VERJETNOSTNA METODA: 1.DEL

Judita Plantev

13. november 2007

1 Verjetnostna metoda

Verjetnostna metoda je danes eno od najbolj močnih ter široko uporabnih orodij v kombinatoriki. Je pomembna tehnika za dokaz obstoja kombinatoričnih objektov z določenimi lastnostmi. Bazirana je na verjetnostni teoriji, ampak presenetljivo je to, da se jo lahko uporablja pri dokazovanju izrekov, ki nimajo ničesar skupnega z verjetnostjo.

Razvil jo je znani madžarski matematik Paul Erdös, ter jo začel uspešno uporabljati v teoriji grafov, kombinatoriki, diskretni geometriji, itn. Paul Erdös je prispeval tako veliko k razvoju verjetnostne metode, da jo nekateri poimenujejo "Erdös-eva metoda".

Osnovno verjetnostno metodo lahko opišemo takole: Radi bi dokazali obstoj kombinatoričnega objekta z določenimi lastnostmi. Včasih ne moremo eksplicitno skonstruirati tega objekta, kar pravzaprav niti ni potrebno. Želimo le dokazati, da obstaja takšen objekt. Skonstruiramo primeren verjetnostni prostor in pokažemo, da ima slučajno izbran element tega prostora željene lastnosti s pozitivno verjetnostjo.

Slučajni graf je graf, ki mu na dani množici vozlišč naključno določimo povezave. Povezave določamo neodvisno med seboj.

Definicija 1.0.1 ***(Slučajni grafi)*** *Verjetnostni prostor slučajnih grafov $G(n,p)$ je končni verjetnostni prostor, katerega elementarni dogodki so grafi na fiksni množici n točk, in kjer je verjetnost grafa z m povezavami enaka*

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

To ustreza ustvarjanju slučajnega grafa z vključitvijo vsake potencialne povezave neodvisno z verjetnostjo p. Za $p = \frac{1}{2}$ si lahko zamislimo metanje kovanca za vsako potencialno povezavo, da odločimo, če naj nastopi v grafu.

1.1 Ramseyeva števila

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

Definicija 1.1.1 ***Ramseyevo število*** $R(k, l)$ *je*

$$\begin{aligned} R(k,l) &= min\,\{n : \text{katerikoli graf na } n \text{ točkah vsebuje kliko velikosti} \\ &\qquad k \text{ ali neodvisno množico velikosti } l\}. \end{aligned}$$

Ramseyevo število $R(k, l)$ je torej najmanjše celo število n, tako da poljuben graf na n točkah vsebuje kliko velikosti k ali neodvisno množico velikosti l.

Ramsey je pokazal, da je število $R(k, l)$ vedno končno za katerikoli števili k in l, torej vsak graf vsebuje kliko ali neodvisno množico dane velikosti. Kljub temu so točne vrednosti $R(k, l)$ še vedno neznane, vendar za majhno število primerov, in je zaželjeno določiti $R(k, l)$ za večje k in l-je.

Da lahko določimo Ramseyeva števila za večje k in l nam pomaga naslednja rekurzivna zveza:

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

Ni težko pokazati, 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.

V dokazu naslednjega izreka uporabimo verjetnostno metodo, da dokažemo spodnjo mejo za $R(k, k)$.

Izrek 1.1.1 *Za vsak* $k \geq 3$ *velja*

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

Dokaz. Imamo slučajni graf $G(n, 1/2)$ na n točkah, kjer vsak par točk tvori povezavo z verjetnostjo $\frac{1}{2}$, neodvisno od ostalih povezav. Želimo pokazati, da za $n \leq 2^{k/2-1}$ obstaja graf, ki nima ne klike ne neodvisne množice velikosti k. Potem bo sledilo $R(k, k) > 2^{k/2-1}$.

Za vsako fiksno množico k točk izračunajmo verjetnost, da tvorijo kliko. Na $\binom{k}{2}$ načinov lahko izberemo 2 točki, ki tvorita povezavo. Torej je $\binom{k}{2}$ maksimalno število povezav v grafu s k vozlišči. Verjetnost, da izberemo vse povezave - le tako dobimo kliko na k točkah, je enaka $\frac{1}{2^{\binom{k}{2}}} = 2^{-\binom{k}{2}}$.

Za nastop neodvisne množice dobimo enako verjetnost, saj v resnici iščemo K_k^C izmed k točk. Ker imamo n točk v grafu, lahko k točk izberemo na $\binom{n}{k}$ načinov.

Definirajmo zdaj dogodka A_k in B_k: A_k naj bo dogodek, da graf vsebuje kliko velikosti k, B_k pa dogodek, da graf vsebuje neodvisno množico velikosti k. Velja

$$P(A_k \cup B_k) = P(A_k) + P(B_k) - P(A_k \cap B_k).$$

$A_k \cup B_k$ je ravno dogodek, da $G(n, 1/2)$ vsebuje kliko ali neodvisno množico velikosti k. Dobimo

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

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

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

Ker velja tudi $\binom{n}{k} \leq n^k$, lahko ocenimo $2 \cdot \binom{n}{k} 2^{-\binom{k}{2}}$:

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

Torej je $P(A_k \cup B_k) < 1$ 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 $R(k,k) > 2^{k/2-1}$. $\square$

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

Ta dokaz bi seveda lahko naredili tudi na kakšen drugačen način, kjer ne bi potrebovali verjetnostne metode. Lahko bi pa dokaz formulirali v izrazih preštevanja objektov. V dokazu štejemo število slabih objektov in skušamo dokazati, da je število manjše od števila vseh objektov, torej mora biti množica dobrih objektov neprazna. Ta izrek sicer spada med preprostejše, težje in bolj zapletene izreke pa enostavneje dokažemo s pomočjo verjetnostne metode kot pa s preštevanjem objektov. Verjetnostna metoda je še posebej dobrodošla pri dokazovanju v primerih, kjer so konstrukcijski dokazi izredno težki.

1.2 Barvanje hipergrafa

Hipergraf je posplošitev grafa, kjer so povezave množice točk. Oglejmo si definicijo za k-uniformni hipergraf, kjer imajo vse povezave oz. množice natanko k točk.

Definicija 1.2.1 **k-*uniformni hipergraf*** *je par* (X, S)*, kjer je* X *množica točk in* $S \subseteq \binom{X}{k}$ *množica povezav.*

Definicija 1.2.2 *Hipergraf je* **c-*obarvljiv***, *če lahko njegove točke pobarvamo s* **c** *barvami tako, da nobena povezava ni enobarvna (vsaj dve različni barvi se pojavijo v vsaki povezavi).*

Definicija 1.2.3 *Naj bo* ***m(k)*** *najmanjše število povezav v k-uniformnem hipergrafu, ki ni 2-obarvljiv.*

Za grafe velja $m(2) = 3$. Za večji k je veliko težje določiti $m(k)$. Dokazati se da $m(3) = 7$, vendar je točna vrednost $m(k)$ neznana za $k > 3$. Lahko pa dobimo spodnjo mejo $m(k)$ s pomočjo verjetnostne metode.

Izrek 1.2.1 *Za vsak* $k \geq 2$ *velja*

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

Dokaz. Imamo k-uniformni hipergraf $\mathcal{H}$ z manj kot 2^{k-1} povezavami. Dokazali bomo, da je 2-obarvljiv. Pobarvajmo vsako točko hipergrafa $\mathcal{H}$ neodvisno z rdečo ali modro, vsako z verjetnostjo $\frac{1}{2}$. Verjetnost, da so vse točke dane povezave 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 $|S| < 2^{k-1}$. Označimo z A dogodek, da obstaja enobarvna povezava, in ocenimo $P(A)$:

$$P(A) = p \cdot |S| < p \cdot 2^{k-1} = 2^{1-k} \cdot 2^{k-1} = 1.$$

Torej je verjetnost, da nobena povezava ni enobarvna, neničelna ($P(\overline{A}) = 1 - P(A) > 0$), zato obstaja pravilno barvanje. Torej je $m(k) \geq 2^{k-1}$. $\square$

2 Linearnost matematičnega upanja

Definicija 2.0.4 ***Matematično upanje*** *slučajne spremenljivke* X *je*

$$\mathbf{E}[X] = \int_{\Omega} X(\omega) dP(\omega).$$

Dokazi v tem poglavju so zasnovani na naslednji lemi:

Lema 2.0.1 *Upanje je linearen operator, t.j. za vsaki dve slučajni spremenljivki X, Y in konstanti α, $\beta \in \mathbb{R}$ velja*

$$\mathbf{E}[\alpha X + \beta Y] = \alpha\, \mathbf{E}[X] + \beta\, \mathbf{E}[Y]. \tag{1}$$

Dokaz. $\mathbf{E}[\alpha X + \beta Y] = \int_\Omega (\alpha X + \beta Y)\mathrm{d}P = \alpha \int_\Omega X\mathrm{d}P + \beta \int_\Omega Y\mathrm{d}P = \alpha\mathbf{E}[X] + \beta\mathbf{E}[Y]$. □

Iz tega sledi, da je upanje vsote slučajnih spremenljivk $X = X_1 + X_2 + \cdots + X_n$ enako

$$\mathbf{E}[X] = \mathbf{E}[X_1] + \mathbf{E}[X_2] + \cdots + \mathbf{E}[X_n].$$

Definicija 2.0.5 ***(Indikatorske spremenljivke)*** *Za vsak dogodek A definiramo indikatorsko spremenljivko χ_A:*

$$\chi_A(\omega) = \begin{cases} 1, & \omega \in A \\ 0, & \omega \notin A. \end{cases}$$

Lema 2.0.2 *Za vsak dogodek A velja*

$$\mathbf{E}[\chi_A] = P[A].$$

Dokaz.

$$\mathbf{E}[\chi_A] = \int_\Omega \chi_A(\omega)\mathrm{d}P = \int_A \mathrm{d}P = P[A].$$

□

V veliko primerih lahko matematično upanje zapišemo z vsoto indikatorskih spremenljivk

$$X = \chi_{A_1} + \chi_{A_2} + \cdots + \chi_{A_n},$$

kjer poznamo verjetnosti dogodkov $A_1, A_2, \ldots, A_n$. Potem velja

$$\mathbf{E}[X] = P[A_1] + P[A_2] + \cdots + P[A_n].$$

2.1 Število fiksnih točk permutacije

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

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

lahko to izrazimo kot vsoto indikatorskih spremenljivk:

$$X(\sigma) = \sum_{i=1}^{n} X_i(\sigma)$$

kjer je $X_i(\sigma) = 1$, če je $\sigma(i) = i$, in 0 obratno. Potem

$$\mathbf{E}[X_i] = P[\sigma(i) = i] = \frac{1}{n}$$

in

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

Torej poljubna permutacija ima v povprečju 1 fiksno točko.

2.2 Hamiltonove poti

Vedno obstaja elementarni dogodek $\omega_1 \in \Omega$, za katerega velja $X(\omega_1) \geq \mathbf{E}[X]$ in podobno, velja $X(\omega_2) \leq \mathbf{E}[X]$ za nek $\omega_2 \in \Omega$. Torej lahko ocenimo minimalno oziroma maksimalno vrednost slučajne spremenljivke X s pomočjo matematičnega upanja:

$$\begin{aligned} \min_{\omega \in \Omega} X(\omega) &\leq \mathbf{E}[X] \\ \max_{\omega \in \Omega} X(\omega) &\geq \mathbf{E}[X]. \end{aligned}$$

Spomnimo se, da je *turnir* orientacija polnega grafa (za katerikoli točki u in v nastopa natanko ena od usmerjenih povezav (u, v) in (v, u)). *Hamiltonova pot* v turnirju je usmerjena pot skoti vse točke. Naslednji izrek (Szele, 1943) nam pokaže obstoj turnirja, ki ima zelo veliko Hamiltonovih poti. Temu izreku oz. dokazu se pogosto pripisuje, da je prvi uporabil verjetnostno metodo.

Izrek 2.2.1 *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 (vsaka povezava ima slučajno orientacijo, izbrano neodvisno z verjetnostjo $\frac{1}{2}$). Za dano permutacijo σ na $\{1, \ldots, n\}$ si oglejmo zaporedje $\sigma(1), \sigma(2), \ldots, \sigma(n)$ in označimo z X_σ indikator dogodka, da vse povezave $(\sigma(i), \sigma(i+1))$ nastopajo v T s to orientacijo. Izračunajmo $\mathbf{E}[X_\sigma]$, kjer upoštevamo, da orientacijo različnih povezav izberemo neodvisno:

$$\mathbf{E}[X_\sigma] = P[\sigma \text{ je prav orientirana}] = \frac{1}{2^{n-1}}.$$

Sledi

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

saj je vseh različnih permutacij na n točkah $n!$. Ker obstaja tak $\omega_1 \in \Omega$, da je $X(\omega_1) \geq \mathbf{E}[X]$, obstaja turnir z vsaj $\frac{n!}{2^{n-1}}$ Hamiltonovimi potmi. $\square$

2.3 Maksimalni prerez grafov

Tukaj obravnavamo problem maksimalnega prereza, ki je predvsem pomemben algoritmični problem. Imamo graf $G = (V, E)$ in razdelimo 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 2.3.1 *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 X_e označi indikatorsko spremenljivko dogodka, da je *natanko ena* od točk na povezavi e v T. Potem velja

$$\mathbf{E}[X_e] = P[(u \in T \text{ in } v \notin T) \text{ ali } (u \notin T \text{ in } v \in T)] = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

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

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

saj je m število vseh povezav v grafu. Torej, za nekatere $T \subseteq V$ obstaja vsaj $\frac{m}{2}$ povezav med T in $V \setminus T$, ki tvorijo dvodelen graf. $\square$

Literatura

[1] N. Alon, J. Spencer, *The Probabilistic Method*, J.Wiley and Sons, New York, 2nd edition, 2000.

[2] J. Matoušek, J. Vondrak, *The probabilistic method (Lecture Notes)*, http://kam.mff.cuni.cz/ matousek/lectnotes.html.