1} \cdot \left(\frac{1}{2}-c\right)$$
$$= \left(\frac{\frac{1}{2}-c}{c}\right)^{i+j} \cdot c = p_{i,j} \cdot p_u = p_{i,j} \cdot p_l.$$

Pokažimo sada stacionarnost. Neka je $v_{i,j}$ čvor Markovljevog lanca koji pripada poziciji (i,j).

$$\sum_{v_{k,l} \in V} p_{k,l}\ p((v_{k,l}, v_{i,j}))$$
$$= 2\left(\frac{\frac{1}{2}-c}{c}\right)^{i+j} \cdot c + 2\left(\frac{\frac{1}{2}-c}{c}\right)^{i+j} \cdot \left(\frac{1}{2}-c\right)$$
$$= \left(2c + 2\left(\frac{1}{2}-c\right)\right) \cdot \left(\frac{\frac{1}{2}-c}{c}\right)^{i+j} = p_{i,j}.$$

Iz činjenice da vjerojatnost da se nalazimo u konačnoj poziciji ne iznosi 1, zaključujemo:

$$\left(\frac{\frac{1}{2}-c}{c}\right)^{n+m} < 1 \iff \left(\frac{\frac{1}{2}-c}{c}\right)^{n+m-1} < \frac{c}{\frac{1}{2}-c} \leq \frac{c}{\frac{1}{2}-\frac{1}{4}} \leq 4c$$

Kako definirani Markovljevi lanci su aperiodični, svaka početna distribucija konvergira k stacionarnoj distribuciji. Prema tome, za dovoljno veliki niz, za svaki labirint vrijedi

$$\mathrm{P}(\text{nije u konačnoj poziciji}) < 4c(nm-1) = 4\Big(\frac{1}{4}\Big)^{nm}(nm-1)$$

gdje je $(nm-1)$ najveći broj dostupnih polja u labiritnu izuzev konačnog polja. Iz σ-subaditivnosti slijedi:

$$\mathrm{P}(\text{nisu svi u konačnoj poziciji}) \leq \sum_{M \in \mathcal{M}} 4\Big(\frac{1}{4}\Big)^{nm}(nm-1)$$
$$\leq 2^{nm-2} \cdot 4\Big(\frac{1}{4}\Big)^{nm}(nm-1) \leq \frac{1}{4}.$$

Druga nejednakost vrijedi jer postoji manje od 2^{nm-2} rješivih nizova dimenzije $n \times m$. Slijedi da je onda

$$\mathrm{P}(\text{svi u konačnoj poziciji}) = 1 - \mathrm{P}(\text{nije u konačnoj poziciji}) \geq 1 - \frac{1}{4} = \frac{3}{4} > 0.$$

Prema tome, savršeni niz postoji. □

Nadalje, pokazat ćemo gornju među na veličinu rješivog niza za proizvoljan skup labirinta dimenzije $n \times m$.

Teorem 9. *Za svaki skup rješivih $n \times m$ labirinta postoji rješivi niz veličine $\mathcal{O}((nm)^3)$.*

Dokaz. Neka je s slučajno odabrani niz takav da $|s| = 8nm(nm-1)(nm+1) \in \mathcal{O}((nm^3))$. Potezi u nizu su birani uniformno slučajno tako da su svi potezi jednako mogući. Neka je $\mathcal{M}_{n,m}$ skup svih rješivih $n \times m$ labirinta i neka je $X_M, M \in \mathcal{M}_{n,m}$ slučajna varijabla takva da:

$$X_M = \begin{cases} 1, & \text{ako } s \text{ rješivi niz za } M \\ 0, & \text{inače} \end{cases}$$

Nadalje, neka je $Y := \sum_{M \in \mathcal{M}_{n,m}} X_M$. Lako vidimo da je s rješivi niz za $\mathcal{M}_{n,m}$ ako i samo ako $Y = 0$. Dovoljno je pokazati da je $\mathbf{E}[Y] < 1$ jer tada prema argumentu očekivanja iz 1 slijedi da rješivi niz za skup $\mathcal{M}_{n,m}$ postoji.

Neka je s konkatenacija $nm+1$ slučajnih nizova $s_1, \ldots, s_{n,m+1}$, pri čemu je svaki duljine $8nm(nm-1)$. Neka je Z slučajna varijabla koja modelira koliko je poteza potrebno kako bi se obišla sva dostupna mjesta u labirintu. Kako je labirint neusmjeren graf, Z modelira slučajnu šetnju pa prema 8 slijedi $\mathbf{E}[Z] \leq 4nm(nm-1)$. Nadalje, prema Markovljevoj nejednakosti

$$\mathrm{P}(Z \geq 8nm(nm-1)) \leq \frac{\mathbf{E}[Z]}{8nm(nm-1)} \leq \frac{4nm(nm-1)}{8nm(nm-1)} \leq \frac{1}{2}.$$

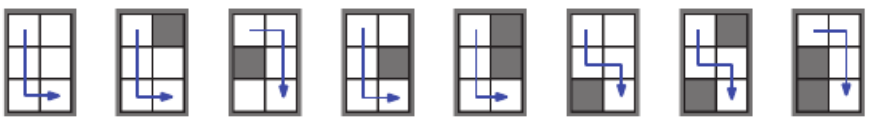
Drugim riječima, vjerojatnost da tokom izvršavanja poteza niza $s_i,\ 1 \leq i \leq nm+1$ ne posjetimo traženo polje (ukoliko počnemo na proizvoljnom polju) iznosi $\frac{1}{2}$. Stoga, vjerojatnost da nećemo posjetiti traženo polje prilikom izvršavanja niza $s = s_1 \cdots s_{nm+1}$ iznosi

$$\mathrm{P}(X_M = 1) \leq \left(\frac{1}{2}\right)^{nm+1} = 2^{-(nm+1)}.$$

Prema tome,

$$\mathbf{E}[Y] = \mathbf{E}\Big[\sum_{M \in \mathcal{M}_{n,m}} X_M\Big] = \sum_{M \in \mathcal{M}_{n,m}} \mathbf{E}[X_M] \leq 2^{nm} \cdot 2^{-(nm+1)} = \frac{1}{2} < 1.$$

Prema argumentu očekivanja slijedi da rješivi niz tražene duljine postoji. □



Slika 2: Svi rješivi nizovi dimenzije 3×2 zajedno s njihovim najkraćim rješivim nizom duljine 5 *ddrdd* koji je ujedno i savršeni niz.

6 Zaključak

Vjerojatnosna metoda daje moćan i elegantan alat za pokazivanje egzistencije rješenja. Također, kao što smo pokazali u problemu globalnog minimalnog reza i maze problema, korisna je kako bi dali među na kompleksnost rješenja. Treba imati na umu da u većini slučajeva, vjerojatnosna metoda neće dati nikakav uvid u rješenje. U maze problemu, pokazali smo da, za dovoljno dugačak niz poteza, rješenje postoji, ali nismo dobili uvid u algoritam koji bi nam pronašao to rješenje. To je najveća mana ove metode jer uglavnom nije konstruktivna. Maze problem je i dalje otvoreno pitanje za koje nije poznat algoritam kojim bi ga efektivno rješili. Idući korak na ovu temu bi bio da, na temelju vjerojatnosti iz 8, simuliramo rješenja te testiramo na nekim skupovima labirinta.

Literatura

[1] N.Alon, J.H.Spencer, *The Probabilistic Method,* Wiley - Interscience Series in Discrete Mathematics and Optimization, 3. izdanje, John Wiley & Songs, Inc., 2008.

[2] Michael Mitzenmacher, Eli Upfal, *Probability and Computing - Randomized Algorithms and Probabilistic Analysis*, Cambridge University Press, 2005

[3] Tianqi Song, *Design and Analysis of Algorithms*, Scribe notes, 2016. `https://www2.cs.duke.edu/courses/spring16/compsci330/Notes/LVMC.pdf`

[4] Mladen Vuković, *Matematička logika 1 - skripta*, PMF - Matematički odjel, Zagreb, 2007.

[5] Mirta Benšić, Nenad Šuvak, *Uvod u vjerojatnost i statistiku*, Sveučilište J. J. Strossmayera, Odjel za matematiku, Osijek, 2014.

[6] Stefan Funke, Andre Nusser, *The Simultaneous Maze Solving Problem*, Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence (AAAI-17)