Osnovna verjetnostna metoda[1]

S pomočjo osnovne metode se dokazuje obstoj kombinatoričnih objektov z določenimi značilnostmi. Metoda temelji na verjetnosti, vendar se z njo dokazuje izreke, ki so popolnoma nepovezani z verjetnostjo.

Ko želimo dokazati obstoj kombinatoričnega objekta z določenimi značilnostmi, je lahko dokaz s konstrukcijo takega objekta zelo težak. V tem primeru z uporabo osnovne metode dokažemo njegov obstoj oziroma dokažemo, da se v verjetnostnem prostoru vsi ostali objekti zgodijo z verjetnostjo strogo manjšo od 1.

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

Dokaz. Za dogodke $A_1, A_2, \ldots, A_n$ velja

$$\mathbf{P}(A_1 \cup A_2 \cup \ldots \cup A_n) \leq \sum_{i=1}^{n} \mathbf{P}(A_i).$$

Zato je

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

■

[1]26. februar 2013

1 Ramseyeva števila

Klika je množica točk, ki tvori poln podgraf 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

$$R(1, l) = R(k, 1) = 1 \quad \text{ter} \quad R(k, l) = R(l, k)$$

za poljubni pozitivni celi števili k in l.

Velja tudi

$$R(3, 3) = 6, R(3, 4) = 9, R(3, 5) = 14, R(4, 4) = 18 \text{ in } R(4, 5) = 25.$$

Opazi še, da velja $R(a, b) \geq R(c, d)$ kadar $a \geq c$ in $b \geq d$.

Številom $R(k, k)$ pravimo *diagonalna* Ramseyeva števila. V dokazu naslednjega izreka uporabimo verjetnostno metodo, da dokažemo spodnjo mejo za $R(k, k)$. Ta nam pove, da Ramseyeva števila hitro naraščajo.

Izrek 2 *Za vsak $k \geq 3$ velja*

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

Dokaz. Želimo pokazati, da za poljuben $n \leq 2^{k/2-1}$ obstaja graf na n točkah, 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

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

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

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

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 pojavijo 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 2-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 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. Pokazali 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

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

Označimo z A dogodek, da obstaja monokromatska hiperpovezava, in ocenimo $\mathbf{P}(A)$:

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

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

■

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 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, tj. vsako povezavo neodvisno od ostalih usmerimo v eno ali drugo smer z verjetnostjo $\frac{1}{2}$. 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

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

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

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

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

Posledica 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

$$\binom{n}{k} < (\frac{en}{k})^k \quad \text{in} \quad (1 - 2^{-k})^{n-k} < e^{-\frac{n-k}{2^k}}$$

se da pokazati, da je $\binom{n}{k}(1 - 2^{-k})^{n-k} < 1$. Potem trditev sledi iz izreka 4. ∎

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 6 *Množico $\{1,2,\ldots,n\}$ lahko pobarvamo z dvema barvama, tako da nobeno aritmetično zaporedje s $2\lg n$ členi ni enobarvno. Torej*

$$W(2,k) > 2^{k/2}.$$

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

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

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

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

Če je $\binom{n}{2}2^{1-k} < 1$, potem obstaja neko barvanje, za katerega ni aritmetičnega zaporedja s k členi in od tod $W(2,k) > n$. Torej 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 neenakost

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

Od tod sledi $W(2,k) > 2^{\frac{k}{2}}$. ∎

5 Spernerjev izrek in njegove posplošitve

Izrek 7 (Sperner 1928) *Če je $\mathcal{F}$ družina podmnožic množice $\{1, 2, \ldots, m\}$, kjer $A \nsubseteq B$ za poljubni različni $A, B \in \mathcal{F}$, potem je $|\mathcal{F}| \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Spodnja izreka implicirata Sperner-jev izrek. Pri dokazu upoštevamo, da $\mathcal{F} = \{A_1, A_2, \ldots, A_n\}$, $B_i = \{1, 2, \ldots, m\}/A_i$ in dejstvo, da velja $\binom{m}{k} \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$ za vsak $k = 0, 1, \ldots, m$.

Izrek 8 (Bollobás, 1965) *Naj bosta k in l naravni števili. Naj bo n maksimalno število, da zanj obstajajo množice $A_1, \ldots, A_n$ in $B_1, \ldots, B_n$, za katere velja:*

1. *$|A_i| = k$ in $|B_i| = l$ za vsak $i = 1, 2, \ldots, n$.*
2. *$A_i \cap B_i = \emptyset$ za vsak $i = 1, 2, \ldots, n$.*
3. *$A_i \cap B_j \neq \emptyset$ za vsak $i \neq j$ in $i, j = 1, 2, \ldots, n$.*

Potem je

$$n = \binom{k+l}{k}.$$

Dokaz. Naj bo $X = \bigcup_{i=1}^{n} (A_i \cup B_i)$. Linearno uredimo elemente množice X v poljubnem vrstnem redu. Naj bo U_i dogodek, da so vsi elementi množice A_i pred vsemi elementi množice B_i (glede urejenosti elementov množice X). Verjetnost tega dogodka je

$$\mathbf{P}[U_i] = \binom{k+l}{k}^{-1}.$$

Za različna $i \neq j$ se dogodka U_i in U_j ne moreta zgoditi hkrati. Res, ker je $A_i \cap B_i \neq \emptyset$ in enakovredno tudi $A_j \cap B_i \neq \emptyset$, velja $\max A_i \geq \min B_j$ in $\max A_j \geq \min B_i$. Če bi se dogodka U_i in U_j zgodila hkrati, bi veljalo $\max A_i < \min B_i$ in $\max A_j < \min B_j$, kar vodi v protislovje:

$$\max A_i \geq \min B_j > \max A_j \geq \min B_i > \max A_i.$$

Dogodka se torej res ne moreta zgoditi hkrati. Iz tega sledi, da je

$$1 \geq \mathbf{P}[\bigcup_{i=1}^{n} U_i] = \sum_{i=1}^{n} \mathbf{P}[U_i] = \frac{n}{\binom{k+l}{k}}$$

in torej je

$$\binom{k+l}{k} \geq n.$$

Zdaj pa poiščimo še primer, ko n doseže to vrednost. Naj bodo $A_1, A_2, \ldots, A_n$ vse podmnožice velikosti k množice $X = \{x_1, x_2, \ldots, x_{k+l}\}$, množice $B_1, B_2, \ldots, B_n$ pa naj bodo njihovi komplementi, torej $B_i = X \setminus A_i$ za vsak $i = 1, 2, \ldots, n$. Pogoji izreka očitno veljajo za tako izbrane množice in $n = \binom{k+l}{k}$. ■

Pravimo, da je množica $T \subseteq V$ *transverzalna množica* hipergrafa $\mathcal{H} = (V, E)$, če $S \cap T \neq \emptyset$ za vsak $S \in \mathcal{H}$.

Transverzalno število $\tau(\mathcal{H})$ je velikost najmanjše transverzalne množice T.

Hipergraf $\mathcal{H}$ se imenuje *τ-kritična*, če $\tau(\mathcal{H} \setminus \{S\}) < \tau(\mathcal{H})$, za vsak $S \in \mathcal{H}$.

Zgornji izrek nam pove kakšno je maksimalno število hiperpovezav v τ-kritičnem k-enakomernem hipergrafu $\mathcal{H}$ z $\tau(\mathcal{H}) = l + 1$.

Naslednji izrek je posplošitev izreka 8 in se dokaže podobno.

Izrek 9 (Bollobás 1965) *Naj bodo $A_1, A_2, \ldots, A_n$ in $B_1, B_2, \ldots, B_n$ množice za katere velja $A_i \cap B_j = \emptyset$ natanko takrat, ko je $i = j$. Potem $\sum_{i=1}^{n} \binom{|A_i|+|B_i|}{|A_i|}^{-1} \leq 1$.*

6 Izrek Erdös-Ko-Rado

Imamo množico z n elementi. Izbrati hočemo m podmnožic, v katerih bo natanko $k \leq \frac{n}{2}$ elementov in za katere bo veljalo, da je presek vsakih dveh neprazen. Erdös-Ko-Radov izrek nam pove, da je takih podmnožic maksimalno $\binom{n-1}{k-1}$.

Bolj formalno zapišemo takole: Družina množic $\mathcal{F}$ je *presečna*, če za vsaki dve množici $A, B \in \mathcal{F}$ velja, da je njun presek neprazen $A \cap B \neq \emptyset$. Zapis $\binom{X}{k}$ pomeni množico vseh podmnožic množice X, velikosti k, torej $\binom{X}{k} = \{Y \subset X; |Y| = k\}$.

Izrek 10 (Erdös-Ko-Rado, 1961) *Če je $|X| = n$, kjer je $n \geq 2k$, $\mathcal{F}$ pa presečna družina podmnožic množice X moči k, potem je $|\mathcal{F}| \leq \binom{n-1}{k-1}$.*

Najprej pokažimo naslednjo lemo.

Lema 11 *Naj bo množica $X = \{0, 1, 2, \ldots, n-1\}$ in naj bo $A_s = \{s, s+1, \ldots, s+k-1\} \subseteq X$ za $0 \leq s < n$ in $n \geq 2k$. Potem velja, da vsaka presečna družina $\mathcal{F} \subseteq \binom{X}{k}$ vsebuje kvečjemu k množic izmed A_s.* ■

Dokaz. Če je $A_i \in \mathcal{F}$, potem mora biti katerikoli drug $A_s \in \mathcal{F}$ eden izmed $A_{i-k+1}, \ldots, A_{i-1}$ ali $A_{i+1}, \ldots, A_{i+k-1}$. To je $2k-2$ podmnožic, ki jih lahko razdelimo v $k-1$ parov oblike (A_s, A_{s+k}). Ker je $n \geq 2k$, je

$$A_s \cap A_{s+k} = 0,$$

torej je v $\mathcal{F}$ kvečjemu eden izmed A_s in A_{s+k}. ■

Dokaz izreka. Recimo, da imamo množico $X = \{0, 1, \ldots, n-1\}$ in presečno družino podmnožic $\mathcal{F} \subseteq \binom{X}{k}$. Izberemo slučajno neodvisno in uniformno permutacijo $\delta : X \to X$ ter $s \in X$. Definirajmo $\delta(A_s) := \{\delta(s), \ldots, \delta(s+k-1)\}$. Ker gre samo za premešanje členov, velja lema tudi tu, torej je tudi samo k podmnožic oblike $\delta(A_s)$ v presečni družini $\mathcal{F}$. Verjetnost, da je $\delta(A_s)$ v $\mathcal{F}$ je torej

$$\mathbf{P}[\delta(A_s) \in \mathcal{F}] \leq \frac{k}{n}.$$

Verjetnostni prostor je $\{1, 2, \ldots, n\} \times S_n$, pri čemer je S_n množica vseh permutacij na $[n]$. Po drugi strani pa je verjetnost, da je $\delta(A_s)$ v $\mathcal{F}$ enaka izbiri slučajne podmnožice s k elementi, torej

$$\mathbf{P}[\delta(A_s) \in \mathcal{F}] = \frac{|\mathcal{F}|}{\binom{n}{k}}.$$

Iz tega sledi

$$\frac{|\mathcal{F}|}{\binom{n}{k}} \leq \frac{k}{n}$$

in od tukaj

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

Omenimo, da v primeru, ko pogoj $k \leq \frac{n}{2}$ ni izpolnjen, t.j. $k > \frac{n}{2}$, je zgornji problem trivialen, ker lahko izberemo vse podmnožice velikosti k in te tvorijo presečno družino. Torej v takem primeru bo naša družina velikosti $\binom{n}{k}$.