Verjetnostna metoda in algoritmi

(20. april 2011)

B. Lužar, V. Vukašinović,

&

R. Škrekovski

Oddelek za Matematiko
Fakulteta za Matematiko in Fiziko
Univerza v Ljubljani

Kazalo

Poglavje 1

Osnovni pojmi verjetnostnega računa

Osnovno orodje verjetnostne metode je verjetnostni račun. V tem poglavju definiramo osnovne pojme, ki jih bomo uporabljali v nadaljevanju.

1.1 Dogodki in verjetnostni prostor

Dogajanju, ki ga opazujemo pravimo *verjetnostni poskus*, rezultatom poskusa pa *izid*. Množico vseh možnih izidov označujemo z Ω. Poljubna podmnožica E množice Ω pa se imenuje *dogodek*. Družino množic $\{E \,|\, E \subset \Omega\}$ bomo označevali z $\mathcal{F}$[1]. Med priljubljene primere verjetnostnega poskusa sodi metanje kocke. Izid poskusa metanja kocke je število pik, primer dogodka pa je, da pade sodo število pik. Nadaljujmo z verjetnostno funkcijo.

Definicija 1.1 *Verjetnostna funkcija* je poljubna funkcija $\mathbf{P} : \mathcal{F} \to \mathbb{R}$, ki zadošča naslednjim pogojem:

(a) Za vsak dogodek $E \in \mathcal{F}$ velja $0 \leq \mathbf{P}(E) \leq 1$;

(b) $\mathbf{P}(\Omega) = 1$;

(c) Za vsako števno zaporedje paroma disjunktnih dogodkov $E_1, E_2, \ldots$, velja:

$$\mathbf{P}\left(\bigcup_{i\geq 1} E_i\right) = \sum_{i\geq 1} \mathbf{P}(E_i)\,.$$

Vrednosti $\mathbf{P}(E)$ bomo rekli verjetnost dogodka E. Ko poznamo množico izidov, možne dogodke ter verjetnostno funkcijo nad dogodki, lahko definiramo *verjetnostni prostor* kot trojico $(\Omega, \mathcal{F}, \mathbf{P})$.

Navadno nas zanima le verjetnost nekega določenega dogodka, vendar je izračun lažji, če dogodek zapišemo kot skupek preprostejših dogodkov, katerih verjetnosti poznamo. Zato si oglejmo, kako lahko dogodke sestavljamo. Operacije med dogodki

[1] $\mathcal{F}$ je σ-algebra nad Ω.

bomo opisovali s standardno notacijo iz teorije množic. *Presek dogodkov* $E_1 \cap E_2$, ponavadi ga označujemo kar kot produkt $E_1\,E_2$, je dogodek, ko se zgodita oba dogodka hkrati. Za primer ponovno vzemimo kocko in jo vržimo dvakrat. Naj bo E_1 dogodek, da smo v prvem metu vrgli 6 in E_2, da smo vrgli 6 v drugem metu. Presek dogodkov $E_1 \cap E_2$ je dogodek, da smo v dveh metih kocke dvakrat vrgli 6. Po drugi strani je *unija dogodkov* $E_1 \cup E_2$ dogodek, da se je zgodil vsaj eden izmed obeh dogodkov, torej da smo vrgli 6 vsaj enkrat.

Komplement dogodka E bomo označevali z $\overline{E}$, zgodi pa se, ko izid poskusa ni vsebovan v dogodku E. Torej, če je dogodek E, da smo vrgli liho pik, je njegov komplement met sodega števila pik.

Naslednja lema govori o odnosu med verjetnostjo unije dogodkov in vsoti verjetnosti le-teh.

Lema 1.2 *Za končno zaporedje dogodkov* $E_1, E_2, \ldots E_k$, *velja*

$$\mathbf{P}\left(\bigcup_{i=1}^{k} E_i\right) \leq \sum_{i=1}^{k} \mathbf{P}(E_i)\,.$$

Za unijo dogodkov E_1 in E_2 velja enačba

$$\mathbf{P}(E_1 \cup E_2) = \mathbf{P}(E_1) + \mathbf{P}(E_2) - \mathbf{P}(E_1 \cap E_2)\,.$$

Seveda poznamo tudi njeno posplošitev, ki jo opiše spodnja lema.

Lema 1.3 *Za poljubne dogodke* $E_1, E_2, \ldots, E_n$ *velja*

$$\mathbf{P}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} (-1)^{i-1} \sum_{k_1<k_2<\cdots<k_i} \mathbf{P}(E_{k_1} \cap E_{k_2} \cap \cdots \cap E_{k_i})\,.$$

Naslednja pomembna relacija med dogodki je neodvisnost. Dogodka E_1 in E_2 sta *neodvisna* natanko tedaj, ko velja

$$\mathbf{P}(E_1 \cap E_2) = \mathbf{P}(E_1) \cdot \mathbf{P}(E_2)\,.$$

Ali splošneje, dogodki $E_1, E_2, \ldots, E_n$ so medsebojno neodvisni natanko tedaj, ko za vsako podmnožico $I \subset \{1, 2, \ldots, n\}$ velja

$$\mathbf{P}\left(\bigcap_{i\in I} E_i\right) = \prod_{i\in I} \mathbf{P}(E_i)\,.$$

1.2 Pogojna verjetnost

Včasih nas zanima, kakšna je verjetnost, da se nek dogodek zgodi, takrat ko se zgodi nek drug dogodek. Na primer, kakšna je verjetnost, da je število pik pri metu

kocke enako 6, takrat ko se zgodi dogodek, da smo vrgli sodo pik. Takšne situacije obravnavamo s pomočjo pogojne verjetnosti.

Pogojna verjetnost, da se zgodi dogodek E ob dogodku F, za katerega je $\mathbf{P}(F) > 0$, je

$$\mathbf{P}(E \mid F) = \frac{\mathbf{P}(E \cap F)}{\mathbf{P}(F)}\,.$$

Pojav dogodka E torej gledamo na podprostoru našega verjetnostnega prostora, kjer se dogodek F zgodi, zato moramo verjetnosti normirati s $\mathbf{P}(F)$.

1.3 Matematično upanje

Matematično upanje slučajne spremenljivke $X : \Omega \to \mathbb{R}$ končnega prostora (Ω, p) je definirano kot vsota produktov vrednosti slučajne spremenljivke ter verjetnosti, da spremenljivka to vrednost zavzame. Torej

$$\mathbf{E}(X) = \sum_{\omega \in \Omega} p(\omega) X(\omega).$$

Iz definicije sledi, da vedno obstaja elementarni dogodek $\omega_1 \in \Omega$, za katerega velja $X(\omega_1) \geq \mathbf{E}(X)$. Podobno, vedno lahko najdemo dogodek $X(\omega_2) \leq \mathbf{E}(X)$ iz Ω. Tako lahko minimalno oziroma maksimalno vrednost slučajne spremenljivke X ocenimo zgolj s pomočjo matematičnega upanja:

$$\min_{\omega \in \Omega} X(\omega) \leq \mathbf{E}(X) \quad \text{in} \quad \max_{\omega \in \Omega} X(\omega) \geq \mathbf{E}(X).$$

Uporabnost matematičnega upanja temelji na njegovi linearnosti.

Trditev 1.4 *Upanje je linearen operator, t.j. za vsak par slučajnih spremenljivk X, Y in konstanti α, $\beta \in \mathbb{R}$ velja*

$$\mathbf{E}(\alpha X + \beta Y) = \alpha\, \mathbf{E}(X) + \beta\, \mathbf{E}(Y)\,.$$

Dokaz.

$$\begin{aligned} \mathbf{E}(\alpha X + \beta Y) &= \sum_{\omega \in \Omega} p(\omega)(\alpha X + \beta Y)(\omega) \\ &= \alpha \sum_{\omega \in \Omega} p(\omega) X(\omega) + \beta \sum_{\omega \in \Omega} p(\omega) Y(\omega) \\ &= \alpha\, \mathbf{E}(X) + \beta\, \mathbf{E}(Y)\,. \end{aligned}$$

□

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

$$\mathbf{E}(X) = \mathbf{E}(X_1) + \mathbf{E}(X_2) + \cdots + \mathbf{E}(X_n)\,.$$

Trditev 1.5 *Če sta slučajni spremenljivki X in Y neodvisni, potem je $E(XY) = E(X)E(Y)$.*

Dokaz. Za poljubna dva elementa $\omega_i, \omega_j \in \Omega$ velja $\mathbf{P}(X = X(\omega_i) \text{ in } Y = Y(\omega_j)) = \mathbf{P}(X = X(\omega_i))\mathbf{P}(Y = Y(\omega_j))$. Od tod izpeljemo:

$$\begin{aligned} E(XY) &= \sum_{\omega_i,\omega_j \in \Omega} \mathbf{P}(X = X(\omega_i) \text{in } Y = Y(\omega_j))X(\omega_i)Y(\omega_j) \\ &= \sum_{\omega_i} \sum_{\omega_j} \mathbf{P}(X = X(\omega_i))\mathbf{P}(Y = Y(\omega_j))X(\omega_i)Y(\omega_j) \\ &= \sum_{\omega_i} \mathbf{P}(X = X(\omega_i))X(\omega_i) \sum_{\omega_j} \mathbf{P}(Y = Y(\omega_j))Y(\omega_j) \\ &= E(X)\, E(Y). \end{aligned}$$

□

Za slučajen dogodek A definiramo *indikatorsko spremenljivko* I_A na naslednji način:

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

Očitno dogodek A enolično določa I_A in obratno. Velja naslednje:

Trditev 1.6 *Za vsak dogodek A velja $\mathbf{E}(I_A) = \mathbf{P}(A)$.*

Dokaz. Izpeljemo takole: $\mathbf{E}(I_A) = \sum_{\omega \in \Omega} p(\omega) I_A(\omega) = \sum_{\omega \in A} p(\omega) = \mathbf{P}(A)$.

□

V veliko primerih obravnavano slučajno spremenljivko lahko zapišemo kot vsoto indikatorskih spremenljivk

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

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

$$\mathbf{E}(X) = \mathbf{P}(A_1) + \mathbf{P}(A_2) + \cdots + \mathbf{P}(A_n)\,.$$

1.4 Varianca in deviacija

Poleg matematičnega upanja, je pomembna številska karakteristika slučajne spremenljivke tudi *varianca*. Redkeje jo imenujemo tudi *razpršenost* ali *disperzija*. Varianca meri odstopanje vrednosti slučajne spremenljivke od matematičnega upanja (npr. varianca konstantne slučajne spremenljivke je 0).

Varianca realne slučajne spremenljivke X je

$$\mathrm{Var}(X) = \mathbf{E}((X - \mathbf{E}(X))^2) = \mathbf{E}(X^2) - (\mathbf{E}(X))^2.$$

Prva enakost sledi iz definicije, drugo pa dobimo po lažjem izračunu. *Standardna deviacija* X je

$$\sigma(X) = \sqrt{\mathrm{Var}(X)}.$$

V primerjavi z matematičnim upanjem, pa varianca ni linearen funkcional. Zato moramo, če želimo izračunati varianco vsote slučajnih spremenljivk, vedeti nekaj o njihovi (paroma) medsebojni odvisnosti. *Kovarianca* slučajnih spremenljivk X in Y je

$$\mathrm{Cov}(X,Y) = \mathbf{E}((X - \mathbf{E}(X))(Y - \mathbf{E}(Y))) = \mathbf{E}(XY) - \mathbf{E}(X)\mathbf{E}(Y)\,.$$

Iz Trditve 1.5 neposredno sledi, da je kovarianca neodvisnih slučajnih spremenljivk enaka 0. Po drugi strani pa iz $\mathrm{Cov}(X,Y) = 0$ ne moremo sklepati na neodvisnost spremenljivk X in Y.

Lema 1.7 *Varianca vsote slučajnih spremenljivk je enaka*

$$\mathrm{Var}(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} \mathrm{Var}(X_i) + \sum_{i \neq j} \mathrm{Cov}(X_i, X_j)\,.$$

Dokaz. Iz definicije sledi

$$\mathrm{Var}(\sum_{i=1}^{n} X_i) = \mathbf{E}(\sum_{i=1}^{n} X_i \sum_{j=1}^{n} X_j) - \mathbf{E}(\sum_{i=1}^{n} X_i)$$

$$\begin{aligned} \mathbf{E}(\sum_{j=1}^{n} X_j) &= \sum_{i=1}^{n} \mathbf{E}(X_i^2) + \sum_{i \neq j} \mathbf{E}(X_i X_j) - \sum_{i=1}^{n} (\mathbf{E}(X_i))^2 - \sum_{i \neq j} \mathbf{E}(X_i)\mathbf{E}(X_j) \\ &= \sum_{i=1}^{n} \mathrm{Var}(X_i) + \sum_{i \neq j} \mathrm{Cov}(X_i, X_j)\,. \end{aligned}$$

□

Če so $X_1, \ldots, X_n$ neodvisne spremenljivke, je kovarianca vsakega para enaka 0. V tem primeru je

$$\mathrm{Var}(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} \mathrm{Var}(X_i)\,.$$

1.5 Uporabne neenakosti

V tem poglavju predstavimo nekaj neenakosti, ki nam pridejo prav pri dokazovanju z verjetnostno metodo.

Za faktiorelo $n!$ pogosto uporabimo očitno oceno zgornje meje $n! \leq n^n$, finejše meje pa so $(\frac{n}{e})^n \leq n! \leq en(\frac{n}{e})^n$.

Za binomski koeficient $\binom{n}{k}$, velja osnovna binomska neenakost

$$\binom{n}{k} \leq n^k$$

Finejša ocena spodnje in zgornje meje pa je

$$(\frac{n}{k})^k \leq \binom{n}{k} \leq (\frac{en}{k})^k.$$

Za vsak k, velja tudi neenakost

$$\binom{n}{k} \leq 2^n.$$

Včasih potrebujemo natančnejšo oceno srednjega binomskega koeficienta $\binom{2m}{m}$. Zanj velja

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}.$$

Pogosto se uporablja neenakost, ki pravi, da za vsak realen x velja $1+x \leq e^x$. V posebnem primeru, za $(1-p)^m$ pri čemer je p majhno pozitivno število, iz prejšnje neenakosti sledi neenakost

$$(1-p)^m \leq e^{-mp}.$$

Za vsak $p \in [0, \frac{1}{2}]$ pa velja:

$$1 - p \geq e^{-2p}.$$

Poglavje 2

Osnovna metoda

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 2.1 *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

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

□

2.1 Ramseyeva števila

Preden definiramo Ramzeyevo število, se spomnimo, kaj je to klika in kaj neodvisna množica. *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 $R(1,l) = 1$ 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 $R(4,5) = 25$. 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 2.2 *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

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

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, zato ga obravnavamo kasneje.

2.2 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 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 2.3 *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

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

Predpostavili smo, da za $\mathcal{H}$ velja $|E| < 2^{k-1}$. 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 $m(k) \geq 2^{k-1}$.

□

2.3 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 2.4 (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 2.5 *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 $\binom{n}{k} < (\frac{en}{k})^k$ 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 2.4.

□

2.4 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 2.6 *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 $W(2,k) > 2^{\frac{k}{2}}$.

□

2.5 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 2.7 (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 $d_i \equiv xb_i \pmod{p}$, 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

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

Tako je pričakovano število elementov b_i, za katere je $d_i \in C$, 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 $\mathbb{Z}_p$.

□

2.6 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 vseh možnih 2^k nizov. 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 2.8 (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 in neodvisno 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

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

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 2.9 *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 $\binom{n}{k} < (\frac{en}{k})^k$ in $(1-2^{-k})^r < e^{-\frac{r}{2^k}}$. Potem dokaz sledi sledi po izreku 2.8.

□

2.7 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 2.10 (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 2.11 *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 $\binom{n}{k}$.

2.8 Spernerjev izrek in njegove posplošitve

Izrek 2.12 (Sperner 1928) *Če je $\mathcal{F}$ družina podmnožic množice $\{1, 2, \ldots, m\}$, kjer $A \not\subseteq B$ 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 2.13 (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 2.13 in se dokaže podobno.

Izrek 2.14 (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* $\sum_{i=1}^{n} \binom{|A_i|+|B_i|}{|A_i|}^{-1} \leq 1$.

Poglavje 3

Linearnost matematičnega upanja

V Poglavju 1.5 smo pokazali, da je matematično upanje linearen operator. To lastnost s pridom uporabljamo za dokazovanje problemov s pomočjo verjetnosti. V naslednjih razdelkih so prikazani primeri uporabe.

3.1 Število fiksnih točk permutacije

Permutacija končne množice A je bijektivna preslikava 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 3.1 *V povprečju ima vsaka permutacija eno 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 $\sigma(i) = i$ in $F_i(\sigma) = 0$ sicer. Torej je

$$\mathbf{E}(F_i) = \mathbf{P}(\sigma(i) = i) = \frac{(n-1)!}{n!} = \frac{1}{n}\,.$$

Od tod sledi

$$\mathbf{E}(F) = \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = 1\,,$$

kar pomeni, da ima permutacija v povprečju eno fiksno točko.

□

3.2 Hamiltonske poti v turnirjih

Turnir je orientiran poln graf, kar pomeni, da med poljubnima točkama u in v nastopa natanko ena usmerjena povezava (u, v) oz. (v, u). *Hamiltonska pot* v turnirju je usmerjena pot skozi vse točke. Znano je, da ima vsak turnir Hamiltonsko pot. Naslednji izrek (Szele, 1943) pravi, da obstoja turnir z velikim številom Hamiltonskih poti. Temu izreku oziroma njegovemu dokazu se pogosto pripisuje prva uporaba verjetnostne metode.

Izrek 3.2 *Obstaja turnir na n točkah, ki ima vsaj $\frac{n!}{2^{n-1}}$ Hamiltonskih poti.*

Dokaz. Izračunajmo pričakovano število Hamiltonskih poti v slučajnem turnirju T na n točkah, kjer ima vsaka povezava slučajno orientacijo, izbrano neodvisno z verjetnostjo $\frac{1}{2}$. Označimo vozlišča 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 $\mathbf{E}[I_\sigma]$:

$$\mathbf{E}(I_\sigma) = \mathbf{P}(\sigma) = \frac{1}{2^{n-1}}\,.$$

Naj bo X vsota vseh Hamiltonskih 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 $n!$. Torej obstaja tak turnir T, ki vsebuje vsaj $\frac{n!}{2^{n-1}}$ Hamiltonskih poti.

□

3.3 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 3.3 *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

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

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 inducirajo dvodelen podgraf.

□

3.4 Uravnoteženi vektorji

TODO: Nekaj spremne besede

Izrek 3.4 *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 kot

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

Uporabimo linearnost 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

$$\mathbf{E}(\varepsilon_i \varepsilon_j) = \mathbf{E}(\varepsilon_i) \cdot \mathbf{E}(\varepsilon_j) = 0\,.$$

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 $X \leq n$. Izrek je s tem dokazan.

□

Izrek 3.5 *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

$$\mathbf{P}(\varepsilon_i = 1) = p_i \quad \text{in} \quad \mathbf{P}(\varepsilon_i = 0) = 1 - p_i\,.$$

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

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

□

3.5 Dominantne podmnožice v grafih

Dominantna podmnožica grafa $G = (V, E)$ je podmnožica vozlišč $D \subseteq V$, za katero velja, da je vsako vozlišče grafa G bodisi v D bodisi ima v D soseda. Na primer, najmanjša dominantna množica cikla C_n velikosti $\lceil \frac{n}{3} \rceil$. Spodnji izrek navzgor oceni najmanjšo dominantno podmnožico.

Izrek 3.6 *Naj bo $G = (V, E)$ graf z n vozlišči in z minimalno stopnjo $\delta > 1$. Potem ima graf G dominantno podmnožico z največ $n\frac{1+\ln(\delta+1)}{\delta+1}$ vozlišči.*

Dokaz. Naj bo S slučajna množica točk iz G tako, da vsako točko izberemo neodvisno z verjetnostjo p. Naj bo T množica točk iz G, za katero velja, da ne vsebuje točk iz S niti točk, ki imajo soseda v S. Množica $T \cup S$ tvori dominantno množico grafa G. Velja

$$\mathbf{E}(|S|) = \sum_{v \in V} p = n\,p \,.$$

Naj bo I_v indikatorska spremenljivka dogodka, da je v izbran v T. Torej

$$I_v = \begin{cases} 1, & \text{niti } v \text{ niti sosedje } v\text{-ja niso v } S \\ 0, & \text{sicer.} \end{cases}$$

Potem je $|T| = \sum_{v \in V} I_v$. Verjetnost, da je neko vozlišče v vsebovano v T, je enaka

$$\mathbf{P}(v \in T) = (1 - p)^{d(v)+1} \leq (1 - p)^{\delta+1} \,.$$

Torej

$$\mathbf{E}(|T|) = \sum_{v \in V} \mathbf{E}(I_v) \leq n(1 - p)^{\delta+1} \leq ne^{-p(\delta+1)}$$

in od tod

$$\mathbf{E}(|S \cup T|) = \mathbf{E}(|S|) + \mathbf{E}(|T|) \leq np + ne^{-p(\delta+1)} .$$

S prijemi matematične analize dobimo najmanjšo zgornjo mejo naše ocene $\mathbf{E}(|S \cup T|)$ za $p = \frac{\ln(\delta+1)}{\delta+1}$. Torej

$$\mathbf{E}(|S \cup T|) \leq n\frac{1 + \ln(\delta + 1)}{\delta + 1} .$$

□

3.6 Bregmanov izrek

Kakšna je verjetnost, da napovemo pravilni vrstni red, v katerem je vseh šest konjev na dirki prišlo na cilj? Če ne bi o konjskih dirkah vedeli prav nič, bi pomislili, da je vseh 6! vrstnih redov enako verjetnih. Torej, da ima vsaka izbira verjetnost uspeha $\frac{1}{6!} = 0.0014$. Strokovnjaki za tovrstne dirke pa so, za razliko od laika, sposobni to verjetnost izračunati veliko bolj natančno. Njihove ocene konjevih možnosti se lahko predstavijo z dvodelnim grafom, v katerem so možne povezave konj z zadnjo pozicijo znatno omejene.

Če za predstavitev takšnega grafa uporabimo $(0, 1)$ matriko, potem *permanenta*[1] matrike natančno določa število možnosti simultanih izbir števila 1 iz vsakega stolpca in vrstice. Vseh možnosti je za naš primer 56, kar pomeni, da je to tudi vrednost permanente naše matrike. Možnost pravilne napovedi se je tako povečala na $\frac{1}{56} = 0,018$. Za velike matrike žal ne poznamo nobene metode, ki bi pridelala vrednost permanente v uporabnem časovnem okviru.

Bregmanova neenakost nam poda dobro zgornjo mejo (v našem primeru z vrednostjo skoraj $\frac{1}{88}$), enakost pa je dosežena natanko takrat, ko je matrika iz diagonalnih blokov, sestavljenih iz samih enic (do permutacij stolpcev in vrstic natančno). Naj bo $A = [a_{ij}]$ $n \times n$ matrika, pri čemer so vsi $a_{ij} \in \{0, 1\}$. Naj bo $r_i = \sum_{i \leq j \leq n} a_{ij}$ število enic v i-ti vrstici. Naj bo S množica permutacij $\sigma \in S_n$ z $a_{i,\sigma i} = 1$ za $1 \leq i \leq n$. Potem je $\mathrm{per}(A)$ enostavno $|S|$. Slednje je domneval že Minc, Bregman pa je leta 1973 to tudi dokazal.

Izrek 3.7 (Bregman)

$$\mathrm{per}(A) \leq \prod_{1 \leq i \leq n} (r_i!)^{\frac{1}{r_i}} .$$

Dokaz. Izberimo neodvisni konstanti $\sigma \in S$ in $\tau \in S_n$. Označimo $A^1 = A$. Naj bo $R_{\tau 1}$ število enic v vrstici $\tau 1$ v A^1. Izbrišimo vrstico $\tau 1$ in stolpec $\sigma\tau 1$ iz A^1, da dobimo A^2. V splošnem naj A^i pomeni A brez vrstic $\tau 1, \ldots, \tau(i-1)$ in stolpcev

[1] $\mathrm{per}(A)$, ("permanenta A"), priredi matriki realno vrednost na podoben način, kot determinanta, le da determinanta prišteva sode in odšteva lihe permutacije členov matrike, permanent pa prišteva tako sode, kot tudi lihe permutacije.

$\sigma\tau 1, \ldots, \sigma\tau(i-1)$ in $R_{\tau i}$ naj pomeni število enic v vrstici τi v A^i. (To je neničelno število, kajti $\sigma\tau i$-ti stolpec ima enico.) Naj bo

$$L = L(\sigma, \tau) = \prod_{1 \leq i \leq n} R_{\tau i}.$$

V grobem si bomo mislili, da je L enak permanentu, izračunanemu na "grobi način". Obstaja $R_{\tau 1}$ izbir za enico v vrstici $\tau 1$, pri čemer vse vodijo v različne podpermanentne rezultate. Namesto tega vzame grobi način faktor $R_{\tau 1}$, odstrani enico iz permutacije σ in nadaljuje z A^2. Ker je $\sigma \in S$ konstantna, se grobi način nagiba proti visokim podpermanentom in je torej možno, da permanent preceni. Da se tega lotimo natančno, definirajmo geometrijsko sredino $G(Y)$. Če $Y > 0$ zavzame vrednosti $a_1, \ldots, a_s$ s pripadajočimi verjetnostmi $p_1, \ldots, p_s$, potem je $G(Y) = \prod_{i=1}^{s} a_i^{p_i}$. Ekvivalentno velja $G(Y) = e^{\mathbf{E}(\ln Y)}$. Linearnost matematičnega upanja se prevede v geometrijsko sredino produkta, ki je produkt geometrijskih sredin.

Lema 3.8

$$\mathrm{per}(A) \leq G(L)\,.$$

Pokažimo to za poljuben τ, ki je fiksen. Zaradi lažjega označevanja recimo, da je $\tau 1 = 1$. Uporabimo indukcijo po velikosti matrike. Preuredimo jo tako, da ima prva vrstica enice v prvih r stolpcih. Očitno je $r = r_1$. Za $1 \leq j \leq r$ naj bo t_j permanent od A brez prve vrstice in j-tega stolpca ali, ekvivalentno, število permutacij $\sigma \in S$, za katere velja $\sigma 1 = j$. Naj bo

$$t = \frac{(t_1 + \ldots + t_r)}{r}\,,$$

tako da $\mathrm{per}(A) = rt$. Če je $\sigma 1 = j$, je $R_2 \ldots R_n$ grob izračun permanenta $\mathrm{per}(A^2)$, pri čemer je A^2 kar A brez prve vrstice in j-tega stolpca. Po indukciji je

$$G(R_2 \ldots R_n | \sigma 1 = j) \geq t_j$$

in je torej

$$G(L) \geq \prod_{j=1}^{r} (rt_j)^{\frac{t_j}{\mathrm{per}(A)}} = r \prod_{j=1}^{r} t_j^{\frac{t_j}{rt}}\,.$$

Lema 3.9

$$(\prod_{j=1}^{r} t_j^{t_j})^{\frac{1}{r}} \geq t^t\,.$$

Dokaz. Če logaritmiramo, je to ekvivalentno

$$\frac{1}{r} \sum_{j=1}^{r} t_j \ln(t_j) \geq t \ln(t)\,,$$

kar pa je res zaradi konveksnosti funkcije $f(x) = x \ln x$.

□

Z uporabo Leme 3.9, dobimo

$$G(L) \geq r \prod_{j=1}^{r} t_j^{\frac{t_j}{rt}} \geq r(t^t)^{\frac{1}{t}} = rt = \mathrm{per}(A)\,.$$

Sedaj izračunamo $G(L)$ pri konstantni σ. Zaradi lažjega označevanja preuredimo tako, da je $\sigma i = i$ za vsak i, in predvidevamo, da ima prva vrstica enice natančno v prvih r_1 stolpcih. Ker smo izbrali konstanten τ, so stolpci $1, \ldots, r_1$ izbrisani, da lahko enačimo vseh $r_1!$ možnosti. R_1 je število tistih stolpcev, ki ostanejo, ko izbrišemo prvi stolpec. Ker je ista verjetnost, da bo prvi stolpec na katerikoli poziciji med tistimi r_1 stolpci, je R_1 enakomerno razporejen od 1 do r_1 in $G(R_1) = (r_1!)^{\frac{1}{r_1}}$. Linearnost upanja nam da

$$G(L) = G\left(\prod_{i=1}^{n} R_i\right) = \prod_{i=1}^{n} G\left(R_i\right) = \prod_{i=1}^{n} (r_i!)^{\frac{1}{r_i}}\,.$$

Splošni $G(L)$ geometrijska sredina pogojne vrednosti $G(L)$ in ima tako isto vrednost. Ta je

$$\mathrm{per}(A) \leq G(L) = \prod_{i=1}^{n} (r_i!)^{\frac{1}{r_i}}\,.$$

□

Poglavje 4

Slučajni grafi

Uporaba verjetnosti v teoriji grafov sloni na pojmu slučajnega grafa. Glavni model oziroma verjetnostni prostor slučajnih grafov $\mathcal{G}(n,p)$ je sestavljen iz vseh grafov z n vozlišči, par vozlišč pa je povezan z verjetnostjo p. Lahko je videti, da se nek graf G_0 z n vozlišči in m povezavami pojavi z verjetnostjo

$$\mathbf{P}(G_0) = p^m \cdot (1-p)^{\binom{n}{2}-m}.$$

Zgornja verjetnost določa pojavitev grafa s točno določenimi povezavami med označenimi vozlišči. Verjetnost, da pa je G izomorfen G_0 je seveda precej večja.
Graf $G \in \mathcal{G}$ imenujemo *slučajni graf* z n vozlišči in verjetnostjo povezave p. Vsako množico grafov v prostoru $\mathcal{G}(n,p)$ si lahko predstavljamo kot dogodek. Recimo, za vsako povezavo $e \in E(G)$ je množica

$$A_e = \{G : G \text{ je graf, ki vsebuje povezavo } e\}$$

dogodek, da je e povezava grafa G. Dogodki A_e so neodvisni in se pojavljajo z verjetnostjo p.

4.1 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 4.1 *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*

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

Dokaz. Verjetnost, da je neka določena množica $U \subseteq V(G)$ z močjo k v grafu G neodvisna, je enaka $(1-p)^{\binom{k}{2}}$. Trditev nato sledi iz dejstva, da je natanko $\binom{n}{k}$ takšnih množic U.

□

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

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

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:

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

in velja

$$\mathbf{E}(X_C) = \mathbf{P}(C \subseteq G) = p^k\,.$$

Takšne cikle predstavlja natanko $(n)_k$ zaporedij $v_0v_1\cdots v_{k-1}$ 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:

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

□

4.2 Lastnosti skoraj vseh grafov

Lastnost grafa je razred grafov, ki so zaprti za izomorfizem, torej razred vsebuje z vsakim grafom G še vse njemu izomorfne grafe. Če je $p = p(n)$ fiksna funkcija (lahko konstantna) in je $\mathcal{P}$ lastnost grafa, nas zanima obnašanje verjetnosti $P(G \in \mathcal{P})$ za $G \in \mathcal{G}(n,p)$, ko $n \to \infty$. Če gre verjetnost proti 1, rečemo da $G \in \mathcal{P}$ za *skoraj vse* $G \in \mathcal{G}(n,p)$, če pa gre proti 0, rečemo, da *skoraj noben* $G \in \mathcal{G}(n,p)$ nima lastnosti $\mathcal{P}$.

Za primer pokažimo, da je za določen p vsak fiksen graf H induciran podgraf na skoraj vseh grafih.

Trditev 4.3 *Za vsako konstanto $p \in (0,1)$ in vsak graf H, skoraj vsak $G \in \mathcal{G}(n,p)$ vsebuje inducirano kopijo H.*

Dokaz. Naj bo H dan in $k = |V(H)|$. Če $n \geq k$ in je $U \subseteq \{0, \ldots, n-1\}$ fiksna podmnožica na k vozliščih grafa G, potem je $G[U]$ izomorfen H z določeno verjetnostjo $r > 0$. Verjetnost r je odvisna od p, ne pa tudi od n. Graf G vsebuje $\lfloor \frac{n}{k} \rfloor$ takih disjunktnih množic U_i za ž $i = 1, \ldots, \lfloor \frac{n}{k} \rfloor$. Verjetnost, da noben izmed grafov $G[U_i]$ ni izomorfen H je $(1-r)^{\lfloor \frac{n}{k} \rfloor}$, saj so ti dogodki med sabo neodvisni zaradi disjunktnsti povezav iz množice $[U]^2$. Zato je

$$\mathbf{P}(H \underbrace{\not\subseteq}_{induciran} G) \leq (1-r)^{\lfloor \frac{n}{k} \rfloor} \to 0, \qquad \text{ko} \quad n \to \infty,$$

in trditev je dokazana.

□

Za sklepanje o velikem številu naravnih lastnosti, ki jih imajo skoraj vsi grafi, je priročna naslednja lema. Za dana $i, j \in \mathcal{N}$ definirajmo lastnost grafa $\mathcal{P}_{i,j}$. Rečemo da je graf $G \in \mathcal{P}_{i,j}$ (oz. graf G ima lastnost $\mathcal{P}_{i,j}$), če za vsak par U, W disjunktnih množic vozlišč z $|U| \leq i$ in $|W| \leq j$, graf vsebuje vozlišče $v \notin U \cup W$, ki je sosedno z vsemi vozlišči iz U in hkrati z nobenim iz W.

Lema 4.4 *Za vsako konstanto $p \in (0,1)$ in $i, j \in \mathbb{N}$, skoraj vsak graf $G \in \mathcal{G}(n,p)$ ima lastnost $\mathcal{P}_{i,j}$.*

Dokaz. Naj bo $q = 1 - p$. Za določena U, W in $v \in G - (U \cap W)$ je verjetnost, da je v sosed vsem vozliščem iz U ter nobenemu iz W

$$p^{|U|} q^{|W|} \geq p^i q^j$$

in zato je verjetnost, da ne obstaja ustrezen v za taka U in W

$$(1 - p^{|U|} q^{|W|})^{n-|U|-|W|} \leq (1 - p^i q^j)^{n-i-j}$$

(za $n \geq i + j$), saj so ustrezni dogodki med seboj neodvisni za različne v. Ker na vozliščih $V(G)$ ni več kot n^{i+j} parov takih množic U, W je verjetnost, da kak tak par nima ustrezenega vozlišča v največ

$$n^{i+j}(1 - p^i q^j)^{n-i-j},$$

to pa gre proti 0, ko $n \to \infty$, saj je $1 - p^i q^j < 1$.

□

Posledica 4.5 *Za vsak $p \in (0,1)$ in $k \in \mathcal{N}$ je skoraj vsak graf v $\mathcal{G}(n,p)$ k-povezan.*

Dokaz. Po lemi 4.4 ima skoraj vsak graf lastnost $\mathcal{P}_{2,k-1}$, zato je dovolj pokazat, da je vsak graf G z lastostjo $\mathcal{P}_{2,k-1}$ k-povezan. Poljuben graf v $\mathcal{P}_{2,k-1}$ je reda vsaj $k+2$. Če grafu G odstranimo manj kot k vozlišč mora biti povezan. Ta vozlišča damo v množico W, saj jo lahko poljubno izberemo in je moči manj kot k. Po definiciji $\mathcal{P}_{2,k-1}$ imata poljubni dve drugi vozlišči x, y, ki ju damo lahko v množico U, skupno sosednje vozlišče $v \notin W$. Zato W ne separira x in y. Graf G je res povezan.

□

V dokazu posledice 4.5 smo pokazali več kot je bilo potrebno. Namesto dokaza o obstoju poti med x in y, ki se izogne množici W, smo pokazali, da imata x in y skupnega soseda $v \notin W$. Zato so vse poti, ki so potrebne za vzpostavitev željene povezanosti, lahko dolžine 2.

Nadalje bomo pokazali, da ima skoraj vsak graf presenetljivo visoko kromatično število χ.

Trditev 4.6 *Za vsak $p \in (0,1)$ in vsak $\epsilon > 0$ ima skoraj vsak graf $G \in \mathcal{G}(n,p)$ kromatično število*

$$\chi(G) > \frac{\log(1/q)}{2+\epsilon} \cdot \frac{n}{\log(n)}.$$

Dokaz. Za poljuben $n \geq k \geq 2$, z uporabo leme 4.1 dobimo

$$P[\alpha(G) \geq k] \leq \binom{n}{k} q^{\binom{k}{2}} \leq n^k q^{\binom{k}{2}} = q^{\log_q(n^k)} q^{\frac{1}{2}k(k-1)}$$

$$= q^{k\frac{\log(n)}{\log(q)} + \frac{1}{2}k(k-1)} = q^{\frac{k}{2}(-\frac{2\log(n)}{\log(1/q)} + k - 1)}.$$

Za

$$k := (2+\epsilon)\frac{\log(n)}{\log(1/q)}$$

gre eksponent tega izraza z n proti neskončnosti, zato gre izraz proti 0. Torej nobena množica k vozlišč ne sme biti enako pobarvana, zato vsako barvanje vozlišč grafa G za skoraj vsak $G \in \mathcal{G}(n,p)$ uporablja več kot

$$\frac{n}{k} = \frac{\log(1/q)}{2+\epsilon} \cdot \frac{n}{\log(n)}$$

barv.

□

Trditev 4.6 je močna v smislu obeh mej, saj če zamenjamo ϵ z $-\epsilon$, se spodnja meja za χ spremeni v zgornjo.

Kot zanimivost omenimo skupno lastnost rezultatov v tem poglavju: vrednost p ne igra nobene vloge, saj če je veljala določena lastnost za skoraj vsak graf v $\mathcal{G}(n, \frac{1}{2})$, je imel to lastnost tudi skoraj vsak graf v $\mathcal{G}(n, \frac{1}{1000})$. Za večino primerov (zgornji primeri so izjema) se nahaja kritična velikost magnitude p, okoli katere se

lastnot ravno se bo oz. ne bo pojavila, veliko nižje od vsake konstante vrednosti in največkrat je to funkcija n-ja, ki gre proti 0, ko $n \to \infty$.

Poglejmo si, kaj se dogaja, če je $p = p(n)$. Za verjetnost povezav p, ki imajo red manjši od n^{-2}, skoraj gotovo slučajni graf $G \in \mathcal{G}(n,p)$ nima nobene povezave. Ko p raste, G pridobiva vedno več strukturiranosti. Nad mejo okoli $p = \sqrt{n}\,n^{-2}$ ima skoraj gotovo komponento z več kot dvemi vozliči, te komponente z večanjem reda rastejo in okoli $p = n^{-1}$ se pojavijo prvi cikli. Kmalu zatem postane graf neravninski, hkrati ena komnponenta nadvlada ostale, vse dokler ne postane pri meji okoli $p = (\log n)n^{-1}$ graf povezan. Ne veliko za tem, pri $p = (1+\epsilon)(\log n)n^{-1}$, ima graf skoraj gotovo Hamiltonov cikel.

Velikokrat se ta razvoj slučajnih grafov, ko p raste, primerja z evolucijo organizmov. Za vsak $p = p(n)$ si mislimo lastnosti skoraj vseh grafov v $\mathcal{G}(n,p)$ kot lastnosti tipičnega slučajnega grafa $G \in \mathcal{G}(n,p)$ in preučujmo, kako se s stopnjo rasti p spreminjajo lastnosti grafa G. Kot pri vrstah, se tudi evolucija slučajnih grafov zgodi v relativno nendadnih skokih. Kot že prej omenjene kritične meje verjetnosti so pragovi, pod katerimi skoraj noben graf nima in nad katerimi skoraj vsi grafi imajo mišljene lastnosti. Kasneje se bomo lotili splošne metode za izračun pragovih oz. pragovnih funkcij.

Poglavje 5

Metoda izbrisa

Osnovni pristop verjetnostne metode pokaže obstoj objekta z določenimi lastnosti tako s konstrukcijo verjetnostnega prostora in dokazom, da objekti z željeno lastnostjo v tem prostoru obstajajo s pozitivno verjetnostjo. Velikokrat takšen pristop ni uspešen. Takrat uporabimo drugo pot, ki jo bomo natančneje opisali v tem poglavju. Pokažemo, da obstaja objekt, ki skoraj zadostuje našim pogojem in ga lahko z nadzorovanimi popravki spremenimo v željenega. Krajše povedano, metoda izbrisa obravnava slučajno konfiguracijo, ki ni dobra, vendar je slaba le na nekaj mestih.

Preden se lotimo primerov, omenimo Markovo neenakost.

Izrek 5.1 (Markova neenakost) *Za nenegativno slučajno spremenljivko in $a > 0$ velja:*

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

Dokaz.

$$\mathbf{E}(X) = \sum_i i\,\mathbf{P}(X = i) \geq \sum_{i \geq a} a\,\mathbf{P}(X = i) = a\,\mathbf{P}(X \geq a).$$

□

5.1 Ramseyeva števila

Trditev 5.2 *Če $\binom{n}{k} 2^{1-\binom{k}{2}} < 1$, potem $R(k,k) > n$.*

Trditev 5.3 (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 enobarvna.

$$\mathbf{E}(X_S) = \mathbf{P}(S \text{ je enobarvna}) = 2^{1-\binom{k}{2}}.$$

Naj bo $X = \sum_S X_S$. Potem je $\mathbf{E}(X) = \sum_S E(X_S) = m$, 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 $R(k,k) > s \geq n - m$.

□

5.2 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 5.4 *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 $\mathbf{E}(X) = pn$ in $\mathbf{E}(Y) = \frac{nk}{2}p^2$. Potem je

$$\mathbf{E}(X - Y) = np - \frac{nk}{2}p^2.$$

Pri $p = \frac{1}{k}$, $\mathbf{E}(X - Y)$ doseže maksimum:

$$\mathbf{E}(X - Y) = \frac{n}{k} - \frac{n}{2k} = \frac{n}{2k}.$$

Torej obstaja množica točk 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 5.5 (Turan) *Za vsak graf G velja*

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

Dokaz. Naj $\preceq$ linearno ureja $V(G)$. Definirajmo

$$I = \{v \in V; vw \in E(G) \Rightarrow v \preceq w\}.$$

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

$$\mathbf{E}(X_v) = \mathbf{P}(v \in I) = \frac{1}{d_v + 1},$$

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

$$\mathbf{E}(X) = \sum_{v \in V} \frac{1}{d_v + 1}$$

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 $x \preceq y$ in $y \preceq x$, 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 5.6 (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 $\alpha(H) = \mathbf{E}(X)$. 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 $\alpha(H) = \mathbf{E}(X)$ sledi, da je H unija klik in je torej $H \cong G_{n,e}$.

□

5.3 Erdösev izrek

V tem razdelku bomo dokazali enega izmed bolj presenetljivih rezultatov v teoriji grafov.

Izrek 5.7 (Erdös, 1959) *Za vsak par naravnih števil g in k obstaja graf G z notranjim obsegom $g(G) > g$ in kromatičnim številom $\chi(G) > k$.*

Pri tem je *notranji obseg* dolžina najkrajšega cikla v grafu. V dokazu bomo uporabili še naslednjo standardno oznako iz kombinatorike

$$(n)_i := \binom{n}{i} i! = n(n-1)(n-2)\cdots(n-i+1)\,,$$

za število zaporedij i različnih elementov iz dane množice z n elementi.

Dokaz. Naj bo $\beta < 1/g$ in G vsebovan v razredu $\mathcal{G}(n,p)$, pri čemer je $p = n^{\beta-1}$. Nadalje, naj bo X slučajna spremenljivka, ki določa število ciklov dolžine kvečjemu g. Potem je matematično upanje te spremenljivke

$$\mathbf{E}(X) = \sum_{i=3}^{g} \frac{(n)_i}{2i}\, p^i \le \sum_{i=3}^{g} \frac{n^{i\beta}}{2i} \in o(n)\,,$$

saj je $\beta g < 1$. Po Markovi neenakosti verjetnost, da je število ciklov z dolžino kvečjemu g večje od $n/2$, je zato

$$\mathbf{P}(X \ge \frac{n}{2}) \in o(1)\,.$$

Definirajmo $\gamma = \lceil \frac{3}{p} \ln n \rceil$. Verjetnost, da je največja neodvisna množica $\alpha(G)$ velikosti vsaj γ je kvečjemu

$$\mathbf{P}(\alpha(G) \ge \gamma) \le \binom{n}{\gamma} (1-p)^{\binom{\gamma}{2}} < \left(ne^{-p(\gamma-1)/2}\right)^{\gamma} \in o(1)\,.$$

Naj bo n tako velik, da imata oba zgornja dogodka verjetnost manjšo od $\frac{1}{2}$. Potem obstaja nek graf G z manj kot $n/2$ ciklov dolžine g in neodvisno množico velikosti manj kot $3n^{1-\beta}\ln n$. Iz vsakega izmed ciklov dolžine kvečjemu g odstranimo eno vozlišče. Tako dobimo graf G' z vsaj $n/2$ vozlišči, ki ima notranji obseg večji od g in velikost neodvisne množice $\alpha(G') \le \alpha(G)$. Torej je kromatično število

$$\chi(G') \ge \frac{|G'|}{\alpha(G')} \ge \frac{n/2}{3n^{1-\beta}\ln n} = \frac{n^{\beta}}{6\ln n}\,.$$

Zagotoviti moramo le še, da je n dovolj velik, torej, da velja

$$k < \frac{n^{\beta}}{6\ln n}\,.$$

□

Poglavje 6

Metoda drugega momenta

Uporabnost matematičnega upanja smo spoznali že nekajkrat. V tem poglavju se ukvarjamo z določanjem verjetnosti, da je vrednost slučajne spremenljivke daleč od pričakovane. Če imamo zgolj podatek o matematičnem upanju spremenljivke, nam najboljšo vrednost poda Markova neenakost. Ko pa o porazdelitvi spremeljivke vemo več, postanejo tudi orodja bolj natančna. Eno izmed glavnih orodij je Čebiševa neenakost.

Matematično upanje imenujemo tudi prvi moment slučajne spremenljivke. Definiramo pa lahko tudi momente višjih redov. *Moment reda k* je $\mathbf{E}(X^k)$. Enostavno je videti, da za diskretno slučajno spremenljivko X velja

$$\mathbf{E}(X^k) = \sum_{\omega \in \Omega} p(\omega) \cdot X(\omega)^k \,.$$

Zanimiva je povezava med prvim in drugim momentom slučajne spremeljivke, varianca, ki smo jo opisali že v uvodu.

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 dovolj razlikuje od matematičnega upanja.

Lema 6.1 (Čebiševa neenakost) *Če ima slučajna spremenljivka X matematično upanje $\mathbf{E}[X]$ in (končno) varianco $\mathrm{Var}(X)$, za vsak pozitiven t velja ocena*

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

Dokaz.

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

□

Ocena ni nujno natančna. Če je $t^2 < \mathrm{Var}(X)$, je celo prazna, saj je tedaj njena desna stran večja od 1. Najboljšo oceno dobimo, če je X enak μ z verjetnostjo p ali enak $\mu \pm t$ z verjetnostjo $\frac{1-p}{2}$.

6.1 Ocena 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[1]. Z metodo drugega momenta na preprost način navzdol omejimo koeficient $\binom{2m}{m}$.

Trditev 6.2 *Za vsak $m \geq 1$ velja*

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

Dokaz. Naj bo X slučajna 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 oceno

$$\mathbf{P}(|X - m| < \sqrt{m}) \geq \frac{1}{2}.$$

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

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

□

6.2 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 takšne množice 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

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

[1] Catalanova števila lahko enostavno izrazimo z binomskimi koeficienti. Ta števila tvorijo zaporedje naravnih števil, ki se pojavljajo v mnogih praštevilskih in rekurzivnih problemih v kombinatoriki.

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, a vendar bolj natančno rešitev problema. Naj bo $\{x_1, x_2, \ldots, x_k\} \subset \{1, 2, \ldots, n\}$ množica z različnimi vsotami. Naj bodo $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$ neodvisne slučajne spremenljivke z verjetnostjo

$$\mathbf{P}(\varepsilon_i = 1) = \mathbf{P}(\varepsilon_i = 0) = \frac{1}{2}$$

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

$$\mathbf{P}(|X - \mu| \geq \frac{\lambda n\sqrt{k}}{2}) \leq \lambda^{-2}.$$

Po drugi strani pa

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

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

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

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 6.3

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

6.3 Pragovna funkcija

Vrnimo se sedaj k slučajnim grafom. Kakšna je verjetnost, da graf $G \in \mathcal{G}(n,p)$ vsebuje cikel dolžine tri? Lastnost, da graf vsebuje tak cikel je monotona, kar pomeni, da ima to lastnost tudi vsak graf H, ki G vsebuje kot podgraf. Za majhne p graf G verjetno 3-cikla ne bo vseboval, medtem ko je za velike p pojav bolj verjeten.

Naj bo T število 3-ciklov v grafu G. Za dano trojico vozlišč je verjetnost, da tvorijo 3-cikel p^3. Zaradi linearnosti matematičnega upanja, je pričakovano število trikotnikov

$$\mathbf{E}(T) = \binom{n}{3} p^3.$$

Če je $p := p(n) \ll \frac{1}{n}$, potem se pričakovana vrednost števila 3-ciklov bliža 0, ko večamo n. Zato se tudi verjetnost, da nek graf G 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 zagotovo 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 nekaj 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 metoda drugega momenta dokazuje, da če je pričakovana vrednost števila trikotnikov dovolj velika, potem slučajni graf skoraj zagotovo vsebuje nekaj trikotnikov.

Lema 6.4 *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

$$\lim_{n\to\infty} \mathbf{P}(X_n > 0) = 1.$$

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

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

Ker za $X_n = 0$ velja $|X_n - \mathbf{E}(X_n)| = |\mathbf{E}(X_n)|$, dobimo

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

□

Ocenimo varianco števila 3-ciklov v grafu G. Število trikotnikov T zapišemo kot $T = \sum_i T_i$, kjer so $T_1, T_2, \ldots$ indikatorske spremenljivke za vseh $\binom{n}{3}$ možnih trikotnikov v grafu G. 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 3-cikel velja

$$\mathrm{Var}(T_i) \leq \mathbf{E}(T_i^2) = p^3$$

in za vsak par 3-ciklov, 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 3-ciklov na petih določenih povezavah.

Indikatorske spremenljivke 3-ciklov, ki nimajo skupne povezave, so neodvisne, zato je kovarianca takih parov enaka 0. Torej seštevamo le kovarianco tistih parov 3-ciklov, ki imajo skupno povezavo. Število le teh je $12\binom{n}{4}$ in tako dobimo

$$\begin{aligned} \mathrm{Var}(T) &\leq \binom{n}{3} p^3 + 12\binom{n}{4} p^5 \leq n^3 p^3 + n^4 p^5 \\ \frac{\mathrm{Var}(T)}{\mathbf{E}(T)^2} &\leq \frac{n^3 p^3 + n^4 p^5}{(\binom{n}{3} p^3)^2} = O(\frac{1}{n^3 p^3} + \frac{1}{n^2 p}), \end{aligned}$$

kar limitira proti 0, če je $p(n) \gg \frac{1}{n}$. Po lemi 6.4 pa iz tega sledi, da se verjetnost, da graf G vsebuje 3-cikle, približuje 1 z naraščanjem n proti neskončnosti.

Za lastnost "graf vsebuje trikotnik", rečemo, da je $r(n) = \frac{1}{n}$ pragovna funkcija. Ta pojem sta vpeljala Erdös in Rényi.

Definicija 6.5 Funkcija $r : \mathbb{N} \to \mathbb{R}$ je *pragovna funkcija* za monotono lastnost $\mathcal{P}$ grafa $G \in \mathcal{G}(n,p)$, če za vsak $p : \mathbb{N} \to [0,1]$ velja:

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

Pragovna funkcija lahko obstaja lahko pa tudi ne. Tudi če obstaja, ni nujno, da je enolično določena. Kot smo že omenili za našo lastnost, da G vsebuje 3-cikel, je pragovna funkcija $r(n) = 1/n$. Vendar pa bi lahko namesto te funkcije 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 (vendar ne nujno induciranega, saj je ta problem veliko bolj zapleten). Izkaže se, da je naš pristop primeren tudi za bolj splošne lastnosti podgrafa, pod pogojem, da je ta uravnotežen. Preden pa povemo kaj je uravnotežen graf, definirajmo še gostoto grafa.

Naj bo H graf z v vozlišči in e povezavami. *Gostoto* grafa H definiramo kot

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

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

Izrek 6.6 *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 $G \in \mathcal{G}(n,p)$.*

Dokaz. Naj bo H graf z v vozlišči in e povezavami. Potem je gostota $\rho(H) = \frac{e}{v}$. Označimo vozlišča grafa H z $a_1, a_2, \ldots, a_v$. Za vsako urejeno v-terico $\beta = (b_1, b_2, \ldots, b_v)$ različnih vozlišč $b_1, b_2, \ldots, b_v \in V(G)$, $G \in \mathcal{G}(n,p)$, naj A_β označuje dogodek, da G vsebuje pravilno urejeno kopijo H na $(b_1, b_2, \ldots, b_v)$. To je, dogodek A_β se zgodi, če velja $b_i b_j \in E(G)$, vedno kadar velja $a_i a_j \in E(H)$. Z drugimi besedami,dogodek A_β se zgodi vedno ko je predpis $a_i \longrightarrow b_i$ homomorfizem na grafu.

Naj X_β označuje indikatorske spremenljivke nanašujoče se na A_β in naj bo $X = \sum_\beta X_\beta$ po vseh urejenih v- tericah β. Upoštevati moramo, da so zaradi možne simetrije H, nekatere kopije H lahko štete večkrat in tako X ni točno število kopij H v grafu G. Kakorkoli, pogoj $X = 0$ je ekvivalenten odsotnosti grafa H v G in $X > 0$ je ekvivalenten pojavu grafa H v grafu G.

Verjetnost A_β je p^e. Zaradi linearnosti matematičnega upanja pa velja

$$\mathbf{E}(X) = \sum_\beta \mathbf{P}(A_\beta) = \Theta(n^v p^e)$$

(upoštevati je treba, da sta v in e konstanti, medtem ko je p funkcija od n).

Če je $p(n) \ll n^{\frac{-v}{e}}$, potem je

$$\lim_{n\to\infty} \mathbf{E}(X) = 0,$$

s čimer je prvi korak dokazan.

Sedaj pa predpostavimo, da je $p(n) \gg n^{\frac{-v}{e}}$ in uporabimo lemo 1.7

$$\mathrm{Var}(X) = \sum_\beta \mathrm{Var}(X_\beta) + \sum_{\beta\neq\gamma} \mathrm{Cov}(X_\beta, X_\gamma).$$

Ker je $\mathrm{Var}(X_\beta) = \mathrm{Cov}(X_\beta X_\beta)$, lahko pišemo tudi

$$\mathrm{Var}(X) = \sum_{\beta,\gamma} \mathrm{Cov}(X_\beta X_\gamma)\,.$$

Kovarianca je neničelna le za pare kopij, ki si delijo nekaj povezav. Naj si β in γ delita $t \geq 2$ vozlišč. Potem imata dve kopiji H največ $t\rho$ skupnih povezav (saj je H uravnotežen), njuna unija pa vsebuje vsaj $2e - t\rho$ povezav. Tako je

$$\mathrm{Cov}(X_\beta X_\gamma) \leq \mathbf{E}(X_\beta X_\gamma) \leq p^{2e-t\rho}.$$

Število parov β in γ, ki si delijo t vozlišč je reda $O(n^{2v-t})$, saj lahko izberemo množico vozlišč moči $2v - t\rho$ na $\binom{n}{2v-t}$ načinov. Za fiksen t dobimo

$$\sum_{|\beta\cap\gamma|=t} \mathrm{Cov}(X_\beta, X_\gamma) = O(n^{2v-t}p^{2e-t\rho}) = O((n^v p^e)^{2-t/v})$$

$$\mathrm{Var}(X) = O(\sum_{t=2}^{v}(n^v p^e)^{2-t/v})$$

in

$$\lim_{n\to\infty} \frac{\mathrm{Var}(X)}{\mathbf{E}(X)^2} = \lim_{n\to\infty} O(\sum_{t=2}^{v}(n^v p^e)^{-t/v}) = 0,$$

če je $\lim_{n\to\infty} n^v p^e = \infty$. S tem pa je izrek dokazan, saj po lemi 6.4 velja

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

in tako se skoraj vedno pojavi kopija H v grafu G.

□

Vprašanje pojava splošnih podgrafov H v grafu sta rešila Erdös in Rényi. Pragovna funkcija za graf H je določena s podgrafom $\bar{H} \subset H$, ki ima maksimalno gostoto. Velja naslednji izrek.

Izrek 6.7 *Naj bo H graf in $\bar{H} \subset H$ z maksimalno gostoto ρ. Potem je*

$$r(n) = n^{\frac{-1}{\rho(H)}}$$

pragovna funkcija za lastnost, da je H podgraf grafa $G \in \mathcal{G}(n,p)$.

6.4 Klično število

Maksimalna klika je klika, ki ni vsebovana v nobeni drugi kliki. *Klično število* $\omega(G)$ je velikost največje klike v grafu G.

Obravnavali bomo klično število v slučajnem grafu $G \in \mathcal{G}(n, 1/2)$. Najprej za fiksno število k preštejmo število klik velikosti k. Za vsako množico S, ki vsebuje k točk, naj X_S označi indikatorsko spremenljivko dogodka, da je S klika. Potem je $X = \sum_{|S|=k} X_S$ število k-klik v grafu. Pričakovano število k-klik v grafu je

$$\mathbf{E}(X) = \sum_{|S|=k} \mathbf{E}(X_S) = \binom{n}{k} 2^{-\binom{k}{2}}.$$

Ta funkcija pade pod 1 približno pri $k = 2\log_2 n$, ki je tipična velikost največje klike v G. Velja

Lema 6.8

$$\lim_{n\to\infty} \mathbf{P}(\omega(G(n,1/2)) > 2\log_2 n) = 0.$$

Dokaz. Postavimo $k(n) = \lceil 2\log_2 n \rceil$ in izračunajmo povprečno število klik te velikosti

$$\mathbf{E}(X) = \binom{n}{k} 2^{-\binom{k}{2}} = \frac{n!}{k!(n-k)!} 2^{-k(k-1)/2} \leq \frac{(2^{k/2})^k}{k!} 2^{-k(k-1)/2} = \frac{2^{k/2}}{k!},$$

saj je

$$\frac{n!}{(n-k)!} \leq n^k = (2^{(\log_2 n)})^k \leq (2^{\frac{\lceil 2\log_2 n \rceil}{2}})^k = (2^{k/2})^k.$$

$\frac{2^{k/2}}{k!}$ pa gre proti 0, ko gre $n \to \infty$. Zato je

$$\lim_{n\to\infty} \mathbf{P}(\omega(G(n,1/2)) > 2\log_2 n) = 0.$$

□

Težje je pojasniti, da bo vedno obstajala klika velikosti blizu praga $2\log_2 n$, kar bomo dokazali. Še prej pa ponovimo lemo, ki jo bomo potrebovali v dokazu. Dokaz leme izpustimo.

Izrek 6.9 *Naj bo $k(n)$ taka funkcija, da bo*

$$\lim_{n\to\infty} \binom{n}{k(n)} 2^{-\binom{k(n)}{2}} = \infty.$$

Potem velja

$$\lim_{n\to\infty} \mathbf{P}(\omega(G \in \mathcal{G}(n,1/2)) \geq k(n)) = 1.$$

Dokaz. Pišimo $E(n,k) = \binom{n}{k} 2^{-\binom{k}{2}}$. Najprej opazimo, da lahko predpostavimo, da je n dovolj velik in da je dovolj gledati le tiste k, za katere velja

$$\frac{3}{2}\log_2 n \leq k < 2\log_2 n,$$

kjer lahko $\frac{3}{2}$ zamenjamo s katerokoli konstanto, manjšo od 2. Pokazali smo že, da $E(n, 2\log_2 n) \to 0$, ko $n \to \infty$. Pokazati moramo še $E(n, \frac{3}{2}\log_2 n) \to \infty$, ko $n \to \infty$. Najprej ocenimo $\log_2 E(n,k)$:

$$\log_2 E(n,k) \geq \log_2[(\frac{n}{k})^k 2^{-k^2/2}] = k\log_2 n - k\log_2 k - \frac{k^2}{2}.$$

Zdaj namesto k vstavimo $\frac{3}{2}\log_2 n$ in dobimo

$$\begin{aligned} \log_2 E(n, \frac{3}{2}\log_2 n) &\geq \frac{3}{2}\log_2^2 n - o(\log_2^2 n) - \frac{9}{8}\log_2^2 n \\ &= \frac{3}{8}\log_2^2 n - o(\log_2^2 n) \to \infty, \end{aligned}$$

ko $n \to \infty$. Torej res velja $E(n, \frac{3}{2}\log_2 n) \to \infty$, ko $n \to \infty$.

Naj $X = \sum_{|S|=k(n)} X_S$ označi število klik velikosti $k(n)$ v $G(n, 1/2)$. Po predpostavki izreka velja $\lim_{n\to\infty} \mathbf{E}[X] = \infty$. Ker želimo uporabiti lemo, moramo izračunati disperzijo X:

$$D(X) = \sum_{|S|=|T|=k} \mathrm{Cov}(X_S, X_T)$$

(zajeli smo vse množice velikosti k, tudi kadar je $S = T$, saj je $D(X) = \mathrm{Cov}(X, X)$). Vemo, da je $\mathrm{Cov}(X_S, X_T)$ enaka 0, če sta X_S in X_T neodvisni slučajni spremenljivki. Spremenljivki X_S in X_T pa sta neodvisni, kadar imata S in T kvečjemu eno skupno točko (zato pripadajoče klike nimajo skupnih povezav). Torej nas zanimajo le tisti pari (S, T), za katere velja $|S \cap T| \geq 2$.

$D(X)$ lahko zapišemo kot

$$D(X) = \sum_{t=2}^{k} C(t),$$

kjer je

$$C(t) = \sum_{|S\cap T|=t} \mathrm{Cov}(X_S, X_T).$$

Za fiksen $t = |S \cap T|$ imajo klike na S in T skupaj $2\binom{k}{2} - \binom{t}{2}$ povezav, torej velja

$$\mathrm{Cov}(X_S, X_T) \leq \mathbf{E}(X_S X_T) = 2^{\binom{t}{2} - 2\binom{k}{2}}.$$

Ker lahko par podmnožic (S, T) z $|S| = |T| = k$ in $|S \cap T| = t$ izberemo na $\binom{n}{k}\binom{k}{t}\binom{n-k}{k-t}$ načinov, je

$$C(t) \leq \binom{n}{k}\binom{k}{t}\binom{n-k}{k-t} 2^{\binom{t}{2} - 2\binom{k}{2}}.$$

Pokazati moramo, da velja

$$\frac{D(X)}{(\mathbf{E}(X))^2} = \sum_{t=2}^{k} \frac{C(t)}{\mathbf{E}(X)^2} \;\to\; 0,$$

saj lahko nato uporabimo lemo. Vsoto razbijemo glede na t na dva dela. Zaradi lažjega računanja predpostavimo, da je $k = k(n)$ sodo.

V prvem delu, kjer je $2 \leq t \leq \frac{k}{2}$, pokažimo, da gre vsota proti 0. Pri ocenjevanju bomo potrebovali, da je $k < 2\log_2 n$. Ker imamo produkt več binomskih koeficientov, jih razširimo, saj se bo kaj pokrajšalo ali lahko kaj ustrezno združimo.

Ocenimo

$$\begin{aligned}
\frac{C(t)}{\mathbf{E}(X)^2} &\leq \frac{\binom{n}{k}\binom{k}{t}\binom{n-k}{k-t}}{(\binom{n}{k})^2 2^{-2\binom{k}{2}}} 2^{\binom{t}{2}-2\binom{k}{2}} \leq \frac{\binom{k}{t}\binom{n-k}{k-t}}{\binom{n}{k}} 2^{\binom{t}{2}} \\
&\leq \frac{k^t}{t!} \cdot \frac{(n-k)(n-k-1)\cdots(n-2k+t+1)}{(k-t)!} \cdot \frac{k!}{n(n-1)\cdots(n-k+1)} \cdot 2^{\binom{t}{2}} \\
&\leq k^{2t} \frac{1}{n(n-1)\cdots(n-k+1)\cdot t!} \cdot 2^{t^2/2} \leq k^{2t} n^{-t} 2^{t^2/2} \\
&\leq k^{2t}(2^{-k/2})^t 2^{t^2/2} = (k^2 2^{-k/2} 2^{t/2})^t \leq (k^2 2^{-k/4})^t,
\end{aligned}$$

saj je $t \leq \frac{k}{2}$. Lahko zapišemo

$$\sum_{t=2}^{k/2} \frac{C(t)}{\mathbf{E}(X)^2} \leq \sum_{t=2}^{k/2} q^t,$$

kjer je $q = k^2 2^{-k/4} = o(1)$ in tako gre vsota na levi proti 0.

V drugem delu, kjer velja $\frac{k}{2} < t \leq k$, pokažimo, da je $\sum_{t=k/2+1}^{k} C(t)/\mathbf{E}(X)) = o(1)$ za $k \geq \frac{3}{2}\log_2 n$. Ker je $\mathbf{E}(X) \to \infty$, bo veljalo tudi $\sum_{t=k/2+1}^{k} C(t)/(\mathbf{E}(X))^2 \to 0$. V tem delu je lažje oceniti binomske koeficiente. Pri ocenjevanju uporabimo formulo $\binom{n}{k} \leq n^k$ in dobimo

$$\begin{aligned}
\frac{C(t)}{\mathbf{E}(X)} &\leq \binom{k}{t}\binom{n-k}{k-t} 2^{\binom{t}{2}-\binom{k}{2}} \leq \binom{k}{k-t}\binom{n}{k-t} 2^{\binom{t}{2}-\binom{k}{2}} \\
&\leq k^{k-t} n^{k-t} 2^{(t^2-k^2-t+k)/2} \\
&= (kn)^{k-t} 2^{-(k-t)(k+t-1)/2} = (kn 2^{-(k+t-1)/2})^{k-t} \\
&\leq (2^{\log_2 k + (2/3)k - (k+t-1)/2})^{k-t} \\
&\leq (2^{\log_2 k + (2/3)k - (3/4)k})^{k-t},
\end{aligned}$$

saj je $t > \frac{k}{2}$. Ker je $2^{\log_2 k + (2/3)k - (3/4)k} = o(1)$, po ocenjevanju z geometrijskimi vrstami sledi, da velja $\sum_{t=k/2+1}^{k} C(t)/\mathbf{E}(X)^2 \to 0$, kot smo trdili. Dokazali smo torej, da je $\lim_{n\to\infty} D(X)/(\mathbf{E}(X))^2 = 0$. Po lemi sledi $\lim_{n\to\infty} \mathbf{P}(X > 0) = 1$. Torej je $\lim_{n\to\infty} \mathbf{P}(\omega(G(n,1/2)) \geq k(n)) = 1$.

□

Opomba 6.10 Če izberemo $k(n) = (2-\varepsilon)\log_2 n$, pogoji izreka veljajo za vsak $\varepsilon > 0$. To pomeni, da število klik $\omega(G(n,1/2))$ vedno leži med $(2-\varepsilon)\log_2 n$ in $2\log_2 n$. Koncentracija števila klik je celo močnejša. Leta 1976 so Bollobás, Erdös in Matula dokazali, da obstaja taka funkcija $k(n)$, da velja

$$\lim_{n\to\infty} \mathbf{P}(k(n) \leq \omega(G(n,1/2)) \leq k(n)+1) = 1.$$

Poglavje 7

Lovaszeva 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 $\mathbf{P}(A_1 \cup A_2 \cup \cdots \cup A_n) \leq \sum \mathbf{P}(A_i)$. Če je vsota $\sum \mathbf{P}(A_i)$ 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 $\sum \mathbf{P}(A_i)$ veliko večja kot $\mathbf{P}(A_1 \cup A_2 \cup \cdots \cup A_n)$.

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

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

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:

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

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

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

Potem velja

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

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 $S \subset \{1, 2, \ldots, n\}$ in $i \notin S$ pokažemo, da je

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

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

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

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

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

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

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

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

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

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

$$\mathbf{P}\big(\bigcap_{i=1}^{n} \bar{A}_i\big) = \mathbf{P}(\bar{A}_1)\mathbf{P}(\bar{A}_2|\bar{A}_1) \cdots \mathbf{P}(\bar{A}_n|\bar{A}_1 \cap \cdots \cap \bar{A}_{n-1}) \geq \prod_{(i=1}^{n}(1 - x_i).$$

□

7.1 Variante lokalne leme

Izrek 7.2 (Simetrična Lovaszova lokalna lema) *Naj bodo $A_1, A_2, \ldots, A_n$ dogodki, za katere je $\mathbf{P}(A_i) \leq p$. Naj za vsak $i = 1, 2, \ldots, n$ 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*

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

Dokaz. Če je $d = 0$, so dogodki med seboj neodvisni in zato velja $\mathbf{P}\big(\bigcap_{i=1}^{n} \bar{A}_i\big) = \mathbf{P}(\bar{A}_1)\mathbf{P}(\bar{A}_2)\cdots\mathbf{P}(\bar{A}_n) > 0$.

Naj bo $x_i = \frac{1}{d+1} < 1$. V odvisnostnem grafu je izhodna 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 $\mathbf{P}\big(\bigcap_{i=1}^{n} \bar{A}_i\big) \geq \prod_{i=1}^{n}(1 - x_i) > 0$.

□

Izrek 7.3 *Naj bo $\mathcal{E} = \{A_1, A_2, \ldots, A_n\}$ množica dogodkov tako, da je vsak A_i vzajemno neodvisen od dogodkov $\mathcal{E} \setminus (\mathcal{D}_i \cup A_i)$, kjer je $\mathcal{D}_i \subseteq \mathcal{E}$. Če obstajajo naravna števila $t_1, \ldots, t_n \geq 1$ in realno število $0 \leq p < \frac{1}{8}$ tako, da za vsak $i \in \{1, \ldots, n\}$ velja*

$$\mathbf{P}(A_i) \leq p^{t_i} \quad in \quad \sum_{A_j \in \mathcal{D}_i} (2p)^{t_j} \leq \frac{t_i}{4},$$

potem se nobeden od dogodkov iz $\mathcal{E}$ s pozitivno verjetnostjo ne zgodi.

Dokaz. Naj bo $\mathcal{E} = \{A_1, A_2, \ldots, A_n\}$ taka množica dogodkov, da je vsak dogodek A_i vzajemno neodvisen od dogodkov $\mathcal{E} \setminus (\mathcal{D}_i \cup A_i)$, kjer je $\mathcal{D}_i \subseteq \mathcal{E}$. Če obstajajo taka realna števila $x_1, x_2, \ldots, x_n \in [0, 1)$, da za vsak $1 \leq i \leq n$ velja

$$\mathbf{P}(A_i) \leq x_i \prod_{A_j \in \mathcal{D}_j} (1 - x_j),$$

potem je

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

Izberemo $x_i = (2p)^{t_i}$, za katera velja $0 \leq x_i \leq \left(\frac{1}{4}\right)^{t_i} < \frac{1}{2}$. Od tod sledi $1 - x_i \geq e^{-2x_i}$. Izpeljimo oceno za $\mathbf{P}(A_i)$:

$$\begin{aligned} x_i \prod_{A_j \in \mathcal{D}_j} (1 - x_j) &\geq x_i \prod_{A_j \in \mathcal{D}_j} e^{-2x_j} \geq x_i e^{-2\sum_{A_j \in \mathcal{D}_j} x_j} \\ &\geq (2p)^{t_i} e^{-2\sum_{A_j \in \mathcal{D}_j} (2p)^{t_j}} \geq (2p)^{t_i} e^{-2\frac{t_i}{4}} = 2^{t_i} p^{t_i} e^{-\frac{t_i}{2}}. \end{aligned}$$

Po predpostavki naloge je $p^{t_i} \geq \mathbf{P}(A_i)$ ter $2^{t_i} e^{-\frac{t_i}{2}} = (2e^{-\frac{1}{2}})^{t_i} \doteq 1.2^{t_i}$. Zato je

$$x_i \prod_{A_j \in \mathcal{D}_j} (1 - x_j) \geq 2^{t_i} e^{-\frac{t_i}{2}} p^{t_i} \geq \mathbf{P}(A_i).$$

Po splošni asimetrični Lovaszevi lokalni lemi sledi

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

Nobeden od dogodkov iz $\mathcal{E}$ se s pozitivno verjetnostjo ne zgodi.

□

Oglejmo si nekoliko drugačno obliko asimetrične Lovaszove lokalne leme:

Izrek 7.4 *Naj bodo $\mathcal{E} = \{A_1, A_2, \ldots, A_n\}$ takšni dogodki, da je vsak A_i vzajemno neodvisen od $\mathcal{E} \setminus (\mathcal{D}_i \cup A_i)$, kjer je $\mathcal{D}_i \subseteq \mathcal{E}$. Če za vsak $1 \leq i \leq n$ velja*

- $\mathbf{P}(A_i) \leq \frac{1}{8}$ *in*
- $\sum_{A_j \in \mathcal{D}_i} \mathbf{P}(A_j) \leq \frac{1}{4}$,

potem se s pozitivno verjetnostjo nobeden od dogodkov A_i ne zgodi.

Dokaz. Vzamemo $x_i = 2\mathbf{P}(A_i)$ in zaradi predpostavke $\mathbf{P}(A_i) \leq \frac{1}{8}$ velja $x_i \leq \frac{1}{4}$. Od tod sledi $(1 - x_i) \geq e^{-2x_i}$, $x_i \in [0, \frac{1}{4}]$. Izpeljemo:

$$\begin{aligned} x_i \prod_{A_j \in \mathcal{D}_i} (1 - x_j) &\geq x_i \prod_{A_j \in \mathcal{D}_i} e^{-2x_j} \geq 2\mathbf{P}(A_i) e^{-2\sum_{A_j \in \mathcal{D}_i} 2\mathbf{P}(A_j)} \\ &\geq 2\mathbf{P}(A_i) e^{-0.5} \geq \mathbf{P}(A_i), \end{aligned}$$

saj velja $2\ e^{-0.5} \doteq 1.2$. Po asimetrični Lovaszevi lokalni lemi se s pozitivno verjetnostjo nobeden od dogodkov A_i ne zgodi.

□

7.2 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 7.5 *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-obarvljiv.*

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

□

7.3 Izpolnjivost SAT problema

Izrek 7.6 *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 $\mathbf{P}(A_i) = 2^{-k} = p$.

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 $\mathbf{P}(\bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_m) > 0$, kar pomeni, da je verjetnost, da je k-SAT problem rešljiv, pozitivna.

□

7.4 Seznamsko barvanje vozlišč

Izrek 7.7 *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 $A_{c,e}$: $\mathbf{P}(A_{c,e}) = \frac{1}{l^2} = p$, 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.

□

7.5 Usmerjeni cikli

Izrek 7.8 *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

$$N^+(v) \cap (N^+(w) \cup \{w\}) = \emptyset. \tag{7.1}$$

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 (7.1). 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 $v_iv_{i+1} \in E$ 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.

□

7.6 Redka barvanja

Izrek 7.9 *Barvanje je* α-redko, *če za vsako barvo* c *in vsako točko* v *je največ* α *sosedov točke* v *obarvanih z barvo* c. *Dokaži, da ima graf z maksimalno stopnjo* $\Delta \geq \alpha^{\alpha}$ α*-redko barvanje z največ* $16\Delta^{1+\frac{1}{\alpha}}$ *barvami.*

Dokaz. Pobarvajmo graf G tako, da vsaki točki slučajno izberemo barvo s seznama $\{1, 2, \ldots, c\}$. Vse barve so izbrane z verjetnostjo $p = \frac{1}{c}$. Naj bo $c = 16\Delta^{1+\frac{1}{\alpha}}$. Sedaj definiramo dve vrsti dogodkov:

- Za vsako povezavo (u, v) naj bo $A_{u,v}$ dogodek, da sta točki u in v enako obarvani.
- Za vsako množico točk $\{u_1, u_2, \ldots, u_{\alpha+1}\}$, ki so sosednje točki v, naj bo $B_{\{u_1,\ldots,u_{\alpha+1}\}}$ dogodek, da so točke $u_1, u_2, \ldots, u_{\alpha+1}$ enake barve.

Če se nobeden od teh dogodkov ne zgodi, smo našli α-redko barvanje grafa G.

Najprej izračunajmo verjetnosti dogodkov $A_{u,v}$ in $B_{\{u_1,\ldots,u_{\alpha+1}\}}$:

$$\mathbf{P}(A_{u,v}) \leq c\ \frac{1}{c}\ \frac{1}{c} = \frac{1}{c} \leq \frac{1}{8},$$

$$\mathbf{P}(B_{\{u_1,\ldots,u_{\alpha+1}\}}) \leq c\left(\frac{1}{c}\right)^{\alpha+1} = \frac{1}{c^{\alpha}} \leq \frac{1}{8}.$$

Izberimo poljuben dogodek in si oglejmo, koliko dogodkov je odvisnih od njega. V nadaljevanju dokažemo, da je od njega odvisnih največ $(\alpha+1)\Delta$ dogodkov tipa $A_{u,v}$ in največ $(\alpha+1)\Delta\binom{\Delta}{\alpha}$ dogodkov tipa $B_{\{u_1,\ldots,u_{\alpha+1}\}}$. Naj bo izbrani dogodek tipa $B_{\{u_1,\ldots,u_{\alpha+1}\}}$ za točko v (v tem primeru dobimo več odvisnih dogodkov). Od njega so odvisni dogodki

$$\{A_{u_i,w};\ i = 1, 2, \ldots, \alpha+1,\ w \text{ sosed } u_i\}.$$

Teh je torej $(\alpha+1)\Delta$, saj ima vsaka izmed točk u_i, ki jih je $(\alpha+1)$, največ Δ sosedov. Označimo $d(A_{u,v}) = (\alpha+1)\Delta$.

Od dogodka $B_{\{u_1,\ldots,u_{\alpha+1}\}}$ so odvisni tudi dogodki

$$\{B_{\{u_i,w_1,\ldots,w_\alpha\}};\ i=1,2,\ldots,\alpha+1;\ w \text{ sosed } u_i,\ w_j \text{ sosed } w \neq u_i,\ j=1,2,\ldots,\alpha\}.$$

Teh dogodkov pa je $(\alpha+1)\Delta\binom{\Delta}{\alpha}$. Točk u_i je $(\alpha+1)$, vsaka pa ima največ Δ sosedov w. Izmed sosedov točke w izberemo α točk w_j na $\binom{\Delta}{\alpha}$ načinov. Označimo $d(B_{\{u_1,\ldots,u_{\alpha+1}\}}) = (\alpha+1)\Delta\binom{\Delta}{\alpha}$.

Sedaj izračunajmo:

$$\begin{aligned}
\sum_{A_i\in\mathcal{D}_i}\mathbf{P}(A_i) &= \sum_{A_{u,v}\in\mathcal{D}_i}\mathbf{P}(A_{u,v}) + \sum_{B_{\{u_i,w_1,\ldots,w_\alpha\}}\in\mathcal{D}_i}\mathbf{P}(B_{\{u_i,w_1,\ldots,w_\alpha\}}) \\
&= (\alpha+1)\Delta\frac{1}{c} + (\alpha+1)\Delta\binom{\Delta}{\alpha}\frac{1}{c^\alpha} \\
&\leq \frac{(\alpha+1)\Delta}{c} + \frac{(\alpha+1)\Delta^{\alpha+1}}{\alpha!\ c^\alpha} = \frac{(\alpha+1)\Delta}{16\Delta^{1+\frac{1}{\alpha}}} + \frac{(\alpha+1)\Delta^{\alpha+1}}{\alpha!\ (16\Delta^{1+\frac{1}{\alpha}})^\alpha} \\
&= \frac{(\alpha+1)}{16\Delta^{\frac{1}{\alpha}}} + \frac{(\alpha+1)}{\alpha!\ 16^\alpha} \leq \frac{(\alpha+1)}{16(\alpha^\alpha)^{\frac{1}{\alpha}}} + \frac{(\alpha+1)}{\alpha!\ 16^\alpha} \\
&= \frac{(\alpha+1)}{16\alpha} + \frac{(\alpha+1)}{\alpha!\ 16^\alpha}\,.
\end{aligned}$$

Dokazati je potrebno, da za izraz velja neenakost $\sum_{A_i\in\mathcal{D}_i}\mathbf{P}(A_i) \leq \frac{1}{4}$. Oglejmo si robni vrednosti:

- $\alpha = 1$:
$$\frac{(\alpha+1)}{16\alpha} + \frac{(\alpha+1)}{\alpha!\ 16^\alpha} = \frac{2}{16} + \frac{2}{16} = \frac{1}{4}.$$
- $\alpha \to \infty$:
$$\frac{(\alpha+1)}{16\alpha} \to \frac{1}{16}, \quad \frac{(\alpha+1)}{\alpha!\ 16^\alpha} \to 0,$$
$$\frac{(\alpha+1)}{16\alpha} + \frac{(\alpha+1)}{\alpha!\ 16^\alpha} \to \frac{1}{16} < \frac{1}{4}.$$

Po asimetrični Lovaszevi lokalni lemi, ki smo jo dokazali na začetku, se s pozitivno verjetnostjo nobeden od odvisnih dogodkov ne zgodi.

□

Poglavje 8

Koncentracija slučajnih spremenljivk

V tem poglavju predstavimo tri neenakosti, ki nam pomagajo določiti vrednosti, okoli katerih se slučajne spremenljivke koncentrirajo.

8.1 Černova neenakost

Izrek 8.1 (Černov) *Naj bodo $X_1, \ldots, X_n$ 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*

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

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 $e^{-t^2/2n} = e^{-t^2/2\sigma^2}$.

□

Izrek 8.2 *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*

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

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

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

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 8.3 *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 $S \in \mathcal{F}$.

□

8.2 Talagrandova neenakost

Izrek 8.4 (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

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

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 8.4 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 $\mathbf{E}(A) = \frac{n}{2}$, vendar:

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

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:

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

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

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

Včasih potrebujemo rezultat naslednjega tipa:

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

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

Izrek 8.5 (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 $0 \leq t \leq \mathbf{E}(X)$ *potem velja*

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

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

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

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.

8.3 Koncentracija vozlišč regularnih grafov

Izrek 8.6 *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.

□

8.4 Naraščajoča podzaporedja

Izrek 8.7 *Naj bo $\sigma = [x_1, x_2, \ldots, x_n]$ poljubna uniformno izbrana permutacija iz S_n ter naj bo X dolžina najdaljšega naraščajočega podzaporedja v σ. Potem je X skoncentrirana.*

Dokaz. Najprej konstruirajmo naključno permutacijo. Izberemo n naključnih realnih števil $y_1, y_2, \ldots, y_n$ z intervala $[0, 1]$. Ker so si števila $y_1, y_2, \ldots, y_n$ z verjetnostjo 1 med seboj različna, jih lahko uredimo v strogo naraščajočem vrstnem redu. Vrstni red indeksov pri tem predstavlja enolično permutacijo števil $1, 2, \ldots, n$. Elementarni dogodek T_i bo torej slučajna izbira števila $y_i \in [0, 1]$.

Sprememba števila y_i lahko spremeni spremenljivko X za največ 1, saj sprememba števila v zaporedju lahko spremeni lego nekega člena, s tem pa tudi zaporedje indeksov v permutaciji. Vendar se dolžina najdaljšega naraščajočega podzaporedja v σ v tem primeru spremeni kvečjemu za 1. Velja torej $c = 1$.

Naj bo $X \geq s$, potem X določa teh s števil ne glede na ostala števila. Sledi $r = 1$.

Velja Talagrandova neenakost

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

Izrek 1 [?]: Izmed n točk z naraščajočo absciso vedno lahko izberemo vsaj $\sqrt{n}$ takih točk, ki imajo bodisi monotono naraščajočo bodisi monotono padajočo ordinato.

Permutacijo σ lahko zapišemo kot zaporedje točk $(1, \sigma(1)), (2, \sigma(2)), \ldots, (n, \sigma(n))$, ki imajo naraščajočo absciso. Po izreku ima torej vsaj $\sqrt{n}$ točk naraščajočo ordinato in sledi $\mathbb{E}(X) \geq \sqrt{n}$. V tem primeru eksponent v Talagrandovi neenakosti ni konstanta.

□

8.5 Barvanje redkih grafov

Izrek 8.8 *Obstaja (velik) Δ_0 tako, da če je G maksimalne stopnje $\Delta \geq \Delta_0$ in $B \geq \Delta(\log \Delta)^3$ in ima soseščina pri vsaki točki največ $\binom{\Delta}{2} - B$ povezav, potem je $\chi(G) \leq \Delta + 1 - \frac{B}{e^6 \Delta}$.*

Dokaz. Trdimo, da v soseščini vsake točke obstaja vsaj $\frac{B}{e^6\Delta}$ barv, ki se pojavijo vsaj dvakrat. Če je to res, lahko s požrešno metodo pobarvamo sosede točke v z največ $\Delta - \frac{B}{e^6\Delta}$ barvami. Ena barva tako ostane za točko v. Tako velja $\chi(G) \leq \Delta + 1 - \frac{B}{e^6\Delta}$.

Sedaj dokažimo navedeno trditev. Naj bo $c = \lfloor \frac{\Delta}{2} \rfloor$. Pobarvamo vsako točko z eno izmed barv $1, 2, \ldots, c$. Barve izbiramo enakomerno in neodvisno. Če sta sosednji

točki po barvanju obarvani z enako barvo, obe razbarvamo. To naredimo z vsemi takimi sosedi.

Naj X_v predstavlja število barv, ki se ohranijo pri vsaj dveh barvah v soseščini točke v, hkrati pa se ta barva v soseščini v ni razbarvala. Za točko v definirajmo dogodek A_v, da je $X_v < \frac{B}{e^6\Delta}$. Množica $\mathcal{E} = \{A_v;\ v \in V(G)\}$ predstavlja slabe dogodke. Dokazati je potrebno, da se s pozitivno verjetnostjo nobeden od dogodkov iz množice $\mathcal{E}$ ne zgodi.

Dogodek A_v je odvisen od sosedov točke v in sosedov sosedov točke v. Definirajmo množico od A_v odvisnih dogodkov $S_v = \{A_w;\ v \text{ in } w \text{ sta na razdalji } \leq 4\}$. Teh dogodkov je

$$|S_v| = \Delta + \Delta(\Delta-1) + \Delta(\Delta-1)^2 + \Delta(\Delta-1)^3 < \Delta^4 = d.$$

Dogodek A_v je vzajemno neodvisen od dogodkov $\mathcal{E} \setminus S_v$. Če za poljubno točko v velja $P(A_v) \leq \frac{1}{4\Delta^5} = p$, potem je

$$4pd < 4\ \frac{1}{4\Delta^5}\ \Delta^4 = \frac{1}{\Delta} < 1.$$

Po simetrični Lovaszevi lokalni lemi sledi $P(\bar{A}_{v_1} \cap \bar{A}_{v_2} \cap \ldots \cap \bar{A}_{v_n}) > 0$. Torej se s pozitivno verjetnostjo nobeden od teh dogodkov ne zgodi.

□

Dokazati je potrebno še, da velja $P(A_v) \leq \frac{1}{4\Delta^5}$. Dokažimo najprej dve lemi.

Lema 8.9 $\mathbb{E}(X_v) \geq \frac{2B}{e^6\Delta}$.

Dokaz. Naj bo X'_v število barv v soseščini točke v, ki se pojavijo natanko dvakrat. Očitno velja $X_v \geq X'_v$ in sledi $\mathbb{E}(X_v) \geq \mathbb{E}(X'_v)$. Dokažimo, da je $\mathbb{E}(X'_v) \geq \frac{2B}{e^6\Delta}$.

Oglejmo si u in w, ki sta sosednji točki točke v, hkrati pa sta edini pobarvani z barvo α. Naj bo S soseščina teh točk, (niso pobarvane z barvo α) $S = [N(v) \cup N(u) \cup N(w)] \setminus \{u, w\}$. Množica S je moči $|S| \leq 3\Delta - 3 \leq 6c$, $c = \lfloor \frac{\Delta}{2} \rfloor$.

Za izračun ocene matematičnega upanja bomo potrebovali nekaj podatkov. Barvo α lahko izberemo na c načinov, točki u in w pa na B načinov, saj lahko izbiramo le med pari točk, ki so sosede točke v in hkrati niso povezane, teh pa je $\binom{\Delta}{2} - (\binom{\Delta}{2} - B) = B$. Verjetnost, da je izbrana barva α na točkah u in w, je $\frac{1}{c^2}$, verjetnost, da pa ni izbrana na sosedih točk v, u in w, je $\geq (1-\frac{1}{c})^{6c}$. Sedaj ocenimo matematično upanje

$$\mathbb{E}(X'_v) \geq c\ B\ \frac{1}{c^2}\left(1-\frac{1}{c}\right)^{6c} = \frac{B}{c}\left(1-\frac{1}{c}\right)^{6c} \geq \frac{2B}{\Delta}\left(1-\frac{1}{c}\right)^{6c} \geq \frac{2B}{e^6\Delta}.$$

□

Lema 8.10 $P(|X_v - \mathbb{E}(X_v)| > \log(\Delta\sqrt{\mathbb{E}(X_v)}) < \frac{1}{4\Delta^5}$.

Dokaz. Definirajmo spremenljivki AT_v in Del_v. Prva predstavlja število barv, ki so bile v soseščini točke v prirejene vsaj dvakrat, druga pa število barv, ki so bile v soseščini točke v prirejene vsaj dvakrat in razbarvane. Velja $X_v = AT_v - Del_v$. Trdimo:

1. $P(|AT_v - \mathbb{E}(AT_v)| > t) < 2e^{-\frac{t^2}{8\Delta}}$,
2. $P(|Del_v - \mathbb{E}(Del_v)| > t) < 4e^{-\frac{t^2}{100\Delta}}$.

Dokažimo trditev 1.: Uporabimo SCB (Simple Concentration Bound), kjer je elementarni dogodek slučajna izbira barve za točko. Hitro ugotovimo, da se s spremembo barve spremenljivka AT_v spremeni za največ $c = 1$. Torej velja $P(|AT_v - \mathbb{E}(AT_v)| > t) \leq 2e^{-\frac{t^2}{8\Delta}}$.

Dokažimo trditev 2.: Uporabimo Talagrandovo neenakost, saj je $n \approx \Delta^2$. Spet opazimo, da je $c = 1$. Naj bo $Del_v \geq s$. Za vsako izmed s barv izberemo dve sosedi v, ki sta obarvani z isto barvo in enega njunega soseda, ki je ravno tako obarvan s to barvo. Torej je $r = 3$. Velja še $\mathbb{E}(Del_v) \leq \Delta$ in $t^* \geq \sqrt{\Delta \log \Delta}$. Sledi

$$P(|Del_v - \mathbb{E}(Del_v)| > t^*) \leq 4e^{-\frac{t^* - 60\sqrt{3\mathbb{E}(Del_v)}}{24\mathbb{E}(Del_v)}} < 4e^{-\frac{t^2}{100\Delta}}.$$

Iz trditev 1. in 2. sledi lema 2. Uporabimo enakost $t = \frac{1}{2}\log\Delta\sqrt{\mathbb{E}(X_v)}$.

$$\begin{aligned} P(|X_v - \mathbb{E}(X_v)| > \log\Delta\sqrt{\mathbb{E}(X_v)}) &\leq P(|AT_v - \mathbb{E}(AT_v)| > t \text{ ali } |Del_v - \mathbb{E}(Del_v)| > t)) \\ &\leq P(|AT_v - \mathbb{E}(AT_v)| > t) + P(|Del_v - \mathbb{E}(Del_v)| > t) \\ &\leq 2e^{-\frac{t^2}{8\Delta}} + 4e^{-\frac{t^2}{100\Delta}} < \frac{1}{4\Delta^5}. \end{aligned}$$

□

Manjka le še dokaz za $P(A_v) \leq \frac{1}{4\Delta^5}$. Dobimo ga z uporabo lem 1 in 2:

$$\begin{aligned} \frac{1}{4\Delta^5} &> P\left(|X_v - \mathbb{E}(X_v)| > \log\Delta\sqrt{\mathbb{E}(X_v)}\right) \geq P\left(\mathbb{E}(X_v) - X_v > \log\Delta\sqrt{\mathbb{E}(X_v)}\right) \\ &\geq P\left(\frac{2B}{e^6\Delta} - \log\Delta\sqrt{\mathbb{E}(X_v)} \geq X_v\right) \geq P\left(\frac{2B}{e^6\Delta} - \log\Delta\sqrt{\Delta} \geq X_v\right) \\ &\geq P\left(\frac{B}{e^6\Delta} \geq X_v\right) = P(A_v) \end{aligned}$$

Po predpostavki velja $B \geq \Delta(\log\Delta)^3$. Preveriti želimo, da velja predzadnja neenakost v zgornji izpeljavi. Želimo, da bo $\frac{B}{e^6\Delta} - \log(\Delta\sqrt{\Delta}) \geq 0$:

$$\frac{B}{e^6\Delta} - \log(\Delta\sqrt{\Delta}) \geq \frac{(\log\Delta)^3}{e^6} - \log(\Delta\sqrt{\Delta}) \geq 0$$

za $\Delta > 10^{11}$.

8.6 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 8.11 *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 $e^{\lambda x} \leq h(x)$ ($y = h(x)$ je ravno sekanta skozi točki $x = \pm 1$ konveksne funkcije $y = e^{\lambda x}$). Velja

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

□

Izrek 8.12 (Azumova neenakost) *Naj bo $0 = X_0, \ldots, X_m$ martingala za katero velja*

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

za vse $0 \leq i < m$. 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 $|Y_i| \leq 1$ in $E[Y_i|X_{i-1}, X_{i-2}, \ldots, X_0] = 0$. Po zgornji lemi sledi

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

Torej je

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

Od tod sledi

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

□

Literatura

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

[2] B. Bollobás, *Random graphs*, Second edition, Cambridge studies in advanced mathematics **73**, Cambridge University Press, Cambridge, 2001.

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

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

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

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

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