Osnove verjetnostne metode

doc. dr. R. Škrekovski

Oddelek za Matematiko
Fakulteta za Matematiko in Fiziko
Univerza v Ljubljani

naslov: Osnove verjetnostne metode

avtorske pravice: dr. Riste Škrekovski

izdaja: prva izdaja

Založnik: samozaložba

avtor: Riste Škrekovski

leto izida: 2010 (v Ljubljani)

natis: elektronsko gradivo
http://www.fmf.uni-lj.si/ skreko/Gradiva/OVM-skripta.pdf

CIP - KatEložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

519.172

ŠKREKOVSKI, Riste
Osnove verjetnostne metode [Elektronski vir] /
R. Škrekovski. - 1. izd. - El. knjiga. - Ljubljana : samozal., 2010

Način dostopa (URL): http://www.fmf.uni-lj.si/ skreko/Gradiva/OVM-skripta.pdf

ISBN 978-961-92887-4-0

251444992

Kazalo

Poglavje 1

Osnovna metoda

Trditev 1.1 *Če so dogodki $A_1, A_2, \ldots, A_n$ slabi in velja $\sum_{i=1}^{n} \Pr(A_i) < 1$, potem se s pozitivno verjetnostjo nobeden od njih ne zgodi.*

Dokaz. Za dogodke $A_1, A_2, \ldots, A_n$ velja $\Pr(A_1 \cup A_2 \cup \ldots \cup A_n) \leq \sum_{i=1}^{n} \Pr(A_i)$. Zato je

$$\begin{aligned} \Pr(\cap A_i^C) &= 1 - \Pr(A_1 \cup A_2 \cup \ldots \cup A_n) \\ &\geq 1 - \sum_{i=1}^{n} \Pr(A_i) \\ &> 0. \end{aligned}$$

□

1.1 Ramseyeva števila

Preden definiramo Ramseyevo število, se spomnimo, kaj je to klika in kaj neodvisna množica. *Klika* je množica točk, ki tvori poln graf in *neodvisna množica* je množica paroma nesosednjih točk.

Ramseyevo število $R(k, l)$ je najmanjše celo število n, tako da poljuben graf na n točkah vsebuje kliko velikosti k ali neodvisno množico velikosti l. Ramsey je pokazal, da število $R(k, l)$ obstaja za katerikoli števili k in l, torej vsak dovolj velik graf vsebuje kliko ali neodvisno množico predpisane velikosti.

Obstoj Ramseyevih števil sledi iz naslednje rekurzivne zveze:

$$R(k, l) \leq R(k-1, l) + R(k, l-1).$$

Kljub temu so točne vrednosti $R(k, l)$ še vedno neznane, razen za majhen k in/ali l. Ni težko opaziti, da velja $R(1, l) = 1$ in $R(k, 1) = 1$ ter $R(k, l) = R(l, k)$ za poljubni pozitivni celi števili k in l. Velja tudi $R(3,3) = 6$, $R(3,4) = 9$, $R(3,5) = 14$, $R(4,4) = 18$ in $R(4,5) = 25$. Številom $R(k,k)$ pravimo *diagonalna* Ramseyeva števila.

V dokazu naslednjega izreka uporabimo verjetnostno metodo, s katero dokažemo spodnjo mejo za $R(k,k)$. Ta nam pove, da Ramseyeva števila hitro naraščajo. Opazi še, da velja $R(a,b) \geq R(c,d)$ kadar $a \geq c$ in $b \geq d$.

Izrek 1.2 *Za vsak $k \geq 3$ velja*

$$R(k,k) > 2^{k/2-1}.$$

Dokaz. Želimo pokazati, da za $n \leq 2^{k/2-1}$ obstaja graf, ki nima ne klike ne neodvisne množice velikosti k. Potem bo sledilo $R(k,k) > 2^{k/2-1}$.

Naj bo G graf na n točkah, kjer vsak par točk tvori povezavo z verjetnostjo $\frac{1}{2}$ in je vsaka povezava izbrana neodvisno od ostalih povezav. Za vsako fiksno množico k točk izračunajmo verjetnost, da tvorijo kliko. Verjetnost, da izberemo vse povezave oziroma kliko na k točkah, je enaka $2^{-\binom{k}{2}}$. Z enako verjetnostjo izberemo neodvisno množico velikosti k. Ker imamo n točk v grafu, lahko k točk izberemo na $\binom{n}{k}$ načinov.

Naj bo A_k dogodek, da graf vsebuje kliko velikosti k, B_k pa dogodek, da graf vsebuje neodvisno množico velikosti k. Tako je $A_k \cup B_k$ dogodek, da G vsebuje kliko ali neodvisno množico velikosti k. Velja

$$\Pr(A_k \cup B_k) = \Pr(A_k) + \Pr(B_k) - \Pr(A_k \cap B_k) \leq \Pr(A_k) + \Pr(B_k) = 2 \cdot \binom{n}{k} 2^{-\binom{k}{2}}.$$

Vemo, da je $n \leq 2^{k/2-1}$ in $k \geq 3$, torej je $n^k \leq 2^{(k/2-1)k}$ in od tod

$$2n^k \leq 2^{k^2/2-k/2-k/2+1} = 2^{\frac{k(k-1)}{2}} \cdot 2^{1-k/2} < 2^{\frac{k(k-1)}{2}}.$$

Ker velja $\binom{n}{k} \leq n^k$, ocenimo

$$2 \cdot \binom{n}{k} 2^{-\binom{k}{2}} \leq 2n^k 2^{-\binom{k}{2}} < 2^{\frac{k(k-1)}{2}} \cdot 2^{-\binom{k}{2}} = 1.$$

Torej je $\Pr(A_k \cup B_k) < 1$ in je zato verjetnost nasprotnega dogodka pozitivna. Torej obstaja tak graf na $\lfloor 2^{k/2-1} \rfloor$ točkah, ki ne vsebuje niti klike velikosti k niti neodvisne množice velikosti k. Torej je $R(k,k) > 2^{k/2-1}$.

□

V resnici se da dokazati, da je $R(k,k) > 2^{k/2}$, vendar je dokaz bolj zapleten, zato ga obravnavamo kasneje.

1.2 Barvanje hipergrafa

Hipergraf je posplošitev grafa, kjer so povezave množice točk poljubne velikosti. Par (V, E) je *k-enoličen hipergraf*, pri čemer je V množica točk in $E \subseteq \binom{V}{k}$ množica hiperpovezav. Torej enostavni grafi so 2-enolični hipergrafi. Hipergraf je *k-obarvljiv*, če lahko njegove točke pobarvamo s k barvami tako, da nobena hiperpovezava ni monokromatska, t.j. vsaj dve različni barvi se pojavita na vsaki hiperpovezavi.

Naj bo $m(k)$ najmanjše število hiperpovezav v k-enoličnem hipergrafu, ki ni 2-obarvljiv. Za grafe velja $m(2) = 3$, ker K_3 ni 2-obarvljiv. Hipergraf Fanove ravnine je najmanjši 3-uniformen hipergraf, ki ima 7 točk, 7 povezav in ni 3-obarvljiv. Zato je $m(3) = 7$. Za večji k je veliko težje določiti $m(k)$. Natančna vrednost $m(k)$ je neznana za $k > 3$. Lahko pa dobimo spodnjo mejo $m(k)$ s pomočjo verjetnostne metode.

Izrek 1.3 *Za vsak $k \geq 2$ velja*

$$m(k) \geq 2^{k-1}.$$

Dokaz. Imamo k-enoličen hipergraf $\mathcal{H} = (V, E)$ z manj kot 2^{k-1} hiperpovezavami. Dokazali bomo, da je 2-obarvljiv. Pobarvajmo vsako točko hipergrafa $\mathcal{H}$ neodvisno z rdečo ali modro z verjetnostjo $\frac{1}{2}$. Verjetnost, da so točke dane hiperpovezave vse rdeče ali vse modre, je

$$p = \frac{1+1}{2^k} = 2 \cdot (\frac{1}{2})^k = 2^{1-k}.$$

Predpostavili smo, da za $\mathcal{H}$ velja $|E| < 2^{k-1}$. Označimo z A dogodek, da obstaja monokromatska hiperpovezava, in ocenimo $\Pr(A)$:

$$\Pr(A) \leq p \cdot |E| < p \cdot 2^{k-1} = 2^{1-k} \cdot 2^{k-1} = 1.$$

Torej nobena hiperpovezava ni monokromatska s pozitivno verjetnostjo t.j. $\Pr(\overline{A}) = 1 - \Pr(A) > 0$ in zato obstaja pravilno barvanje. Torej je $m(k) \geq 2^{k-1}$.

□

1.3 Turnirji z lastnostjo $\mathcal{P}_k$

Usmerjen poln graf T imenujemo *turnir*. Turnir predstavlja igro, pri kateri vsak par igralcev igra med sabo in eden izmed njiju vedno zmaga. Vozlišča grafa predstavljajo igralce. Usmerjena povezava (a, b) pa pomeni, da je igralec a premagal igralca b.

Pravimo, da ima turnir lastnost $\mathcal{P}_k$, če vsako množico igralcev $S \subset V(T)$ moči k premaga nek igralec $v \in V(T) \setminus S$.

Izrek 1.4 (Erdös, 1963) *Če velja $\binom{n}{k}(1-2^{-k})^{n-k} < 1$, potem obstaja turnir z n vozlišči in lastnostjo $\mathcal{P}_k$.*

Dokaz. Naj bo T slučajen turnir z n igralci in naj bo S množica k igralcev. Naj bo A_S dogodek, da noben igralec $v \in V(T) \setminus S$ ne premaga vseh igralcev iz S. Verjetnost, da se A_S zgodi je enaka

$$\Pr(A_S) = (1-2^{-k})^{n-k}\,.$$

Torej je verjetnost, da se tak dogodek zgodi za katerokoli množico S enaka

$$\Pr(\cup A_S) \leq \binom{n}{k}(1-2^{-k})^{n-k} < 1\,.$$

Verjetnost, da se noben izmed dogodkov A_S ne zgodi, je pozitivna, zato obstaja turnir z n igralci in lastnostjo $\mathcal{P}_k$.

$\square$

Posledica 1.5 *Za vsak $n \geq k^2 \cdot 2^{k+1}$ obstaja turnir z lastnostjo $\mathcal{P}_k$.*

Dokaz. Naj bo $n \geq k^2 \cdot 2^{k+1}$. Z uporabo neenačb $\binom{n}{k} < \left(\frac{en}{k}\right)^k$ in $(1-2^k)^{n-k} < e^{-\frac{n-k}{2^k}}$ se da pokazati, da je $\binom{n}{k}(1-2^k)^{n-k} < 1$. Potem trditev sledi iz izreka 1.4.

$\square$

1.4 Van der Waerdenova števila

Van der Waerdenovo število $W(r,k)$ imenujemo najmanjši $n \in \mathbb{N}$, za katerega imamo pri vsakem barvanju množice $\{1,2,\ldots,n\}$ z r barvami neko enobarvno aritmetično zaporedje s k členi, tj. obstajata $a, b \in \mathbb{N}$, za katera velja, da je zaporedje $a, a+b, a+2b, \ldots, a+(k-1)b$ enobarvno.

Leta 1927 je Van der Waerden dokazal, da takšna števila obstajajo, njihova rast pa je izredno hitra. Pokazali bomo, da že za $r=2$ naraščajo eksponentno.

Izrek 1.6 *Velja $W(2,k) > 2^{k/2}$. Torej množico $\{1,2,\ldots,n\}$ lahko pobarvamo z dvema barvama, tako da nobeno aritmetično zaporedje z $2\ln n$ členi ni enobarvno.*

Dokaz. Števila $\{1, 2, \ldots, n\}$ pobarvajmo naključno z barvama R in M. Naj bo S aritmetično zaporedje s k členi in A_S dogodek, da je S enobarvno. Verjetnost, da se A_S zgodi je enaka

$$\Pr(A_S) = 2 \cdot 2^{-|S|} = 2^{1-k}\,.$$

Vsako aritmetično zaporedje s k členi je določeno s prvima dvema členoma. Torej imamo kvečjemu $\binom{n}{2}$ takšnih aritmetičnih zaporedij v množici $\{1, 2, \ldots, n\}$ in velja

$$\Pr(\cup A_S) < \binom{n}{2} 2^{1-k} < 1\,.$$

Torej obstaja neko barvanje, za katerega ni aritmetičnega zaporedja s k členi in $W(2, k) > n$. Od tukaj sledi, da je $W(2, k)$ večji od vsakega n-ja, za katerega velja $\binom{n}{2} 2^{1-k} < 1$. Ni težko preveriti, da za $n = 2^{\frac{k}{2}}$ velja ta neenakost, torej $W(2, k) > 2^{\frac{k}{2}}$.

□

1.5 Množice proste za vsote

Podmnožica A Abelove grupe je *prosta za vsoto*, če je $(A + A) \cap A = \emptyset$, torej vsota poljubnih dveh elementov množice A ni v množici A. Naslednji Erdösev izrek nam pove, da je v vsaki množici neničelnih celih števil več kot tretjina takšnih, ki se med seboj ne seštejejo v kakšno drugo število iz te množice.

Izrek 1.7 (Erdös, 1965) *Vsaka množica $B = \{b_1, \ldots, b_n\}$ neničelnih celih števil vsebuje za vsoto prosto podmnožico velikosti več kot $\frac{n}{3}$.*

Dokaz. Naj bo $p = 3k + 2$ praštevilo, večje od $2 \max_{1 \leq i \leq n} |b_i|$ in naj bo $C = \{k + 1, k + 2, \ldots, 2k + 1\}$. Opazimo, da je C za vsoto prosta podmnožica ciklične grupe $\mathbb{Z}_p$ in da velja

$$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}.$$

Izberimo si naključno naravno število x, $1 \leq x < p$, glede na enakomerno porazdelitev na množici $\{1, 2, \ldots, p-1\}$ in definirajmo $d_1, \ldots, d_n$ s predpisom $d_i \equiv x b_i \pmod p$, torej je $0 \leq d_i < p$. Očitno za vsak fiksen i, $1 \leq i \leq n$ velja, da če x zasede vse vrednosti $1, 2, \ldots, p - 1$, potem d_i doseže vse neničelne elemente množice $\mathbb{Z}_p$ in tako je

$$\Pr(d_i \in C) = \frac{|C|}{p-1} > \frac{1}{3}.$$

Pričakovano število elementov b_i, za katere je $d_i \in C$, je večje od $\frac{n}{3}$. Torej obstaja x, $1 \leq x < p$ in podmnožica $A \subset B$ z močjo $|A| > \frac{n}{3}$, tako da je $xa \pmod p \in C$ za vsak $a \in A$. Tak A je očitno prost za vsoto. Če bi obstajala števila $a_1, a_2, a_3 \in A$, za katera bi veljalo $a_1 + a_2 = a_3$, potem bi veljalo tudi $xa_1 + xa_2 \equiv xa_3 \pmod p$, kar pa je v protislovju z dejstvom, da je C za vsoto prosta podmnožica množice $\mathbb{Z}_p$.

□

1.6 Univerzalne množice

Množica A nizov oblike $\{0,1\}^n$ je (n,k)-*univerzalna*, če za vsako podmnožico $S = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ projekcija

$$A|_S = \{(a_{i_1}, a_{i_2}, \ldots, a_{i_k}) \quad | \quad (a_1, a_2, \ldots, a_n) \in A\}$$

vsebuje vse možne 2^k nize. Zanima nas, kakšna je moč najmanjše univerzalne množice A. Enostavno je videti, da velja

$$2^k \leq |A| \leq 2^n \,.$$

Boljšo zgornjo mejo nam zagotovi naslednji izrek.

Izrek 1.8 (Kleitman in Spencer, 1973) *Če velja $\binom{n}{k} 2^k (1 - 2^{-k})^r < 1$, potem obstaja (n,k)-univerzalna množica moči r.*

Dokaz. Naj bo A množica r naključno izbranih nizov oblike $\{0,1\}^n$. Naj bo S izbrana podmnožica množice $\{1, 2, \ldots, n\}$ moči k in v izbran niz oblike $\{0,1\}^k$. Velja

$$\Pr(v \notin A|_S) = \prod_{a \in A} \Pr(v \neq a|_S) = \prod_{a \in A} (1 - 2^{|S|}) = (1 - 2^{-k})^r \,.$$

Ker imamo natanko $\binom{n}{k} 2^k$ možnosti za izbiro para (S, v), množica A ni (n,k)-univerzalna z verjetnostjo kvečjemu

$$\binom{n}{k} 2^k (1 - 2^{-k})^r < 1 \,.$$

Sledi, da obstaja vsaj ena univerzalna množica z r nizi, ki je (n,k)-univerzalna. S tem je izrek dokazan.

□

Posledica 1.9 *Za $k \geq 2$ obstaja (n,k)-univerzalna množica velikost $k\,2^k \lg n$.*

Dokaz. Pokaži, da velja $\binom{n}{k}2^k(1-2^{-k})^r < 1$ z uporabo neenakosti $\binom{n}{k} < \left(\frac{en}{k}\right)^k$ in $(1-2^{-k})^r < e^{-\frac{r}{2^k}}$. Potem dokaz sledi po izreku 1.8.

$\square$

Poglavje 2

Linearnost matematičnega upanja

2.1 Število fiksnih točk permutacije

Permutacija končne množice A je bijektivna preslikava iz množice A nase. Brez škode za splošnost lahko elemente množice A označimo z naravnimi števili $\{1, 2, \ldots, n\}$. Taki permutaciji rečemo, da je *reda* n. Množico vseh permutacij reda n označimo z S_n. Velja $|S_n| = n!$. Če za permutacijo σ obstaja $i \in \{1, 2, \ldots, n\}$, pri čemer $\sigma(i) = i$, potem točki i pravimo *fiksna točka permutacije* σ. Število fiksnih točk je očitno med 0 in n.

Zanima nas pričakovano število fiksnih točk v naključno izbrani permutaciji.

Izrek 2.1 *V povprečju ima vsaka permutacija* 1 *fiksno točko.*

Dokaz. Izračunajmo verjetnost pričakovanega števila fiksnih točk slučajne permutacije σ na $\{1, \ldots, n\}$. Če je

$$F(\sigma) = |\{i : \sigma(i) = i\}|,$$

lahko to izrazimo kot vsoto indikatorskih spremenljivk:

$$F(\sigma) = \sum_{i=1}^{n} F_i(\sigma),$$

kjer je $F_i(\sigma) = 1$, če je $\sigma(i) = i$, sicer pa je $F_i(\sigma) = 0$. Potem je

$$\mathbf{E}[F_i] = \Pr[\sigma(i) = i] = \frac{(n-1)!}{n!} = \frac{1}{n}$$

in od tod

$$\mathbf{E}[F] = \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = 1.$$

Torej poljubna permutacija ima v povprečju 1 fiksno točko.

□

2.2 Hamiltonove poti v turnirjih

Turnir je orientiran polni graf, kar pomeni, da med poljubnima točkama u in v nastopa natanko ena usmerjena povezava (u, v) oz. (v, u). *Hamiltonova pot* v turnirju je usmerjena pot skoti vse točke. Dobro je znano in ni težko pokazati, da ima vsak turnir Hamiltonovo pot. Naslednji izrek (Szele, 1943) nam pokaže obstoj turnirja, ki ima zelo veliko Hamiltonovih poti. Temu izreku oz. dokazu se pogosto pripisuje prva uporaba verjetnostne metode.

Izrek 2.2 *Obstaja turnir na n točkah, ki ima vsaj $\frac{n!}{2^{n-1}}$ Hamiltonovih poti.*

Dokaz. Izračunajmo pričakovano število Hamiltonovih poti v slučajnem turnirju T na n točkah, kjer ima vsaka povezava slučajno orientacijo, izbrano neodvisno z verjetnostjo $\frac{1}{2}$. Označimo točke turnirja T z elementi množice $\{1, 2, \ldots, n\}$.

Za dano permutacijo σ na $\{1, \ldots, n\}$ si oglejmo zaporedje $\sigma(1), \sigma(2), \ldots, \sigma(n)$ in označimo z I_σ indikator dogodka, da vse povezave $(\sigma(i), \sigma(i+1))$ nastopajo v T s to orientacijo. Upoštevajmo, da orientacijo različnih povezav izberemo neodvisno in izračunajmo $\mathbf{E}[I_\sigma]$:

$$\mathbf{E}[I_\sigma] = \Pr[\sigma] = \frac{1}{2^{n-1}}.$$

Naj bo X vsota vseh Hamiltonovih poti v turnirju. Sledi

$$X = \sum_{\sigma \in S_n} I_\sigma$$

in od tod

$$\mathbf{E}[X] = \sum_{\sigma} \mathbf{E}[I_\sigma] = \sum_{\sigma} \frac{1}{2^{n-1}} = \frac{1}{2^{n-1}} \sum_{\sigma} 1 = \frac{n!}{2^{n-1}},$$

saj je vseh različnih permutacij na n točkah $n!$, tj. $|S_n| = n!$. Torej obstaja tak turnir T, ki vsebuje vsaj $\frac{n!}{2^{n-1}}$ Hamiltonovih poti.

□

2.3 Maksimalni prerez grafov

Tukaj obravnavamo problem maksimalnega prereza, ki je predvsem pomemben algoritmičen problem. Imamo graf $G = (V, E)$ in želimo razdeliti množico točk v dva razreda, A in $B = V \setminus A$ tako, da je število povezav med A in B maksimalno. Naslednji izrek nam pove, da je vedno možno doseči, da je število povezav med A in B vsaj polovica vseh povezav v grafu.

Izrek 2.3 *Vsak graf z m povezavami vsebuje dvodelen podgraf z vsaj $m/2$ povezavami.*

Dokaz. Naj bo $G = (V, E)$. Izberimo slučajno podmnožico $T \subseteq V$ z vstavljanjem vsake točke v T neodvisno z verjetnostjo $\frac{1}{2}$. Za dano povezavo $e = uv$ naj I_e označuje indikatorsko spremenljivko dogodka, da je natanko ena od točk u in v v T. Potem velja

$$\mathbf{E}[I_e] = \Pr\big[(u \in T \text{ in } v \notin T) \text{ ali } (u \notin T \text{ in } v \in T)\big] = \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{2}.$$

Če X označuje število povezav, ki imajo natanko eno točko v T, potem je

$$X = \sum_{e\in E} I_e$$

in zato

$$\mathbf{E}[X] = \sum_{e\in E}\mathbf{E}[I_e] = \sum_{e\in E}\frac{1}{2} = \frac{1}{2}\sum_{e\in E}1 = \frac{m}{2},$$

saj je m število vseh povezav v grafu. Torej, za nekatere $T \subseteq V$ obstaja vsaj $\frac{m}{2}$ povezav med T in $V\setminus T$. Te povezave seveda inducirajo dvodelen podgraf.

$\square$

2.4 Uravnoteženi vektorji

Izrek 2.4 *Naj bodo $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ za katere velja $|v_i| = 1$ za vsak $i \in \{1, 2, \ldots, n\}$. Potem obstajajo taki $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$, ki lahko zavzamejo vrednosti 1 ali -1, da velja*

$$|\varepsilon_1 v_1 + \ldots + \varepsilon_n v_n| \leq \sqrt{n}$$

in taki, da velja

$$|\varepsilon_1 v_1 + \ldots + \varepsilon_n v_n| \geq \sqrt{n}.$$

Dokaz. Naj bodo $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ izbrani enakomerno in neodvisno iz množice $\{1, -1\}$. In naj bo

$$X = |\varepsilon_1 v_1 + \ldots + \varepsilon_n v_n|^2.$$

Potem je

$$X = \sum_{i=1}^{n}\sum_{j=1}^{n}\varepsilon_i v_i \cdot \varepsilon_j v_j,$$

kar zapišemo malo drugače

$$X = \sum_{i=1}^{n} \sum_{j=1}^{n} \varepsilon_i \varepsilon_j v_i \cdot v_j.$$

Tako je zaradi linearnosti matematičnega upanja

$$\mathbf{E}[X] = \sum_{i=1}^{n} \sum_{j=1}^{n} v_i \cdot v_j \mathbf{E}[\varepsilon_i \varepsilon_j].$$

Če je $i \neq j$, potem je

$$\mathbf{E}[\varepsilon_i \varepsilon_j] = \mathbf{E}[\varepsilon_i] \mathbf{E}[\varepsilon_j] = 0.$$

Če pa je $i = j$, je $\varepsilon_i^2 = 1$ in zato je

$$\mathbf{E}[\varepsilon_i^2] = 1.$$

Tako je

$$\mathbf{E}[X] = \sum_{i=1}^{n} v_i v_i = n.$$

Od tod sledi, da obstajajo taki $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$, katerih zaloga vrednosti je $\{1, -1\}$ in je $X \geq n$ in taki, da je $X \leq n$. Ko te neenakosti korenimo, dobimo ravno to kar smo želeli dokazati.

$\square$

Izrek 2.5 *Naj bodo $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ za katere velja $|v_i| = 1$ za vsak $i \in \{1, 2, \ldots, n\}$. Naj bodo $p_1, p_2, \ldots, p_n \in [0, 1]$ poljubni in naj bo $w = p_1 v_1 + p_2 v_2 + \ldots + p_n v_n$. Potem obstajajo taki $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{0, 1\}$, da za $v = \varepsilon_1 v_1 + \ldots + \varepsilon_n v_n$ velja*

$$|w - v| \leq \frac{\sqrt{n}}{2}.$$

Dokaz. Izberimo vsak ε_i neodvisno z verjetnostjo

$$\Pr[\varepsilon_i = 1] = p_i \quad \text{in} \quad \Pr[\varepsilon_i = 0] = 1 - p_i.$$

Naključna izbira ε_i nam da slučajno spremenljivko v. Sedaj si oglejmo slučajno spremenljivko

$$X = |w - v|^2,$$

za katero velja:

$$\begin{aligned} X &= |\sum_{i=1}^{n}(p_i - \varepsilon_i)v_i|^2 \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n}(p_i - \varepsilon_i)v_i\,(p_j - \varepsilon_j)v_j \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} v_i \cdot v_j (p_i - \varepsilon_i)(p_j - \varepsilon_j). \end{aligned}$$

Zato je

$$\mathbf{E}[X] = \sum_{i=1}^{n}\sum_{j=1}^{n} v_i \cdot v_j \mathbf{E}[(p_i - \varepsilon_i)(p_j - \varepsilon_j)].$$

Če je $i \neq j$, potem sta slučajni spremenljivki $p_i - \varepsilon_i$ in $p_j - \varepsilon_j$ neodvisni in zato velja

$$\mathbf{E}[(p_i - \varepsilon_i)(p_j - \varepsilon_j)] = \mathbf{E}[(p_i - \varepsilon_i)]\mathbf{E}[(p_j - \varepsilon_j)] = 0.$$

Za $i = j$ pa je

$$\mathbf{E}[(p_i - \varepsilon_i)^2] = p_i(p_i - 1)^2 + (1 - p_i)p_i^2 = p_i(1 - p_i) \leq \frac{1}{4}.$$

Torej je

$$\mathbf{E}[X] = \sum_{i=1}^{n} p_i(1 - p_i)|v_i|^2 \leq \frac{1}{4}\sum_{i=1}^{n}|v_i|^2 = \frac{n}{4}.$$

$\square$

Poglavje 3

Slučajni grafi

3.1 Pojem slučajnega grafa

Naj bo V množica vozlišč z n elementi. Naš cilj je spremeniti množico $\mathcal{G}$ vseh grafov na V v verjetnostni prostor in potem poskusiti odgovoriti na najbolj tipično zastavljeno vprašanje o slučajnih objektih, ki sprašuje, kakšna je verjetnost, da ima nek graf $G \in \mathcal{G}(n,p)$ to ali ono lastnost.

Lahko je videti, da graf G zgradimo naključno tako, da se za vsako povezavo $e \in V \times V$ naključno odločimo ali je oziroma ni vsebovana v grafu G. Te odločitve so izvedene neodvisno, verjetnost dogodka, da je e povezava grafa G, pa je enaka $p \in [0,1]$.

Naj bo G_0 nek graf na množici vozlišč V z m povezavami. Verjetnost, da ga bomo izbrali, je enaka

$$p^m(1-p)^{\binom{n}{2}-m}.$$

Torej je za vsak izbran graf G verjetnost, da je G enak G_0, enaka zgornji. Verjetnost, da je G izomorfen G_0, bo seveda precej večja. Če so verjetnosti vseh elementarnih dogodkov določene na tak način, je na tak način določena tudi mera želenega prostora $\mathcal{G}(n,p)$. Preveriti je potrebno, da verjetnostna mera na $\mathcal{G}(n,p)$, ki se pojavi za vsako povezavo neodvisno z verjetnostjo p, obstaja.

Naj bo $\Omega_e = \{0_e, 1_e\}$ verjetnostni prostor za vsako povezavo $e \in V \times V$. Definirajmo verjetnosti $\mathrm{Pr}_e(\{1_e\}) = p$ in $\mathrm{Pr}_e(\{0_e\}) = q$, da povezava je oziroma ni v grafu (verjetnosti elementarnih dogodkov prostora Ω_e). Za verjetnostni prostor $\mathcal{G}(n,p)$ vzemimo produktni prostor

$$\Omega = \prod_{e \in V \times V} \Omega_e.$$

Element Ω je preslikava ω, ki vsaki povezavi $e \in V \times V$ priredi 0_e ali 1_e. Verjetnostna mera P na Ω pa je produktna mera vseh Pr_e. V praksi to pomeni, da ω predstavlja graf G na n vozliščih s povezavami

$$E(G) = \{e \mid \omega(e) = 1_e\}.$$

Grafu G pravimo *slučajni graf* na V z verjetnostjo povezave p. Vsako množico grafov na V si v prostoru $\mathcal{G}(n,p)$ lahko predstavljamo kot dogodek. Ali drugače, za vsako povezavo $e \in V \times V$ je množica

$$A_e = \{\omega \mid \omega(e) = 1_e\}$$

vseh grafov G na V, dogodek, da je e povezava v G. S pomočjo teh dogodkov pa lahko dokažemo prvo trditev.

Trditev 3.1 *Dogodki A_e so neodvisni in se pojavljajo z verjetnostjo p.*

Dokaz. Po definiciji je

$$A_e = \{1_e\} \times \prod_{e' \neq e} \Omega_{e'}.$$

Ker je P produktna mera vseh mer P_e, dobimo

$$\mathrm{Pr}(A_e) = p \prod_{e' \neq e} 1 = p\,.$$

Podobno, če je $\{e_1, \ldots, e_k\}$ poljubna podmnožica $V \times V$, velja

$$\begin{aligned}
\mathrm{Pr}(A_{e_1} \cap \cdots \cap A_{e_k}) &= \mathrm{Pr}(\{1_{e_1}\} \times \cdots \times \{1_{e_k}\} \times \prod_{e \notin \{e_1,\ldots,e_k\}} \Omega_e) \\
&= p^k \\
&= \mathrm{Pr}(A_{e_1}) \cdots \mathrm{Pr}(A_{e_k}).
\end{aligned}$$

$\square$

P je torej enolično določen s p in našo predpostavko, da so dogodki A_e neodvisni. Pri izračunavanju verjetnosti v prostoru $\mathcal{G}(n,p)$ zadošča operirati s tema predpostavkama in uporaba prostora ni več potrebna.

3.2 Grafovske invariante kot slučajne spremenljivke

V kontekstu slučajnih grafov lahko vsako izmed invariant grafa (npr. povprečno stopnjo, povezanost, notranji obseg, kromatično število) interpretiramo kot nenegativno slučajno spremenljivko X na $\mathcal{G}(n,p)$. Za zgled poglejmo naslednjo trditev, kako omejimo invarianto neodvisnostnega števila α grafa $G \in \mathcal{G}(n,p)$.

Lema 3.2 *Za vsa naravna števila n in k, za katere velja $n \geq k \geq 2$, je verjetnost, da $G \in \mathcal{G}(n,p)$ vsebuje množico s k neodvisnimi vozlišči, največ*

$$\Pr(\alpha(G) \geq k) \leq \binom{n}{k} q^{\binom{k}{2}}.$$

Dokaz. Verjetnost, da je neka določena množica $U \subseteq V$ z močjo k v grafu G neodvisna, je enaka $q^{\binom{k}{2}}$. Trditev nato sledi iz dejstva, da je natanko $\binom{n}{k}$ takšnih množic U.

□

Pričakovana vrednost X neke slučajne spremenljivke oz. grafovske invariante je

$$E(X) = \sum_{G \in \mathcal{G}(n,p)} \Pr(G) \cdot X(G).$$

Izračun povprečne vrednosti slučajne spremenljivke X je preprost in učinkovit način za dokaz obstoja grafa G z $X(G) < a$ za določen $a > 0$, pri čemer pa ima G neko lastnost L. Če je pričakovana vrednost X majhna, je $X(G)$ velik le za nekaj grafov iz $\mathcal{G}(n,p)$, ker je $X(G)$ nenegativna slučajna spremenljivka. Torej mora biti vrednost X majhna za večino grafov iz $\mathcal{G}(n,p)$ in lahko pričakujemo, da bomo med njimi našli nekega z želeno lastnostjo L.

Ta preprosta ideja s slučajnimi grafi je jedro številnih nekonstruktivnih dokazov obstoja objekta z določenimi lastnostmi.

Izračunajmo število pričakovanih ciklov neke dane dolžine $k \geq 3$ v slučajnem grafu $G \in \mathcal{G}(n,p)$. Naj bo $X : \mathcal{G}(n,p) \to \mathbb{N}$ slučajna spremenljivka, ki vsakemu izmed slučajnih grafov G priredi število k-ciklov v njem. Definirajmo

$$(n)_k = n(n-1)(n-2)\cdots(n-k+1).$$

To je število zaporedij k različnih elementov na množici z n elementi.

Lema 3.3 *Pričakovano število k-ciklov v $G \in \mathcal{G}(n,p)$ je*

$$E(X) = \frac{(n)_k}{2k} p^k.$$

Dokaz. Za vsak k-cikel C z vozlišči v $V = \{0, \ldots, n-1\}$ naj $X_C : \mathcal{G}(n,p) \to \{0,1\}$ predstavlja indikatorsko slučajno spremenljivko za C:

$$X_C : G \mapsto \begin{cases} 1 & C \subseteq G; \\ 0 & \text{sicer.} \end{cases}$$

Ker X_C dobi samo 1 za pozitivno vrednost, je pričakovana vrednost $E(X_C)$ enaka meri $\Pr(X_C = 1)$ množice vseh grafov v $\mathcal{G}(n,p)$, ki vsebujejo C. To pa je natanko verjetnost, da je $C \subseteq G$:

$$E(X_C) = \Pr(C \subseteq G) = p^k.$$

Takšne cikle predstavlja natanko $(n)_k$ zaporedij $v_0 v_1 \cdots v_{k-1}$ različnih vozlišč v V in vsak izmed ciklov je opisan z $2k$ takšnimi zaporedji. Torej je natanko $(n)_k/2k$ različnih ciklov. Slučajna spremenljivka X priredi vsakemu grafu G število k-ciklov, torej je X vsota vseh vrednosti $X_C(G)$ in tako dobimo:

$$E(X) = E\big(\sum_C X_C\big) = \sum_C E(X_C) = \frac{(n_k)}{2k} p^k.$$

□

Poglavje 4

Metoda izbrisa

Kot je razvidno iz prejšnih poglavij, osnovni pristop verjetnostne metode pokaže obstoj objekta z določenimi lastnosti tako, da skonstruiramo poseben verjetnostni prostor objektov in pokažemo, da želene lastnosti v tem prostoru veljajo s pozitivno verjetnostjo. Velikokrat ta direkten pristop ni uspešen. Takrat pogosto lahko pokažemo, da obstaja objekt, ki "skoraj" zadostuje našim pogojem in se ga da modificirati do želenega. Krajše povedano, metoda izbrisa obravnava slučajno konfiguracijo, ki ni "dobra" in je "slaba" le na nekaj mestih. Iz konfiguracije odstranimo par objektov in tako dobimo (manjšo) "dobro"konfiguracijo.

Preden se lotimo primerov omenimo Markovo neenakost, ki se najpogosteje uporablja v tem pristopu.

Izrek 4.1 (Markova neenakost) *Za nenegativno slučajno spremenljivko in $a > 0$ velja:*

$$P[X \geq t] \leq \frac{E(X)}{t}.$$

Dokaz.

$$E(X) = \sum_{i} i\Pr[X = i] \geq \sum_{i \geq t} t\Pr[X = i] = t\Pr[X \geq t]\,.$$

$\square$

4.1 Ramseyeva števila

Trditev 4.2 *Če $\binom{n}{k}2^{1-\binom{k}{2}} < 1$, potem $R(k,k) > n$.*

Trditev 4.3 (Spencer 1987) *Za vsak n velja: $R(k,k) > n - \binom{n}{k}2^{1-\binom{k}{2}}$.*

Dokaz. Obravnavajmo 2-barvanje povezav grafa K_n. Za množico S, s k točkami, naj bo X_S indikatorska spremenljivka za dogodek, da je S monokromatska.

$$E[X_S] = P[S \text{ je monokromatska}] = 2^{1-\binom{k}{2}}.$$

Naj bo $X = \sum_S X_S$. Potem je $E[X] = \sum_S E[X_S] = m$, pri čemer je $m = \binom{n}{k}2^{1-\binom{k}{2}}$. Torej obstaja barvanje, ki ima največ m monokromatskih k-klik, t.j. $X \leq m$. Iz vsake take klike odstranimo eno točko in dobimo ustrezno pobarvan K_s, za $s \geq n-m$. Od tod sledi $R(k,k) > s \geq n - m$.

□

4.2 Največji neodvisni podgrafi

Neodvisni podgraf grafa G je množica vozlišč iz grafa G, ki v G niso povezana. Naslednji izrek bo navzdol omejil velikost največjega neodvisnega grafa v G. Naj bo $\alpha(G)$ velikost največje neodvisne množice grafa G.

Izrek 4.4 *Naj bo G graf na n točkah z $\frac{nk}{2}$ povezavami. Potem je $\alpha(G) \geq \frac{n}{2k}$.*

Dokaz. Naj bo S slučajna podmnožica točk v grafu G. Množico S dobimo tako, da vsako točko iz grafa G izberemo z verjetnostjo p. Naj bo X število točk in Y število povezav v S.

Velja $E[X] = pn$ in $E[Y] = \frac{nk}{2}p^2$. Potem je

$$E[X - Y] = np - \frac{nk}{2}p^2.$$

Pri $p = \frac{1}{k}$, $E[X - Y]$ doseže maksimum:

$$E[X - Y] = \frac{n}{k} - \frac{n}{2k} = \frac{n}{2k}.$$

Torej obstaja množica S, ki ima vsaj $\frac{n}{2k}$ več točk kot povezav. Vsaki povezavi odstranimo eno točko in dobimo neodvisno množico z vsaj $\frac{n}{2k}$ točkami.

□

V nadaljevanju naj bo d_v stopnja vozlišča $v \in V$ za graf $G = (V, E)$.

Izrek 4.5 (Turan) *Za vsak graf G velja*

$$\alpha(G) \geq \sum_{v \in V} \frac{1}{d_v + 1}.$$

Dokaz. Naj $<$ linearno ureja V. Definirajmo

$$I = \{v \in V; \{v, w\} \in E \Rightarrow v < w\}.$$

Naj bo X_v indikator naključne spremenljivke za $v \in I$ in $X = \sum_{v \in V} X_v = |I|$. Za vsak v velja

$$E[X_v] = \Pr[v \in I] = \frac{1}{d_v + 1},$$

ker je $v \in I$ natanko tedaj, ko je v najmanjši element med v in njegovimi sosedi. Torej je

$$E[X] = \sum_{v \in V} \frac{1}{d_v + 1}$$

in torej obstaja specifično urejanje $<$ z

$$|I| \geq \sum_{v \in V} \frac{1}{d_v + 1}.$$

Toda če sta $x, y \in I$ in $\{x, y\} \in E$, potem $x < y$ in $y < x$, kar je protislovje. Torej je I neodvisen in $\alpha(G) \geq |I|$.

□

Za vsak $m \leq n$, naj q, r ustrezata $n = mq + r, 0 \leq r < m$, in naj bo

$$e = r\binom{q+1}{2} + (m - r)\binom{q}{2}.$$

Definirajmo graf $G = G_{n,e}$ na n vozliščih in e povezavah tako, da enakovredno (kolikor je to mogoče) razdelimo množico vozlišč v m razredov in združimo dve vozlišči natanko tedaj, ko ležita v istem razredu. Očitno je, da $\alpha(G_{n,e}) = m$.

Izrek 4.6 (Turan, 1941) *Naj ima H n vozlišč in e povezav. Potem je $\alpha(H) \geq m$ in $\alpha(H) = m \Leftrightarrow H \cong G_{n,e}$.*

Dokaz. $G_{n,e}$ ima $\sum_{v \in V} \frac{1}{d_v + 1} = m$, ker vsaka klika doprinese 1 k vsoti. Če fiksiramo $e = \sum_{v \in V} \frac{d_v}{2}$, je $\sum_{v \in V} \frac{1}{d_v + 1}$ minimiziran z d_v, ki so kolikor se le da blizu. Tako velja za vsak H,

$$\alpha(H) \geq \sum_{v \in V} \frac{1}{d_v + 1} \geq m.$$

Za $\alpha(H) = m$ moramo imeti enakost zgoraj na obeh straneh. Iz druge enakosti vidimo, da morajo biti d_v kolikor se le da blizu. Če predpostavimo, da je $X = |I|$ kot v prejšnjem izreku, lahko sklepamo, da je $\alpha(H) = E(X)$. Toda $\alpha(H) \geq X$ za vse vrednosti $<$, torej mora biti X konstanta. Recimo, da H ni unija klik. Potem obstajajo $x, y, z \in V$ z $\{x, y\}, \{x, z\} \in E, \{y, z\} \notin E$. Naj bo $<$ ureditev, ki se prične z x, y, z in $<'$ ista ureditev, ki pa se prične z y, z, x in naj bosta I, I' pripadajoči množici vozlišč, za katere velja, da so vsi njihovi sosedje večji. Potem sta I, I' identični, razen da $x \in I$, $y, z \notin I$, medtem ko je $x \notin I'$, $y, z \in I'$. Torej X ni konstanta. Potem iz $\alpha(H) = E[X]$ sledi, da je H unija klik in je torej $H \cong G_{n,e}$.

$\square$

Poglavje 5

Drugi moment

Čebiševo neenakost uporabljamo, kadar želimo oceniti verjetnost, da se bo slučajna spremenljivka odklonila od njenega matematičnega upanja za vsaj dano število t. Ali drugače, Čebiševa neenakost ocenjuje kakšna je verjetnost, da se slučajna spremenljivka veliko razlikuje od matematičnega upanja.

Lema 5.1 (Čebiševa neenakost) *Če ima slučajna spremenljivka X matematično upanje $\mathbf{E}[X]$ in končno varianco* Var[X], *velja za vsak pozitiven t ocena*

$$P[|X - \mathbf{E}[X]| \geq t] \leq \frac{\mathrm{Var[X]}}{t^2}.$$

Dokaz.

$$\mathrm{Var}[X] = \mathbf{E}[(X - \mathbf{E}[X])^2] \geq t^2 P[|X - \mathbf{E}[X]| \geq t]\,.$$

□

Ocena ni natančna. Če je $t^2 < \mathrm{Var}[X]$, je celo prazna, saj je tedaj njena desna stran večja od 1, verjetnost pa tako ali tako ne more biti večja od 1. Najboljši rezultat pa nam da ocena, če je X enak μ z verjetnostjo p ali enak $\mu \pm t$ z verjetnostjo $\frac{1-p}{2}$.

5.1 Ocenjevanje srednjega binomskega koeficienta

Med binomskimi koeficienti $\binom{2m}{k}$, kjer je $k = 0, 1, \ldots, 2m$, je $\binom{2m}{m}$ največji in se pogosto uporablja v različnih formulah (npr. Catalanova števila imajo enostavno enačbo z binomskimi koeficienti. Ta števila tvorijo zaporedje naravnih števil, ki se pojavljajo v mnogih preštevilskih in velikokrat rekurzivnih problemih v kombinatoriki). Metoda s pomočjo drugega momenta je preprost način s katerim navzdol omejimo koeficient $\binom{2m}{m}$. Sicer pa obstajajo tudi drugi pristopi in nekateri med njimi nam dajo celo bolj natančno oceno. Vendar je trik s Čebiševo neenakostjo bolj preprost in tudi ocena je dovolj natančna.

Trditev 5.2 *Za vsak $m \geq 1$ velja*

$$\binom{2m}{m} \geq \frac{2^{2m}}{(4\sqrt{m}+2)}.$$

Dokaz. Naj bo X naključna spremenljivka za katero velja $X = X_1+X_2+\cdots+X_{2m}$, kjer so spremenljivke X_i med seboj neodvisne in vsaka od njih doseže vrednost 0 in 1 z verjetnostjo $\frac{1}{2}$. Torej je $\mathbf{E}[X] = m$ in $\mathrm{Var}[X] = \frac{m}{2}$. Za $t = \sqrt{m}$ nam Čebiševa neenakost da naslednjo oceno:

$$P[|X-m| < \sqrt{m}] \geq \frac{1}{2}.$$

Verjetnost, da X doseže vrednost $m+k$, kjer je $|k| < \sqrt{m}$, je $\binom{2m}{m+k}2^{-2m} \leq \binom{2m}{m}2^{-2m}$, saj je $\binom{2m}{m}$ največji binomski koeficient. Torej imamo

$$\frac{1}{2} \leq \sum_{|k|<\sqrt{m}} P[X = m+k] \leq (2\sqrt{m}+1)\binom{2m}{m}2^{-2m}.$$

$\square$

5.1.1 Različne vsote

Naj bo $A = \{x_1, x_2, \ldots, x_k\}$ množica pozitivnih celih števil. Pravimo, da ima množica A različne vsote, če za vse vrste

$$\sum_{i\in S} x_i, \quad \text{kjer je} \quad S \subseteq \{1,2,\ldots,k\}$$

velja, da so si različne. Naj $f(n)$ označuje maksimalen k, za katerega obstaja množica $\{x_1, x_2, \ldots, x_k\} \subset \{1,2,\ldots,n\}$ z različnimi vsotami. Najpreprostejši primer take množice z različnimi vsotami je $\{2^i; i \leq \log_2 n\}$. Ta primer implicira $f(n) \geq 1 + (log_2 n)$.

Kako pa bi $f(n)$ lahko omejili navzgor? Erdös je obljubil 300 \$ tistemu, ki dokaže ali ovrže trditev

$$f(n) \leq \log_2 n + C,$$

kjer je C neka konstanta. Iz zgornjega vidimo, da če so vse $2^{f(n)}$ vsote različne in manj kot nk, potem

$$f(n) < nk = nf(n)$$

in tako

$$f(n) < \log_2 n + \log_2(\log_2 n) + O(1).$$

Razmišljanje z metodo drugega momenta (torej s pomočjo Čebiševe neenakosti) nam da lažjo rešitev problema in izkaže se, da tudi malo bolj natančno. Naj bo $\{x_1, x_2, \dots, x_k\} \subset \{1, 2, \dots, n\}$ množica z različnimi vsotami. Naj bodo $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$ neodvisne slučajne spremenljivke z verjetnostjo

$$P[\varepsilon_i = 1] = P[\varepsilon_i = 0] = \frac{1}{2}$$

in naj bo $X = \varepsilon_1 x_1 + \varepsilon_2 x_2 + \ldots + \varepsilon_k x_k$ (o X tudi lahko razmišljamo kot o slučajni spremenljivki). Naj bo

$$\mu = \mathbf{E}[X] = \frac{x_1 + x_2 + \ldots + x_k}{2}$$

in $\sigma^2 = \mathrm{Var}[X]$. Omejimo varianco

$$\sigma^2 = \frac{x_1^2 + x_2^2 + \ldots + x_k^2}{4} \leq \frac{n^2 k}{4}$$

in zato je

$$\sigma = \frac{n\sqrt{k}}{2}.$$

S Čebiševo neenakostjo za vsak $\lambda > 1$ velja

$$P[|X - \mu| \geq \frac{\lambda n\sqrt{k}}{2}] \leq \lambda^{-2}.$$

Po drugi strani pa

$$1 - \frac{1}{\lambda^2} \leq P[|X - \mu| < \frac{\lambda n\sqrt{k}}{2}].$$

Ampak X zavzame vrednost z verjetnostjo 0 ali 2^{-k}, ker vsoto lahko dobimo na en sam način. Tako

$$P[|X - \mu| < \frac{\lambda n\sqrt{k}}{2}] \leq 2^{-k}(\lambda n\sqrt{k} + 1)$$

in

$$n \geq \frac{2^k(1 - \lambda^{-2}) - 1}{\lambda\sqrt{k}}.$$

Medtem, ko da $\lambda = \sqrt{3}$ optimalen rezultat, nam da vsaka izbira $\lambda \geq 1$:

Izrek 5.3

$$f(n) \leq \log_2 n + \frac{1}{2}\log_2(\log_2 n) + O(1)$$

5.2 Pragovna funkcija

Vrnimo se sedaj k slučajnim grafom in razmislimo naslednje vprašanje. Kakšna je verjetnost, da graf $G(n,p)$ vsebuje trikotnik? Omenimo še, da je lastnost, da graf vsebuje trikotnik, monotona, kar pomeni, da če ima graf G neko določeno lastnost in je $G \subset H$, potem ta lastnost velja tudi za graf H. Za majhne p graf $G(n,p)$ verjetno trikotnika ne bo vseboval, medtem ko je za velike p pojav trikotnika v grafu bolj verjeten.

Naj bo T število trikotnikov v grafu $G(n,p)$. Za dano trojico točk je verjetnost, da tvorijo trikotnik p^3. Zaradi linearnosti matematičnega upanja, je pričakovano število trikotnikov

$$\mathbf{E}[T] = \binom{n}{3} p^3.$$

Če je $p(n) \ll \frac{1}{n}$, potem se pričakovana vrednost števila trikotnikov bliža 0, ko večamo n. Zato se tudi verjetnost, da nek graf $G(n,p)$ vsebuje trikotnike nagiba k 0, če je $p(n) \ll \frac{1}{n}$ pri velikih n. Po drugi strani pa, če predpostavimo, da je $p(n) \gg \frac{1}{n}$, matematično upanje števila trikotnikov narašča v neskončnost z naraščanjem n, kar pa ne pomeni, da graf $G(n,p)$ sigurno vsebuje trikotnike. Lahko se zgodi, da nekaj grafov vsebuje veliko trikotnikov in tako dvigne pričakovano vrednost. To lahko ponazorimo tudi z naslednjim življenskim primerom.

Požarno zavarovanje: Letna cena zavarovanja proti požaru na gospodinjstvo narašča. To odraža rast škode, ki jo povzroči ogenj v gospodinjstvu vsako leto. Ampak ali to pomeni, da verjetnost, da bo ogenj povzročil nesrečo, narašča? Ali to celo pomeni, če gledamo v limiti, da bo skoraj vsako gospodinjstvo gorelo vsako leto? Težko. Dvig pričakovane cene škode je posledica parih požarnih nesreč vsako leto, katerih cena se viša.

Na srečo pa se naši trikotniki ne obnašajo tako nepredvidljivo kot požarne nesreče. Za večino slučajnih grafov velja, da je število trikotnikov, ki jih vsebujejo, relativno blizu pričakovane vrednosti. Pravzaprav nam ravno ta metoda s pomočjo drugega momenta dokazuje, da če je pričakovana vrednost števila trikotnikov dovolj velika, potem slučajni graf skoraj sigurno vsebuje nekaj trikotnikov.

Lema 5.4 *Naj bodo $X_1, X_2, \ldots$ nenegativne slučajne spremenljivke za katere velja*

$$\lim_{n\to\infty} \frac{\mathrm{Var}[X_n]}{(\mathbf{E}[X_n])^2} = 0.$$

Potem

$$\lim_{n\to\infty} P[X_n > 0] = 1.$$

Dokaz. Naj bo $t = \mathbf{E}[X_n]$ in uporabimo Čebiševo neenakost:

$$P[|X_n - \mathbf{E}[X_n]| \geq \mathbf{E}[X_n]] \leq \frac{\mathrm{Var}[X_n]}{(\mathbf{E}[X_n])^2}.$$

Tako dobimo

$$\lim_{n\to\infty} P[X_n \leq 0] \leq \lim_{n\to\infty} \frac{\mathrm{Var}[X_n]}{(\mathbf{E}[X_n])^2} = 0.$$

□

Zdaj moramo oceniti varianco števila trikotnikov v grafu $G(n,p)$. Število trikotnikov T zapišemo kot $T = \sum_i T_i$, kjer so $T_1, T_2, \ldots$ indikatorske spremenljivke za vse $\binom{n}{3}$ možne trikotnike v grafu $G(n,p)$. Varianca vsote slučajnih spremenljivk je

$$\mathrm{Var}[T] = \sum_i \mathrm{Var}[T_i] + \sum_{i\neq j} \mathrm{Cov}[T_i, T_j].$$

Za vsak trikotnik velja

$$\mathrm{Var}[T_i] \leq \mathbf{E}[T_i^2] = p^3$$

in za vsak par trikotnikov, ki ima skupno eno povezavo velja

$$\mathrm{Cov}[T_i, T_j] \leq \mathbf{E}[T_i T_j] = p^5,$$

(torej sta T_i in T_j indikatorski spremenljivki dveh trikotnikov na petih določenih povezavah).

Indikatorske spremenljivke trikotnikov, ki nimajo skupne povezave, so neodvisne in je torej kovarianca takih parov enaka 0. Zato seštevamo le kovarianco tistih parov trikotnikov, ki imajo skupno povezavo. Število le teh je $12\binom{n}{4}$ in tako dobimo

$$\mathrm{Var}[T] \leq \binom{n}{3}p^3 + 12\binom{n}{4}p^5 \leq n^3p^3 + n^4p^5$$

$$\frac{\mathrm{Var}[T]}{(\mathbf{E}[T])^2} \leq \frac{n^3p^3 + n^4p^5}{(\binom{n}{3}p^3)^2} = O(\frac{1}{n^3p^3} + \frac{1}{n^2p}),$$

kar limitira proti 0, če je $p(n) \gg \frac{1}{n}$. Po lemi 5.4 pa iz tega sledi, da se verjetnost, da graf $G(n,p)$ vsebuje trikotnike, približuje 1 z naraščanjem n proti neskončnosti.

Lastnost, ali graf vsebuje trikotnik, lahko preverimo tudi s pomočjo pragovne funkcije. Ta pojem sta vpeljala Erdös in Rényi.

Preden pa definiramo pragovno funkcijo, ponovimo še kaj pomeni, da je lastnost A monotona. Naj bosta G in H grafa, za katera velja $V(H) = V(G)$ in $E(H) \subseteq E(G)$. Lastnost A je monotona, če velja: H ima lastnost A, potem sledi, da ima lastnost A tudi G.

Definicija 5.5 Funkcija $r : \mathbb{N} \to R$ je *pragovna funkcija* za monotono lastnost A grafa $G(n,p)$, če za vsak $p : \mathbb{N} \to [0,1]$ velja:

1. $p(n) \ll r(n) \Rightarrow \lim_{n\to\infty} P[A \text{ velja za } G(n,p(n))] = 0$,

2. $r(n) \ll p(n) \Rightarrow \lim_{n\to\infty} P[A \text{ velja za } G(n,p(n))] = 1$.

Pragovna funkcija lahko obstaja lahko pa tudi ne. Tudi če že obstaja, ni nujno, da je enolično določena. Na primer za našo lastnost, da $G(n,p)$ vsebuje trikotnik, je pragovna funkcija $r(n) = 1/n$. Vendar pa bi lahko namesto tega zapisa uporabili tudi $r(n) = c/n$ (za vsak $c > 0$).

Lahko pa bi se ukvarjali tudi s pragovno funkcijo bolj splošnih lastnosti, kot je na primer pojav podgrafa v grafu $G(n,p)$ (vendar ne nujno induciranega, saj je ta problem veliko bolj zapleten). Izkaže se, da je naš ukrep primeren tudi za bolj splošne lastnosti podgrafa, pod pogojem, da je ta uravnotežen. Preden pa povemo kaj je uravnotežen graf, pa definirajmo še gostoto grafa.

Naj bo H graf z v vozlišči in e povezavami. Definiramo *gostoto* grafa H kot

$$\rho(H) = \frac{e}{v}.$$

Grafu H rečemo, da je uravnotežen, če noben njegov podgraf nima večje gostote kot graf H sam.

Izrek 5.6 *Naj bo H uravnotežen graf z gostoto ρ. Potem je $r(n) = n^{\frac{-1}{\rho}}$ pragovna funkcija za lastnost, da je H podgraf grafa $G(n,p)$.*

Poglavje 6

Lovaszeva lokalna lema

6.1 Lokalna in simetrična lokalna lema

Običajno je cilj verjetnostne metode pokazati, da se s pozitivno verjetnostjo ne zgodi nič "slabega". Ponavadi imamo neke slabe dogodke $A_1, A_2 \ldots, A_n$, ki se jim poskušamo izogniti, recimo enobarvne povezave pri barvanju (hiper)grafa. Vemo, da je $\Pr(A_1 \cup A_2 \cup \cdots \cup A_n) \leq \sum \Pr(A_i)$. Če je vsota $\sum \Pr(A_i)$ strogo manjša od 1, potem je očitno, da se s pozitivno verjetnostjo nobeden od teh dogodkov ne zgodi. Sicer pa v praksi v veliki večini primerov ta pristop ni uporaben, ker je lahko vsota $\sum \Pr(A_i)$ veliko večja kot $\Pr(A_1 \cup A_2 \cup \cdots \cup A_n)$.

Poseben primer, pri katerem smo bolj uspešni je, kadar so dogodki $A_1, \ldots, A_n$ neodvisni in netrivialni. Tedaj velja, da je

$$\begin{aligned}
\Pr(A_1 \cup A_2 \cup \cdots \cup A_n) &= 1 - \Pr(\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n) \\
&= 1 - \Pr(\bar{A}_1)\Pr(\bar{A}_2) \cap \cdots \cap \Pr(\bar{A}_n) \\
&> 0.
\end{aligned}$$

Zadnja neenakost sledi iz tega, da so vsi A_i netrivialni.

Pričakovati je, da nekaj podobnega velja tudi, če so dogodki le "skoraj neodvisni". V nadaljevanju bomo potrebovali naslednji dve definiciji. Dogodek A je *neodvisen* od dogodkov $B_1, \ldots, B_k$, če za vsako podmnožico $J \subseteq \{1, 2, \ldots, k\}$ velja:

$$\Pr(A \cap \bigcap_{j \in J} B_j) = \Pr(A)\Pr(\bigcap_{j \in J} B_j).$$

Naj bodo $A_1, \ldots, A_n$ dogodki v verjetnostnem prostoru. Usmerjeni graf G z vozlišči $\{1, \ldots, n\}$ imenujemo *odvisnostni* graf, če je dogodek A_i neodvisen od vseh dogodkov A_j, za katere $(i, j) \notin E(G)$. Pri tem velja opozoriti, da odvisnostni graf ni enolično določen.

Oglejmo si najprej splošno asimetrično obliko Lovaszove lokalne leme:

Izrek 6.1 (Asimetrična Lovaszova lokalna lema) *Naj bodo $A_1, \dots, A_n$ dogodki ter $D = (V, E)$ odvisnostni graf teh dogodkov. Za vsa števila $i \in \{1, \dots, n\}$ naj bodo $x_i \in [0, 1)$ realna števila, za katera velja:*

$$\Pr(A_i) \leq x_i \prod_{(i,j) \in E} (1 - x_j).$$

Potem velja

$$\Pr(\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n) \geq \prod_{i=1}^{n} (1 - x_i) > 0.$$

Dokaz. Komplementarni dogodki $\bar{A}_i$ se sicer zgodijo s pozitivno verjetnostjo, vendar želimo, da se s pozitivno verjetnostjo zgodijo sočasno. To ne bo mogoče, če kombinacija dogodkov $\bar{A}_j$ zahteva, da se zgodi nek dogodek A_i $(i \neq j)$. Zato moramo omejiti verjetnost dogodka A_i pri pogoju, da se ostali dogodki niso zgodili. Najprej za poljubno podmnožico $S \subset \{1, 2, \dots, n\}$ in $i \notin S$ pokažemo, da je

$$\Pr(A_i | \cap_{j \in S} \bar{A}_j) \leq x_i.$$

To pokažemo z indukcijo po velikosti množice S. Za $S = \emptyset$ trditev drži po privzetku izreka:

$$\Pr(A_i) \leq x_i \prod_{(i,j) \in E} (1 - x_j) \leq x_i.$$

Privzemimo, da zgornja trditev velja za poljubno množico S', $|S'| < |S|$, torej velja za množici $S_1 = \{j \in S : (i, j) \in E\}$ in $S_2 = S \setminus S_1$. Privzamemo lahko, da $S_1 \neq \emptyset$, sicer trditev trivialno sledi, saj je A_i neodvisna od $\cap_{j \in S} \bar{A}_j$. Velja

$$P\big(A_i | \bigcap_{j \in S} \bar{A}_j\big) = \frac{P\big(A_i \cap \bigcap_{j \in S_1} \bar{A}_j | \bigcap_{l \in S_2} \bar{A}_l\big)}{P\big(\bigcap_{j \in S_1} \bar{A}_j | \bigcap_{l \in S_2} \bar{A}_l\big)}.$$

Ker je A_i neodvisen od dogodkov $\{A_l : l \in S_2\}$, lahko omejimo:

$$P\big(A_i \cap \bigcap_{j \in S_1} \bar{A}_j | \bigcap_{l \in S_2} \bar{A}_l\big) \leq P\big(A_i | \bigcap_{l \in S_2} \bar{A}_l\big) = \Pr(A_i) \leq x_i \prod_{(i,j) \in E} (1 - x_j).$$

Naj bo $S_1 = \{j_1, j_2, \dots, j_r\}$. Potem po indukcijski predpostavki lahko omejimo tudi:

$$\begin{aligned}
P\big(\bar{A_{j_1}} \cap \dots \cap \bar{A_{j_r}} \big| \bigcap_{l \in S_2} \bar{A_l}\big) &= P\big(\bar{A_{j_1}} \big| \bigcap_{l \in S_2} \bar{A_l}\big) P\big(\bar{A_{j_2}} | \bar{A_{j_1}} \cap \bigcap_{l \in S_2} \bar{A_l}\big) \\
&\quad \cdots P\big(\bar{A_{j_r}} | \bar{A_{j_1}} \cap \dots \cap A_{j_{r-1}}^{-} \cap \bigcap_{l \in S_2} \bar{A_l}\big) \\
&\geq (1 - x_{j_1})(1 - x_{j_2}) \cdots (1 - x_{j_r}) \\
&\geq \prod_{(i,j) \in E} (1 - x_j).
\end{aligned}$$

Torej je $P\big(A_i \big| \bigcap_{j \in S} \bar{A_j}\big) \leq x_i$ in zato:

$$P\big(\bigcap_{i=1}^{n} \bar{A_i}\big) = \Pr(\bar{A_1}) \Pr(\bar{A_2} | \bar{A_1}) \cdots \Pr(\bar{A_n} | \bar{A_1} \cap \dots \cap A_{n-1}^{-}) \geq \prod_{(i=1}^{n} (1 - x_i).$$

□

Izrek 6.2 (Simetrična Lovaszova lokalna lema) *Naj bodo $A_1, A_2, \dots, A_n$ dogodki, za katere je $\Pr(A_i) \leq p$. Naj za vsak $i = 1, 2, \dots, n$ velja, da je A_i neodvisen od A_j za vsak $j \neq i$, razen za največ d dogodkov A_j (torej največ d dogodkov A_j je odvisnih od dogodka A_i, $(j \neq i)$). Če je $ep(d+1) \leq 1$ (kjer je e osnova naravnega logaritma), potem je*

$$P\big(\bigcap_{i=1}^{n} \bar{A_i}\big) > 0.$$

Dokaz. Če je $d = 0$, so dogodki med seboj neodvisni in zato velja $\mathrm{P}\big(\bigcap_{i=1}^{n} \bar{A_i}\big) = \mathrm{P}(\bar{A_1}) \mathrm{P}(\bar{A_2}) \cdots \mathrm{P}(\bar{A_n}) > 0$.

Naj bo $x_i = \frac{1}{d+1} < 1$. V odvisnostnem grafu je izhodnja stopnja vsakega vozlišča največ d, zato velja:

$$x_i \prod_{(i,j) \in E} (1 - x_j) \geq \frac{1}{d+1} (1 - \frac{1}{d+1})^d \geq \frac{1}{e(d+1)} \geq p.$$

Po asimetrični lovaszovi lokalni lemi velja $\mathrm{P}\big(\bigcap_{i=1}^{n} \bar{A_i}\big) \geq \prod_{i=1}^{n} (1 - x_i) > 0$.

□

6.2 Barvanje hipergrafov

Pokazali smo že, da so *k-uniformni* hipergrafi z manj kot 2^{k-1} povezavami *2-obarvljivi*. Sedaj pa bomo s pomočjo simetrične Lovasz-eve lokalne leme dokazali podobni rezultat, ki velja za hipergrafe s poljubnim številom povezav, ki pa ne smejo biti preveč incidenčne.

Izrek 6.3 *Naj bo $\mathcal{H}$ hipergraf, v katerem ima vsaka povezava vsaj k točk in je incidenčna z največ d drugimi povezavami. Če je $e(d+1) \leq 2^{k-1}$, potem je $\mathcal{H}$ 2-barvljiv.*

Dokaz. Točke grafa $\mathcal{H}$ pobarvajmo (slučajno) z rdečo ali modro barvo, z verjetnostjo $1/2$. Za vsako povezavo f naj A_f označuje dogodek, da je f enobarvna. Ker ima vsaka povezava vsaj k točk, je verjetnost dogodka A_f največ $\frac{2}{2^k} = 2^{1-k}$. Očitno je dogodek A_f neodvisen od A_g, razen tistih, kjer se f in g sekata (teh je največ d).

Poglejmo, koliko je $e \ \mathrm{P}(A_f)\ (d+1)$. Po predpostavki je $e(d+1) \leq 2^{k-1}$, zato je $\mathrm{P}(A_f)\ e\ (d+1) \leq 2^{1-k}\ 2^{k-1} = 1$. Torej lahko uporabimo Lovaszovo lokalno lemo, ki v tem primeru pravi: verjetnost, da nobena povezava ni enobarvna je večja od 0.

□

6.3 Izpolnjivost SAT problema

Izrek 6.4 *Naj bo $\mathcal{F}$ primerek k-SAT problema tak, da se vsaka spremenljivka pojavi v največ $\frac{2^{k-2}}{k}$ stavkov. Potem je $\mathcal{F}$ izpolnjiv.*

Dokaz. Naj bodo $x_1, x_2, \ldots, x_n$ spremenljivke, za katere velja $x_i \in \{T, F\}$, $i = 1, 2, \ldots, n$, vsaka vrednost pa je izbrana z verjetnostjo $p = \frac{1}{2}$. Naj bo A_i dogodek, da je i-ti stavek nepravilen (ima vrednost F), $i = 1, 2, \ldots, m$ (m stavkov). Verjetnost dogodka A_i je enaka verjetnosti, da imajo vse spremenljivke oziroma njihove negacije v i-tem stavku vrednost F. Torej velja $\Pr(A_i) = 2^{-k} = p$.

Izračunajmo še največjo izhodno stopnjo odvisnostnega grafa. V i-tem stavku se pojavi k spremenljivk, vsaka od njih pa se pojavi v največ $\frac{2^{k-2}}{k}$ stavkih. Torej je od tega stavka (in posledično dogodka A_i) odvisnih največ $k\frac{2^{k-2}}{k} = 2^{k-2}$ preostalih stavkov (dogodkov). Tako velja $d \leq 2^{k-2}$.

Sedaj izračunamo $4pd \leq 4\ 2^{-k}\ 2^{k-2} = 1$ in po simetrični Lovaszevi lokalni lemi velja $\Pr(\bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_m) > 0$, kar pomeni, da je verjetnost, da je k-SAT problem rešljiv, pozitivna.

□

6.4 Seznamsko barvanje vozlišč

Izrek 6.5 *Naj bo G tak graf, da ima vsaka točka seznam dopustnih barv velikosti $l > 0$. Za vsako točko v in vsako barvo c velja, da je c vsebovana v največ $l/8$*

seznamov od sosedov točke v. Potem obstaja pravilno barvanje tako, da vsaka točka dobi barvo iz svojega seznama.

Dokaz. Graf pobarvajmo slučajno, tako da vsako točko v pobarvamo s poljubno barvo iz njenega seznama barv L_v. Pri tem je vsaka izmed barv seznama izbrana z enako verjetnostjo $\frac{1}{l}$. Za vsako povezavo $e = (u, v) \in E(G)$ in barvo $c \in L_u \cap L_v$ definirajmo dogodek $A_{c,e}$, da sta obe krajišči povezave obarvani z barvo c.

Najprej izračunajmo verjetnost dogodka $A_{c,e}$: $\Pr(A_{c,e}) = \frac{1}{l^2} = p$, saj barve izbiramo enakomerno iz obeh seznamov krajišč povezave e. Opazimo, da je dogodek $A_{c,e}$ odvisen le od barv s seznamov L_u in L_v. Tako so od $A_{c,e}$ odvisni dogodki:

- $\mathcal{E}_u = \{A_{d,f}; d \in L_u, u \text{ je krajišče povezave } f\}$,
- $\mathcal{E}_v = \{A_{d,f}; d \in L_v, v \text{ je krajišče povezave } f\}$.

Seznam L_u ima l barv, točka u pa ima največ $\frac{l}{8}$ sosedov, ki so lahko pobarvani z barvo c (imajo jo v svojem seznamu). Zato velja $|\mathcal{E}_u| \leq l\ \frac{l}{8} = \frac{l^2}{8}$. Enako velja za $|\mathcal{E}_v| \leq \frac{l^2}{8}$. Od dogodka $A_{c,e}$ je torej odvisnih največ $\frac{l^2}{8} + \frac{l^2}{8} = \frac{l^2}{4}$ dogodkov in velja $d \leq \frac{l^2}{4}$.

Velja $4dp \leq 4\ \frac{l^2}{4}\ \frac{1}{l^2} = 1$ in po simetrični Lovaszevi lemi velja

$$P\Big(\bigcap \bar{A}_{c,e};\ e = (u, v) \in E(G),\ c \in L_u \cap L_v\Big) > 0.$$

Torej s pozitivno verjetnostjo obstaja pravilno barvanje, kjer vsaka točka dobi barvo iz svojega seznama.

□

6.5 Usmerjeni cikli

Izrek 6.6 *Naj bo $D = (V, E)$ usmerjen graf z minimalno izhodno stopnjo δ in maksimalno vhodno stopnjo Δ. Potem za vsak $k \in \mathcal{N}$, za katerega velja*

$$k \leq \frac{\delta}{1 + \ln(1 + \delta\Delta)},$$

D vsebuje usmerjen cikel, dolžine deljive s k.

Dokaz. Oglejmo si podgraf digrafa D, v katerem je izhodna stopnja vsake točke natanko δ. Naj bo $f : V \longrightarrow \{0, 1, \ldots, k-1\}$ naključno barvanje, ki ga dobimo tako, da za vsak $v \in V$ izberemo $f(v)$ neodvisno (in vse z enako verjetnostjo). Z $N^+(v)$ označimo množico točk $\{w : (v, w) \in E\}$ in z A_v dogodek, da nobena točka v $N^+(v)$ ni pobarvana z $f(v) + 1 \pmod k$.

Verjetnost dogodka A_v je $p = (\frac{k-1}{k})^\delta = (1 - \frac{1}{k})^\delta$. Trdimo, da je vsak A_v neodvisen od vseh A_w, za katere je

$$N^+(v) \cap (N^+(w) \cup \{w\}) = \emptyset. \tag{6.1}$$

To pomeni, da w ni naslednik od v ter w in v nimata skupnega naslednika.

Toda v je lahko naslednik od w. V tem primeru neodvisnost ni tako očitna kot sicer, toda vseeno drži: celo, če so barve vseh točk razen $N^+(v)$ že fiksne (natanko določene), bo verjetnost dogodka A_v še vedno enaka $(1 - \frac{1}{k})^\delta$.

Naj d označuje število točk w, ki ne zadošča (6.1). Potem je

$$d \leq \delta + \delta(\Delta - 1) = \delta\ \Delta.$$

Zato je $ep(d + 1) \leq e(1 - \frac{1}{k})^\delta(\delta\ \Delta + 1) \leq e^{1-\delta/k}(\delta\ \Delta + 1)$. Ko uporabimo začetno predpostavko, dobimo

$$e^{1-\delta/k}(\delta\ \Delta + 1) \leq \frac{1}{1 + \delta\ \Delta}(1 + \delta\ \Delta) = 1.$$

Torej je $ep(d+1) \leq 1$. Potem po Lovaszovi lokalni lemi sledi, da je $\mathrm{P}\left[\cap_{i \in V} \bar{A}_i\right] > 0$. To pomeni, da obstaja barvanje pri katerem za vsako točko $v \in V$ obstaja $w \in N^+(v)$, tako da je $f(w) = f(v) + 1 \pmod k$.

Če si sedaj izberemo poljubno točko $v_0 \in V$, potem lahko generiramo zaporedje $v_0, v_1, v_2, \ldots$, tako da $v_i v_{i+1} \in E$ in $f(v_{i+1}) = f(v) + 1 \pmod k$, dokler ne najdemo usmerjenega cikla v D. Glede na to, kako smo skonstruirali barvanje, mora biti dolžina cikla deljiva s k.

$\square$

Poglavje 7

Koncentracija slučajnih spremenljivk

7.1 Černova neenakost

Izrek 7.1 (Černov) *Naj bodo $X_1, \dots, X_n$ neodvisne slučajne spremenljivke, ki zavzamejo vrednosti -1 ali 1, obe z verjetnostjo $\frac{1}{2}$. Naj bo $X = X_1 + \cdots + X_n$. Potem za vsak realen $t \geq 0$ velja*

$$P(X \geq t) < e^{-t^2/2\sigma^2} \quad in \quad P(X \leq -t) < e^{-t^2/2\sigma^2},$$

kjer je $\sigma = \sqrt{\mathrm{var}(X)} = \sqrt{n}$.

Dokaz. Dokažimo le prvo neenakost, druga bo namreč sledila iz simetrije. Definirajmo novo slučajno spremenljivko $Y = e^{uX}$, kjer je $u > 0$ realni parameter (za zdaj še nedoločen). Potem velja $P[X \geq t] = P[Y \geq e^{ut}]$. Po Markovi neenakosti velja $P[Y \geq q] \leq \frac{E[Y]}{q}$. Računajmo

$$E[Y] = E[e^{u\sum_{i=1}^n X_i}] = E[\prod_{i=1}^n e^{uX_i}] = \prod_{i=1}^n E[e^{uX_i}]$$

(zaradi neodvisnosti X_i)

$$= \left(\frac{e^u + e^{-u}}{2}\right)^n \leq e^{nu^2/2}.$$

Zadnja ocena sledi iz neenakosti $\frac{e^x+e^{-x}}{2} = \cosh x \leq e^{x^2/2}$, ki velja za vsa realna števila x (obe strani razvijemo v Taylorjevo vrsto in primerjamo koeficiente). Potem je

$$P[Y \geq e^{ut}] \leq \frac{E[Y]}{e^{ut}} \leq e^{nu^2/2-ut}.$$

Zadnji izraz je minimiziran za $u = \frac{t}{n}$, od koder sledi $e^{-t^2/2n} = e^{-t^2/2\sigma^2}$.

$\square$

Izrek 7.2 *Naj bodo $X_1, \ldots, X_n$ neodvisne slučajne spremenljivke, ki zavzamejo vrednosti 1 z verjetnostjo p in 0 z verjetnostjo $1-p$. Naj bo $X = X_1 + \cdots + X_n$. Potem za vsak $0 \leq t \leq np$ velja*

$$P(|X - np| > t) < 2e^{-t^2/3np}.$$

Če je $t > np$ je običajno dovolj uporabiti naslednjo oceno:

$$P(|X - np| > t) < P(|X - np| > np) < 2e^{-np/3}.$$

Naj bo X množica z n točkami in naj bo $\mathcal{F}$ družina podmnožic množice X. Radi bi pobarvali točke množice X z rdečo in modro barvo tako, da vsaka množica družine $\mathcal{F}$ vsebuje uravnoteženo število točk modre in rdeče barve (uravnoteženo barvanje). Naj ima rdeča barva vrednost $+1$ in modra vrednost -1. Barvanje podamo s preslikavo $\psi : X \to \{-1, +1\}$. Za poljubno množico $S \in \mathcal{F}$ določa $\psi(S) = \sum_{x \in S} \psi(x)$ razliko med številom rdečih in modrih točk. Zanima nas barvanje ψ, pri katerem je največja razlika med številom modrih in rdečih točk v množicah družine $\mathcal{F}$ minimalna:

$$urb(\mathcal{F}) = \min_{\psi} \max_{S \in \mathcal{F}} |\psi(S)|.$$

Trditev 7.3 *Naj bo $|X| = n$ in $|\mathcal{F}| = m$. Potem velja* $\mathrm{urb}(\mathcal{F}) \leq \sqrt{2n \ln(2m)}$. *Če je maksimalno število množic v $\mathcal{F}$ največ s, potem velja* $\mathrm{urb}(\mathcal{F}) \leq \sqrt{2s \ln(2m)}$.

Dokaz. Naj bo $\psi : X \to \{-1, +1\}$ slučajno barvanje množice X, kjer so barve točk izbrane enotno in neodvisno. Za vsako fiksno množico $S \subseteq X$ je $\psi(S) = \sum_{x \in S} \psi(x)$ vsota $|S|$ neodvisnih slučajnih ± 1 spremenljivk. Po Černovi neenakosti velja:

$$P[|\psi(S)| > t] < 2e^{-t^2/2|S|} \leq 2e^{-t^2/2s}.$$

Za $t = \sqrt{2s \ln(2m)}$, $2e^{-t^2/2s}$ postane $\frac{1}{m}$. Torej s pozitivno verjetnostjo slučajno barvanje zadošča $|\psi(S)| \leq t$ za vse $S \in \mathcal{F}$.

□

7.2 Talagrandova neenakost

Izrek 7.4 (enostavna meja koncentracije) *Naj bo X slučajna spremenljivka določena z n neodvisnimi poskusi $T_1, T_2, \ldots, T_n$ ter naj velja, da*

(1) *sprememba izida kateregakoli poskusa T_i spremeni X za največ c (ponavadi majhno število),*

potem je

$$P(|X - E[X]| > t) < 2e^{-t^2/2c^2n}.$$

Naj bo

$$T_i = \begin{cases} 0 & p = 1/2 \\ 1 & p = 1/2. \end{cases}$$

ter naj bo $B = \Sigma_{i=1}^{n} T_i$. Potem je $E[B] = \frac{n}{2}$ in po Izreku 7.4 dobimo:

$$P(|B - \frac{n}{2}| > t) < 2e^{-t^2/2n},$$

pri čemer velja, da sprememba izida kateregakoli poskusa T_i spremeni X za največ 1 ($c = 1$).

Naj bo $A = nT_n$, t.j.

$$T_i = \begin{cases} 0 & p = 1/2 \\ n & p = 1/2, \end{cases}$$

V tem primeru pogoj (1) ne velja, t.j. za poljuben c obstaja poskus T_k, $k > c$ katerega sprememba izida spremeni X za več kot c.

Sicer podobno kot pri spremenljivki B, velja $E[A] = \frac{n}{2}$, vendar:

$$P(|A - E[A]| \geq \frac{n}{2}) = 1.$$

Enostavna meja koncentracije ne da dobrih rezultatov pri binomsko porazdeljenih slučajnih spremenljivkah $b(n, p)$, ko je $p = o(1)$. Na primer, če je $p = n^{-1/2}$ z enostavno mejo koncentracije dobimo naslednjo oceno:

$$P(|b(n,p) - np| > \frac{1}{2}np) < 2e^{-\frac{1}{16}},$$

ki pa je veliko slabša od ocene, ki jo dobimo s Černovo neenakostjo:

$$P(|b(n,p) - np| > \frac{1}{2}np) < 2e^{-\frac{\sqrt{n}}{12}}.$$

Včasih potrebujemo rezultat naslednjega tipa:

$$P(|X - E[X]| > \alpha E[X]) < e^{-\beta E[X]}.$$

V takem primeru uporabimo enostavno mejo koncentracije, če je $E[X] \geq cn$. Sicer pa uporabimo Talagrandovo neenakost, ki da dobre ocene tudi, ko je $E[X] = o(n)$.

Izrek 7.5 (Talagrandova neenakost) *Naj bo $X \neq 0$ nenegativna slučajna spremenljivka določena z n neodvisnimi poskusi $T_1, T_2, \ldots, T_n$ in naj obstajata (majhna) $c, r > 0$ tako, da:*

(1) *sprememba poljubnega poskusa T_i spremeni X za največ c,*

(2) *če je $X \geq s$, potem obstaja $r \cdot s$ poskusov, katerih izidi nam zagotovijo, da je $X \geq s$.*

Za $0 \leq t \leq E[X]$ potem velja

$$P(|X - E[X]| > t + 60c\sqrt{rE[X]}) \leq 4e^{-\frac{t^2}{8c^2rE[X]}}.$$

V praksi sta c in r majhna in velja $t \gg \sqrt{E[X]}$. Od tod dobimo naslednjo poenostavitev:

$$P(|X - E[X]| > t) \leq 2e^{\frac{-\beta t^2}{E[X]}}.$$

Za boljši občutek si oglejmo naslednji primer. Naj bo G graf z $v = |V(G)|$ številom vozlišč. Izberimo slučajni podgraf $H \subseteq G$ tako, da vsako povezavo izberemo z verjetnostjo p. Z X označimo število točk, ki so krajišča teh povezav. Ali je X skoncentrirana?

Černove neenakosti v tem primeru ne moremo uporabiti. Pogoj (1) enostavne meje koncentracije je izpolnjen za $c = 2$, vendar pa je $E(X) \leq v$, medtem ko je število povezav v grafu G in zato število poskusov reda v^2. Zato nam enostavna meja koncentracije ne da dobre ocene. Pogoj (1) pri Talagrandovi neenakosti je prav tako izpolnjen pri $c = 2$. Za izpolnitev pogoja (2) pa izberemo s povezav (poskusov), ki pokrivajo vsaj s različnih vozlišč grafa G. Potem lahko uporabimo Talagrandovo neenakost po kateri je slučajna spremenljivka X skoncentrirana.

7.3 Koncentracija vozlišč regularnih grafov

Izrek 7.6 *Naj bo G r-regularen graf. Če konstruiramo slučajni graf H tako, da vsako povezavo iz G izberemo z verjetnostjo $\frac{1}{2}$, potem je število točk stopnje ≥ 2 skoncentrirano.*

Dokaz. Naj bo X nenegativna slučajna spremenljivka, ki označuje število točk stopnje vsaj 2. Določena je z m neodvisnimi poskusi $T_1, T_2, \ldots, T_m$, kjer je T_i poskus, v katerem je i-ta povezava grafa G izbrana z verjetnosjo $p = \frac{1}{2}$. Naj bo n število točk grafa G in velja $m = \frac{rn}{2}$.

Opazimo, da sprememba poljubnega poskusa T_i spremeni X za največ $c = 2$, saj se pri tem stopnja spremeni le dvema točkama. Če je $X \geq s$, obstaja rs poskusov, ki zagotovijo tak rezultat. Izberimo si s točk stopnje vsaj 2. Vsako tako točko določata vsaj 2 poskusa, torej je $r = 2$. Tedaj velja Talagrandova neenakost

$$P\big(|X - \mathbb{E}(X)| > t + 120\sqrt{2\mathbb{E}(X)}\big) \leq 4e^{-\frac{t^2}{64\mathbb{E}(X)}}.$$

Izračunajmo matematično upanje $\mathbb{E}(X)$. Potrebujemo verjetnost posamezne točke v, da ima stopnjo večjo od 2. To storimo na naslednji način:

$$P(d(v) \geq 2) = 1 - P(d(v) = 1) - P(d(v) = 0).$$

Izračunajmo najprej $P(d(v) = 0) = 2^{-r}$ in $P(d(v) = 1) = r2^{-r}$. Torej velja $P(d(v) \geq 2) = 1 - (1 + r)2^{-r}$, matematično upanje pa je $\mathbb{E}(X) = n(1 - (1 + r)2^{-r})$. Tako velja $\mathbb{E}(X) = O(n)$ in eksponent v Talagrandovi neenakosti ni konstanta.

$\square$

7.4 Azumova neenakost

Martingala je zaporedje $X_0, \ldots, X_m$ slučajnih spremenljivk, takih da za $0 \leq i < m$ velja

$$E[X_{i+1}|X_i, X_{i-1}, \ldots, X_0] = X_i.$$

Predstavljajmo si, da gre kockar v igralnico z X_0 denarja. V igralnici je mnogo iger na srečo. Vse igre so poštene, kar pomeni, da je njihovo matematično upanje enako 0. Igralec lahko izbere strategijo, da podvoji stavo vsakič, ko izgubi, z razlogom da bo prva zmaga pokrila vse prejšnje vložke in prinesla še dodaten dobiček v vrednosti originalnega vložka. Naj slučajna spremenljivka X_i predstavlja kockarjevo srečo v času i. Če je $X_i = a$, potem mora biti pogojna verjetnost spremenljivke X_{i+1} enaka a, torej je to martingala.

Poglejmo si preprost, a poučen primer. Predpostavimo, da slučajna spremenljivka X_n predstavlja kockarjevo srečo po n metih poštenega kovanca, kjer igralec dobi 1 evro, če pade cifra in izgubi 1 evro, če pade grb. Očitno zaporedje zadošča pogojem zgornje definicije, zato je to martingala.

Lema 7.7 *Naj bo X slučajna spremenljivka in naj velja $E[X] = 0$ in $|X| \leq 1$. Naj bo $\lambda > 0$. Potem velja*

$$E[e^{\lambda X}] \leq e^{\lambda^2/2}.$$

Dokaz. Definirajmo linerano fukcijo

$$h(x) = \frac{e^\lambda + e^{-\lambda}}{2} + \frac{e^\lambda - e^{-\lambda}}{2}x.$$

Za $x \in [-1, 1]$ velja $e^{\lambda x} \le h(x)$ ($y = h(x)$ je ravno sekanta skozi točki $x = \pm 1$ konveksne funkcije $y = e^{\lambda x}$). Velja

$$E[e^{\lambda X}] \le E[h(X)] = h(E[X]) = h(0) = \cosh(\lambda) = e^{\lambda^2/2}.$$

$\square$

Izrek 7.8 (Azumova neenakost) *Naj bo* $0 = X_0, \ldots, X_m$ *martingala za katero velja*

$$|X_{i+1} - X_i| \le 1$$

za vse $0 \le i < m$. *Naj bo* $\lambda > 0$. *Potem velja*

$$P[X_m > \lambda\sqrt{m}] < e^{-\lambda^2/2}.$$

Dokaz. Naj bo $\alpha = \frac{\lambda}{\sqrt{m}}$. Označimo $Y_i = X_i - X_{i-1}$. Iz predpostavk očitno sledi, da je $|Y_i| \le 1$ in $E[Y_i|X_{i-1}, X_{i-2}, \ldots, X_0] = 0$. Po zgornji lemi sledi

$$E[e^{\alpha Y_i}|X_{i-1}, X_{i-2}, \ldots, X_0] \le \cosh(\alpha) = e^{\alpha^2/2}.$$

Torej je

$$\begin{aligned}
E[e^{\alpha X_m}] &= E[\prod_{i=1}^{m} e^{\alpha Y_i}] \\
&= E[\left(\prod_{i=1}^{m-1} e^{\alpha Y_i}\right) E[e^{\alpha Y_m}|X_{m-1}, X_{m-2}, \ldots, X_0]] \\
&\le E[\prod_{i=1}^{m-1} e^{\alpha Y_i}]e^{\alpha^2/2} \le e^{\alpha^2 m/2}.
\end{aligned}$$

Od tod sledi

$$\begin{aligned}
P[X_m > \lambda\sqrt{m}] &= P[e^{\alpha X_m} > e^{\alpha\lambda\sqrt{m}}] \\
&< E[e^{\alpha X_m}]e^{-\alpha\lambda\sqrt{m}} \\
&\le e^{\alpha^2 m/2 - \alpha\lambda\sqrt{m}} \\
&= e^{-\lambda^2/2}.
\end{aligned}$$

$\square$

Literatura

[1] N. Alon, and J. H. Spencer, *The probabilistic method*, John Wiley & Sons, 2000.

[2] L. Cowen, *The Probabilistic Method*, lecture notes, 1995.

[3] M. Molloy, and B. Reed, *Graph Colouring and the Probabilistic Method*, Algorithms and Combinatorics, Springer-Verlag, Berlin 2002.

[4] P. Erdős, *Graph theory and probability*, Canad. J. Math. (1959) 34—38.

[5] P. Erdős, *Graph theory and probability, II*, Canad. J. Math. 13 (1961) 346-–352.

[6] J. Matoušek, J. Vondrak, *The Probabilistic Method*, lecture notes, 2002.