Přehled.

Definice. *Pravděpodobnostní prostor* je trojice (Ω, σ, p) kde:

- Ω je nosná množina,
- $\Sigma \subseteq 2^\Omega$, která je σ-algebra splňující:
  1. $\emptyset \in \Sigma$
  2. Pokud $A \in \Sigma$, potom $\Omega \setminus A \in \Sigma$,
  3. Pokud $A_i)_{i=1}^\infty$, kde každá je v Σ, potom $\bigcup_{i=1}^\infty \in \Sigma$ a
- p je funkce $p : \Sigma \to [0, 1]$ splňující:
  - $P[\emptyset] = 0$
  - $P[\Omega] = 1$
  - Pokud $(A_i)_{i=0}^\infty$ jsou navzájem disjunktní množiny ze Σ, potom $P[\bigcup_{i=1}^\infty A_i] = \sum_{i=1}^\infty P[A_i]$.

Prvky Σ se nazývají *jevy*, prvky Ω nazýváme *elementární jevy* a p se nazývá *pravděpodobnost* na Ω.

Příklad. Diskrétní konečný pravděpodobnostní prostor, ve kterém Ω je konečná množina, $\Sigma = 2^\Omega$ a p může být jednoznačně definovaná přes elementární jevy, tedy $p : \Omega \to [0, 1]$, $\sum_{\omega \in \Omega} p(\omega) = 1$, a tedy $P[A] = \sum_{\omega \in A}, P[\omega] = p(\{\omega\})$.
Rovnoměrný pravděpodobnostní prostor je diskrétní prostor, kde navíc $p(\omega) = 1/|\Omega| \ \forall \omega \in \Omega$.

Příklad. Nekonečný prostor – $\Omega = [0, 1]^2$, Σ je měřitelná podmnožina Ω. Potom $P[A]$ je obsah A, $(\lambda(A))$.

Příklad jevu v takovém prostoru je $A = [0, 1]^2 \setminus [0.1, 0.9]^2$.

Lemma 1. *Nechť $A_1, A_2, \ldots, A_k$ jsou náhodné jevy. Potom* $\sum_{i=1}^k P[A_i] \geq P[\bigcup_{i=1}^k A_i]$.

Důkaz. Uvažme $B_i := A_i \setminus (A_1 \cup A_2 \cup \cdots \cup A_{i-1})$. Ty jsou rovněž jevy. Tudíž $P[\bigcup_{i=1}^k A_i] = P[\bigcup_{i=1}^k B_i]$ (lze dokázat indukcí přes rovnost jevů nalevo a vpravo).

Tuto pravděpodobnost dále upravíme na $\sum_{i=1}^k P[B_i] \leq \sum_{i=1}^k P[A_i]$. To platí, protože $B \subseteq A \Rightarrow P[B] \leq P[A]$: $P[A] = P[B \cup (A \setminus B)] = P[B] + P[A \setminus B] \geq P[B]$. □

Definice. Nechť $n \in \mathbb{N}, p \in [0,1]$, potom definujeme $G(n,p)$ jako pravděpodobnostní prostor *náhodných grafů o n vrcholech s pravděpodobností hrany p* takový, že Ω je množina všech grafů o n vrcholech a pravděpodbnost grafu s právě m hranami je $p^m(1-p)^{\binom{n}{2}-m}$.

Intuitivně, chceme m hran, ty získáme s pravděpodobností p^m. Celkem hran je $\binom{n}{2}$. Zbytek hran nechceme, proto vynásobíme pravděpodobnost $(1-p)^{\text{zb.}}$.

Aplikace. Ramseyova věta a čísla:

$\forall k, l \in \mathbb{N}\, \exists N \in \mathbb{N}$, kde každý graf na alespoň N vrcholech obsahuje buď kliku velikosti k nebo nezávislou množinu velikosti l. Nejmenší takové N nazýváme Ramseyovým číslem $R(k,l)$.

Z dřívějška jsme dokázali, že $R(k,k) \leq \binom{2k}{k} \leq 4^k$. Ukážeme i dolní odhad:

Věta 2. $R(k,k) \geq 2^{k/2}$.

Důkaz. Pokud $n \leq 2^{k/2}$, chceme najít graf neobsahující kliku ani nezávislou množinu velikosti k.

Uvažujme náhodný graf $G = G(n, 1/2)$. Pravděpodobnost, že G obsahuje kliku velikosti k je nejvýše $p_k = \binom{n}{k} 2^{-\binom{k}{2}}$ (přes pravděpodobnosti sjednocení). Pravděpodobnost, že graf obsahuje nezávislou množinu velikosti k je taktéž nejvýše p_k.

Pravděpodobnost, že nastane jedno z toho je proto nejvýše $2p_k \leq n^k/k! \cdot 2^{k^2/2+k/2+1}$. Za n dosaďme $2^{k/2}$. Dostáváme $\leq 2^{k^2/2-k^2/2+k/2+1-k+1} = 2^{-k/2+2<2^0=1}$, jestliže $k \geq 5$.

Pravděpodobnost opačného jevu je proto větší, než 0. Tudíž pro $k \geq 5$ pravděpodobnost grafu bez kliky nebo nezávislé množiny velikosti k je nenulová a takový graf existuje. Pro $k \leq 4$ lze ukázat jinak. □

Odhady pro faktoriál a binomické koeficienty.

- Existuje zjevný odhad $\left(\frac{n}{2}\right)^{n/2} \leq n! \leq n^n$.
  Přesnější odhad říká $\left(\frac{n}{e}\right)^n \leq n! \leq e \cdot n \cdot \left(\frac{n}{e}\right)^n$.
  Stirlingova formule říká, že $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$.

- Pro binomy máme jednoduchý odhad $\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \frac{n^k}{k!} \leq n^k$.

  Přesnější odhad říká $\binom{n}{k} \leq \left(\frac{en}{k}\right)^k$.

  Pro střední binom máme ještě lepší odhad: $\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$.
- Víme, že $1 + x \leq e^x$, což je ekvivalentní s $1 + x - e^x \leq 0$. To lze dokázat zderivováním levé strany, čímž dostaneme $1-e^x$, dosazení x nikdy neporuší.

  To můžeme využít na odhad $(1 - p)^m \leq e^{-pm}$.

Definice. Řekněme, že dva jevy A, B jsou nezávislé, jestliže $P[A \cap B] = P[A] \cdot P[B]$.

Obecněji, $A_1, \ldots, A_k$ jsou nezávislé, jestliže pro každé $I \subseteq [k]$ platí $P[\bigcup_{i \in I} A_i] = \prod_{i \in I} P[A_i]$.

Definice. Nechť A, B jsou jevy. Potom *podmíněná pravděpodobnost A za předpokladu B* je definovaná jako

$$P[A|B] = \frac{P[A \cap B]}{P[B]}.$$

Pokud jsou jevy A, B nezávislé, potom $P[A|B] = P[A]$.

Mějme booleovské proměnné $x_1, x_2, \ldots, x_n$.

Literál je proměnná x_i nebo její negace $\neg x_i$.

Klauzule je formule ve formě $({}_1 \vee l_2 \vee \ldots l_k)$, kde l_i jsou literály.

CNF-Formule je formule $c_1 \wedge c_2 \wedge \cdots \wedge c_m$, kde c_i jsou klauzule.

Formule je *splnitelná*, pokud existuje ohodnocení proměnných takové, že se formule vyhodnotí pravdivě.

Příklad. Formule $(\neg x_1) \wedge (x_1 \vee x_2 \vee x_4) \wedge (\neg x_2 \vee x_3)$ je splnitelná, například pro ohodnocení $(x_1, x_2, x_3, x_4) = (0, 1, 1, 1)$.

SAT problém Je daná CNF-formule Φ splnitelná? Tento problém je NP-težký.

Tvrzení 3. *Nechť Φ je CNF-formule s m klauzulemi taková, že každá klauzule obsahuje k různých literálů. Pokud $m \leq 2^k$, potom Φ je splnitelná.*

Důkaz. Uvažujme náhodné ohodnocení, kde každá $x_i = 1$ s pravděpodobností $1/2$ nezávisle na ostatních proměnných.

Uvažujme klauzuli c_i, potom c_i je splněná s pravděpodobností alespoň $1 - 2^{-k}$: Pokud se v c_i nachází literál x_j i $\neg x_j$, potom pravděpodobnost je jistě 1. V opačném případě, aby klauzule byla nesplnitelná, musí být každý literál ohodnocen opačně, nastavení je nezávislé.

Pravděpodobnost, že existuje nesplněná klauzule je nejvýše $m2^{-k}$ podle Union bound. dle předpokladu $m2^{-k} < 1$. Pravděpodobnost, že je formule splnitelná, je tedy větší, než 0. □

Erdös-ko-Radova věta.

Definice. Rodina množin $\mathcal{F}$ je *protinající se*, pokud $A \cap B \neq \emptyset$ pro každé $A, B \in \mathcal{F}$.

Jaká je maximální protínající se rodina množin velikosti k nad množinou velikosti n?

Nechť $k \leq n/2$. Když zafixujeme jeden prvek, dostáváme rodinu velikosti $\binom{n-1}{k-1}$.

Věta 4. *Nechť n, k jsou přirozená čísla taková, že $k \leq n/2$. Potom maximální velikost protinající se rodiny k-množin nad n-prvkovou množinou je právě $\binom{n-1}{k-1}$.*

Lemma 5. *Uvažujme množinu $X = \{0, 1, \ldots, n-1\}$ se sčítáním modulo n, definujeme $A_s = \{s, s+1, \ldots, s+k-1\}$ pro $s \in X$. Pokud $\mathcal{F}$ je protinající se rodina k-prvkových podmnožin X, potom $\mathcal{F}$ obsahuje nejvýše k množin A_s.*

Důkaz. Pro nějaké s mějme $A_s \in \mathcal{F}$. Množiny protínající A_s jsou mimo jiné $A_{s-k+1}, \ldots, A_{s-1}, A_{s+1}, \ldots, A_{s+k-1}$.

Pro páry A_t, A_{t+k}, kde $t \in \{s-k+1, \ldots, s-1\}$, pouze jedna z množin může být ve $\mathcal{F}$. To dává celkem nejvýše k množin A_s. □

Důkaz věty. Nechť X je n-prvková množina z předpokladu. BÚNO $X = \{0, \ldots, n-1\}$ se sčítáním modulo n.

Pro permutaci σ množiny X a $s \in X$ mějme $A_{\sigma,s} = \{\sigma(s), \sigma(s+1), \ldots, \sigma s + k - 1\}$. Uvažujme σ, s, kde σ je náhodná permutace zvolena

uniformně a s je náhodně zvolený prvek X, taktéž uniformně. Chceme odhadnout $P[A_{\sigma,s} \in \mathcal{F}]$.

Dle lemmatu $P[A_{\sigma,s} \in \mathcal{F}] \leq k/n$ (volíme σ, pak s). Na druhou stranu $P[A_{\sigma,s} \in \mathcal{F}] = |\mathcal{F}|/\binom{n}{k}$ (volíme s, pak σ).

Tudíž $|\mathcal{F}| = P[A_{\sigma,s} \in \mathcal{F}]\binom{n}{k} \leq \frac{n}{k}\binom{n}{k} = \binom{n-1}{k-1}$. □

Definice. Nechť (Ω, Σ, P) je pravděpodobnostní prostor. Potom *náhodná veličina* je měřitelná funkce $X : \Omega \to \mathbb{R}$.

Měřitelná funkce splňuje $X^{-1}([a, \infty]) \in \Sigma$).

Zavedeme si ještě zkratku $P[X = a] = P[\{\omega \mid X(\omega) = a\}]$. Podobně pro $P[X \leq a]$ a další relační operátory.

Definice. *Střední hodnota* náhodné veličiny X je definovaná jako výraz $\mathbb{E}[X] = \int_\Omega X(\omega) dP(\omega)$ (obecně).

Pro konečný prostor: $\mathbb{E}[X] = \sum_{\omega\in\Omega} X(\omega)p(\omega) = \sum_{a\in X(\Omega)} aP[X = a]$.

Lemma 6 (Linearita střední hodnoty)**.** *Nechť X_1, X_2 jsou náhodné veličiny a $\alpha, \beta \in \mathbb{R}$. Potom $\mathbb{E}[\alpha X_1 + \beta X_2] = \alpha\mathbb{E}[X_1] + \beta\mathbb{E}[X_2]$.*

Důkaz. (pouze pro konečné prostory) $\mathbb{E}[\alpha X_1+\beta X_2] = \sum_{\omega\in\Omega}(\alpha X_1(\omega)+\beta X_2(\omega))p(\omega) = \alpha\sum_{\omega\in\Omega} X_1(\omega)p(\omega) + \beta\sum_{\omega\in\Omega} X_2(\omega)p(\omega)$. □

Definice. Řekneme, že dvě náhodné veličiny X, Y jsou nezávislé, pokud $P[X \in A \wedge Y \in B] = P[X \in A]P[Y \in B]$ pro každé A, B měřitelné podmnožiny $\mathbb{R}$.

Je postačující zkontrolovat, že $P[X \leq a \wedge Y \leq b] = P[X \leq a]P[Y \leq b]$ pro libovolné $a, b \in \mathbb{R}$.

Tvrzení 7. *Nechť X, Y jsou nezávislé náhodné veličiny. Potom platí $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$.*

Důkaz. $\mathbb{E}[XY] = \sum_{c\in XY(\Omega)} c \cdot P[XY = c] = \sum_{a\in X(\Omega), y\in Y(\Omega)} ab \cdot P[X = a \wedge Y = b] = \sum ab \cdot P[X = a]P[Y = b]$. To můžeme rozdělit na dvě sumy, dostaneme definice $\mathbb{E}[X]\mathbb{E}[Y]$. □

Nechť A je náhodný jev. Indikátor I_A je náhodná veličina definovaná jako $I_A(x) = |\{x\} \cap A|$. Potom $\mathbb{E}[I_A] = P[A]$.

Očekávaný počet fixních bodů v náhodné permutaci. Uvažujme náhodnou permutaci $\sigma \in S_n$ a jevy A_i, že i je fixní bod. Vidíme, že $\mathbb{E}[I_{A_i}] = P[A_i] = 1/n$. Tedy střední hodnota počtu fixních bodů je $n \cdot \mathbb{E}[I_{A_n}] = 1$.

Hamiltonovské cesty v turnajích.

Definice. Turnaj je orientovaný úplný graf.

Každý turnaj obsahuje orientovanou Hamiltonovskou cestu. Existuje turnaj s právě jednou; stačí uvažovat lineární uspořádání jako graf. Můžeme mít vysoké množství cest?

Věta 8 (Szele)**.** *Pro každé n existuje turnaj na n vrcholech obsahující alespoň $n!/2^{n-1}$ orientovaných hamiltonovských cest.*

Důkaz. Postavíme turnaj T na n vrcholech tak, že zvolíme orientaci každé hrany náhodně rovnoměrně a nezávisle. Spočítáme střední hodnotu počtu OHC.

Zvolme σ jako permutaci $V(T)$. Uvažujme jev A_σ, že σ indikuje OHC. Potřebujeme, aby každá hrana byla orientovaná každým směrem. Tedy $P[A_\sigma] = 1/2^{n-1}$.

Nechť X je počet OHC, potom $\mathbb{E}[X] = \sum_\sigma \mathbb{E}[I_{A_\sigma}] = n!/2^{n-1}$. To tedy znamená, že existuje hledaný turnaj. □

MAXSAT problém. Máme Φ booleovskou funkci v CNF. Kolik klauzulí může být splněno zároveň pro dané ohodnocení?

Tvrzení 9. *Nechť Φ je BF v CNF taková, že každá klauzule obsahuje k různých literálů. Potom alespoň $\frac{2^k-1}{2^k} \cdot m$ klauzulí může být splněno, kde m je počet klauzulí.*

Důkaz. Každou proměnnou Φ nastavíme na 0 nebo 1 náhodně uniformně nezávisle. Mějme klauzuli C. Pak $P[C = 1] \geq \frac{2^{k-1}}{2^k}$. Pak díky indikátorům $\mathbb{E}[\text{počet splněných klauzulí}] \geq m \cdot \frac{2^{k-1}}{2^k}$. □

Ukážeme derandomizovaný algoritmus (zhruba), jak toto ohodnocení najít:

Nechť $x_1, \ldots, x_n$ jsou proměnné. Předpokládejme, že jsme nastavili $x_1, \ldots, x_i$ a chceme nastavit x_{i+1}. Pro Φ mějme Φ' takovou, kde zahodíme splněné klauzule a odstraníme literály patřící $x_1, \ldots, x_i$ ze zbylých klauzulí.

Dále porovnáme $\mathbb{E}[|C = 1| \mid x_{i+1} = 1]$ a $\mathbb{E}[\cdots \mid x_{i+1} = 0]$ a zvolíme lepší hodnotu. Toto funguje, jelikož $\mathbb{E}[I_A] = 1/2(\mathbb{E}[I_{A|B}] + \mathbb{E}[I_{A|B^C}])$ pro $P[B] = 1/2$.

MAX-CUT problém. Máme graf G a chceme znát velikost nejmenšího řezu.

Tvrzení 10. *Nechť G je graf s m hranami. Pak obsahuje řez obsahující alespoň $m/2$ hran.*

Důkaz. Pro každý vrchol $v \in V(G)$ se rozhodneme, zda jej vložíme do A nebo B uniformně náhodně nezávisle. Tím dostaneme žez $C(A, B)$.

Tudíž $P[e \in C(A, B)] = 1/2$, protože $e = \{u, v\}$, máme 4 možnosti, v jakých množinách se nacházejí u, v a právě 2 z nich implikují, že $e \in C(A, B)$.

Nyní sečtením indikátoru dostaneme střední počet hran v řezu. □

Tím dostáváme náhodný algoritmus, který nalezne řez o alespoň $m/2$ hranách s nenulovou pravděpodobností. Ukážeme však derandomizaci:

Budeme stavět A, B postupně. Zvolme nějakou hranu a rozdělme její koncové vrcholy do A a B. V každém kroku zvolme vrchol v, který ještě nemá přidělení.

Protože chceme maximalizovat počet hran v řezu, podíváme se na počet hran vycházející z v do A i do B a zvolíme tu množinu, pro kterou je tento počet menší. V každém kroku proto přibyde alespoň polovina hran do řezu.

Vyvážené vektory. Nechť $v_1, \ldots, v_n$ jsou jednotkové vektory v $\mathbb{R}^n$. Chceme najít $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ tak, že $\|\varepsilon_1 v_1 + \ldots \varepsilon_n v_n\|$ je co největší (nejmenší).

Tvrzení 11. *Nechť $v_1, \ldots, v_n \in \mathbb{R}^n, \|v_i\| = 1$ pro $i \in [n]$. Pak:*

1. *Existuje $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ tak, že $\|\varepsilon_1 v_1 + \ldots \varepsilon_n v_n\| \geq \sqrt{n}$,*
2. *Existuje $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ tak, že $\|\varepsilon_1 v_1 + \ldots \varepsilon_n v_n\| \leq \sqrt{n}$.*

Odhady jsou nejlepší možné, stačí uvažovat ortonormální bázi.

Důkaz. Zvolme $\varepsilon_1, \ldots, \varepsilon_n$ uniformně náhodně nezávisle. Nechť $X = \|\varepsilon_1 v_1 + \cdots + \varepsilon_n v_n\|^2 = \langle \ldots, \ldots \rangle$. Pak $\mathbb{E}[X] = \mathbb{E}[\sum_{i,j=1}^n \varepsilon_i \varepsilon_j \langle v_i, v_j \rangle] = \sum_{i,j=1}^n \mathbb{E}[\varepsilon_i \varepsilon_j] \langle v_i, v_j \rangle$.
Uvažujme $\mathbb{E}[\varepsilon_i \varepsilon_j]$. Pokud $i = 1$, je to přesně $\mathbb{E}[1] = 1$. Jinak můžeme použít nezávislost a linearitu součinu, dostáváme $\mathbb{E}[\varepsilon_i]\mathbb{E}[\varepsilon_j] = 0$. Proto $\mathbb{E}[X] = \sum_{i=1}^n \langle v_i, v_i \rangle = n$. Z toho již vyplývá tvrzení. □

Metoda alterace

Věta 12 (Slabá Turánova)**.** *Nechť G je graf s n vrcholy a m hranami. Nechť $d = 2m/n$ je jeho průměrný stupeň. Pak $\alpha(g) \geq n/2d$.*

Důkaz. Zvolme $S \subseteq V(G)$ náhodnou podmnožinu $V(G)$. Každý vrchol vložíme do S s pravděpodobností p, nezávisle.

Mějme X náhodnou veličinu označující počet vrcholů. Očividně $\mathbb{E}[X] = pn$. Dále Y je počet hran v grafu indukovaném S. Hranu budeme počítat pouze, když každý koncový vrchol je v S. Tudíž $\mathbb{E}[Y] = p^2 m$.

Nyní $\mathbb{E}[X - Y] = pn - p^2 m = pn(1 - pd/2)$. Když zvolíme $p = 1/d$, dostáváme $\mathbb{E}[X - Y] = 1/d \cdot n \cdot 1/2 = n/2d$. Tedy existuje S taková, kde $X - Y \geq n/2d$. Pro každou hranu S odstraníme jeden koncový vrchol z S. Tím dostaneme nezávislou množinu správné velikosti. □

Lemma 13 (Markovova nerovnost)**.** *Nechť X je nezáporná náhodná veličina, $a > 0$. Pak $P[X \geq a] \leq \mathbb{E}[X]/a$.*

Důkaz. Ekvivalentně $\mathbb{E}[X] \geq P[X \geq a] \cdot a$. Protože X je nezáporná, nerovnost je platná přímo z definice střední hodnoty. □

Grafy s vysokým [girth] a vysokým barevným číslem. Nechť G je graf. Potom $g(G)$ (girth) je délka nejkratšího cyklu v G. Pokud G je les, $g(G) = \infty$.

Graf s vysokým [girth] se lokálně chová jako strom. Avšak...

Věta 14 (Erdös)**.** *Pro každé kladné celé čísla k, l existuje graf G, pro který $g(G) > l, \xi(G) > k$.*

Důkaz. Nechť $G' = G(n,p)$. Nastavíme $p = n^{\varepsilon-1} = n^{1/(1-\varepsilon)}$, kde $\varepsilon = 1/2l$.

Uvažujme počet i-cyklů v K_n pro $i \in 3,\ldots,l$. To je $\binom{n}{i} \cdot i! \cdot 1/2i \leq n^i$. Zvolme veličinu X říkající počet cyklů délky nejvýše l ve grafu G'. Pak $\mathbb{E}[X] \leq \sum_{i=3}^{l} n^i p^i = \sum_{i=3}^{l} n^{\varepsilon i} \leq l \cdot n^{1/2l \cdot l} = l \in o(n)$.

Pokud n je dostatečně velké, pak $\mathbb{E}[X] \leq n/4$. Dle Markovovy nerovnosti $P[X \geq n/2] \leq 1/2$.

Nyní se přesuňme k barevnému číslu. Nechť $a = \lceil 3/p \cdot \log n \rceil + 1$. Pak pro dostatečně vysoké n platí $3/p \log n \leq a - 1 \leq 4/p \log n$. Uvažujme α velikost nezávislé množiny G'. Pak $P[\alpha \geq a] \leq \binom{n}{a}(1-p)^{a(a-1)/2} \leq n^a e^{pa(a-1)/2}$. Díky volbě a můžeme pravděpodobnost odhadnout shora $n^a \cdot n^{-3a/2} = n^{-a/2} \to 0$.

Pokud n je dostatečně velké, pak $P[\alpha \geq a] < 1/2$. Celkově obrácením $P[X < n/2 \wedge \alpha < a] > 0$. Tudíž existuje G' s méně, než $n/2$ cykly délky nejvýše l. Z každého cyklu délky $\leq l$ odstraňme jeden vrchol.

Dostáváme graf G, kde $|V(G)| \geq n/2$ a $\alpha(G) \leq a - 1$, díky odstranění vrcholů $g(G) > l$. Zbývá odhadnout $\xi(G) \geq |V(G)|/\alpha(G) \geq \frac{n/2}{4 \log n/p} = \frac{np}{8 \log n} = \frac{n^\varepsilon}{\log n} \to \infty$. Pro každé k existuje n, kde $\xi(G) > k$. □

Věta 15 (Bayesova)**.** *Nechť $A, B_1, \ldots, B_n$ jsou neprázdné náhodné jevy prostoru (Ω, Σ, P), kde $B_1, \ldots, B_n$ tvoří disjunktní pokrytí Ω. Pak $P[B_i \mid A] = \frac{P[A|B_i]P[B_i]}{\sum_{j=1}^{n} P[A|B_j]P[B_j]}$.*

👁 $\sum_{j=1}^{n} P[A \mid B_j]P[B_j] = P[A]$. To platí, protože z definice platí $P[A \mid B] = P[A \cap B]/P[B]$. Tudíž $P[A] = \sum_{j=1}^{n} P[A \cap B_i]$.

Důkaz. $\frac{P[A|B_i]P[B_i]}{\sum P[A|B_j]P[B_j]} = \frac{P[A \cap B_i]}{P[A]} = P[B_i \mid A]$. □

Testování násobení matic. Nechť máme na vstupu $n \times n$ matice A, B, C. Platí, že $C = AB$? Chtěli bychom to spočítat rychleji, než prostým vynásobením A a B, nejrychleji to zatím umíme v čase $\Omega(n^{2.37})$.

Ukážeme však algoritmus pracující v čase $\mathcal{O}(n^2 \cdot k)$, kde k je parametr. Může však zahlásit chybně s pravděpodobností nejvýše 2^{-k}.

Uvažujme náhodný vektor $r = (r_1, \ldots, r_n)^T$, kde $r_i \in \{0,1\}$ nezávisle. Pak spočítáme $A(Br)$ a porovnáme s Cr. Vynásobení matice s vektorem umíme v $\mathcal{O}(n^2)$.

Nechť $D = AB - C$, speciálně $Dr = ABr - Cr$. Pokud $ABr \neq Cr$, pak jistě $AB \neq C$. Chceme, aby $ABr \neq Cr$, jestliže $AB \neq C$ s pravděpodobností alespoň $1/2$. Potom můžeme r vygenerovat k-krát nezávisle, tím pravděpodobnost $ABr = Cr, AB \neq C$ klesne na 2^{-k}.

$AB \neq C \leftrightarrow D \neq 0$. Chceme odhadnout $P[Dr \neq 0]$. Víme, že $\exists i, j : d_{ij} \neq 0$. Pak $v_i = \sum_{k=1}^{n} d_{ik} r_k = d_{ij} + r_j + \sum_{k \neq j} d_{ik} r_k$. Sumu nazvěme y, jedná se o náhodnou veličinu.

$P[v_i = 0] = P[v_i = 0 \mid y = 0]P[y = 0] + P[v_i = 0 \mid y \neq 0]P[y \neq 0]$. Pokud $y = 0$, potom r_i musí být 0. Podobně, pokud $y \neq 0$, r_i nesmí být 0. Tedy $P[v_i = 0] \leq 1/2(P[y = 0] + P[y \neq 0]) = 1/2$. Tudíž $P[Dr = 0] \leq 1/2$.

Chceme rozmístit n bodů do $[0, 1]^2$ tak, abychom nedostali žádný trojúhelník s malým obsahem.

Tvrzení 16. *Pro každé (dostatečně vysoké) n existuje n bodů v $[0, 1]^2$ takových, že každá trojice tvoří trojúhelník s obsahem alespoň $\frac{1}{101n^2}$.*

S mnohem komplikovanějším argumentem lze získat $c \log n/n^2$.

Důkaz. Uvažujme $2n$ náhodných bodů v $[0, 1]^2$ nezávisle. Zvolme tři náhodné body Q, R, S, pak $\lambda(QRS)$ bude obsah trojúhelníku daného QRS. Chceme odhadnout $P[\lambda \leq \varepsilon]$ pro nějaké ε (rovno výrazu v tvrzení).

Uvažujme $w = |QR|$, parametr $\Delta > 0$ a událost $B_i : w \in ((i-1)\Delta, i\Delta)$. Pak $P[\lambda \leq \varepsilon] = \sum_{i\Delta < \sqrt{2}} P[\lambda \leq \varepsilon \mid B_i]P[B_i]$.

Nejprve odhadneme B_i: aby w bylo v daném intervalu, R se musí nacházet v mezikruží se středem v Q. Proto $P[B_i] \leq \pi(i^2\Delta^2 - (i-1)^2\Delta^2) = \pi(2i-1)\Delta^2$. Nyní můžeme odnadnout podmíněnou pravděpodobnost: Protože známe polohy Q, R, bod S musí být na dostatečně blizké rovnoběžce QR, konkrétně nejvýše $2\varepsilon/w$ (dostáváme pás). Navíc délka vzniklého pásu je nejvýše $\sqrt{2}$. Tedy $O[\lambda \leq \varepsilon \mid B_i] \leq 4\varepsilon/(i-1)\Delta \cdot \sqrt{2}$.

$P[\lambda \leq \varepsilon] = P[\lambda \leq \varepsilon \mid B_1] \cdot \pi\Delta^2 + \sum_{i=2}^{\lfloor\sqrt{2}/\Delta\rfloor} \pi(2i-1)\Delta^2 \cdot \frac{4\varepsilon\sqrt{2}}{(i-1)\Delta} \leq \pi\Delta^2 + 24\pi\varepsilon$. Pokud limitně zvolíme $\Delta \to 0$, pak $P[\lambda \leq \varepsilon] \leq 24\pi\varepsilon$.

Vygenerujeme náhodně $2n$ bodů v $[0, 1]^2$. Nechť X je počet trojúhelníků s obsahem nejvýše ε. Pak pro $\varepsilon = 101n^2$: $\mathbb{E}[X] \leq \binom{2n}{3} \frac{24\pi}{101n^2} \leq \frac{8n^3 24\pi}{6 \cdot 101n^2} \leq n$. Stačí odstranit bod z každého trojúhelníku obsahu menšího ε, dostáváme alespoň n bodů z věty. □

Definice. Nechť X je náhodná veličina, pak *rozptyl* X je definován jako $\mathrm{Var}[X] = \mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - \mathbb{E}^2[X]$.

Směrodatná odchylka $\sigma = \sqrt{\mathrm{Var}[X]}$ je $\mathbb{E}[|X - \mathbb{E}[X]|]$, bohužel kvůli absolutní hodnotě s ní není jednoduché pracovat.

Definice. Nechť X, Y jsou dvě náhodné veličiny. Pak *kovariance* X a Y je $\mathrm{Cov}[X, Y] = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])] = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$.

Pokud X, Y jsou nezávislé, pak $\mathrm{Cov}[X, Y] = 0$.

Lemma 17. *Nechť $X_1, X_2, \ldots, X_m$ jsou náhodné veličiny. Pak platí* $\mathrm{Var}[\sum_{i=1}^n X_i] = \sum_{i=1}^n \mathrm{Var}[X_i] + \sum_{i \neq j} \mathrm{Cov}[X_i, X_j] = \sum_{i,j} \mathrm{Cov}[X_i, X_j]$.

Důkaz. Úpravami: $\mathrm{Var}[\sum_{i=1}^n X_i] = \mathbb{E}[(\sum_{i=1}^n X_i)^2] - \mathbb{E}^2[\sum_{i=1}^n X_i] = \mathbb{E}[\sum_{i,j=1}^n X_i X_j] - (\sum_{i=1}^n \mathbb{E}[X_i])^2 = \ldots$ □

Lemma 18 (Čebyšeova nerovnost)**.** *Nechť X je náhodná veličina a parametr $t > 0$. Pak $P[|X - \mathbb{E}[X]| \geq t] \leq \frac{\mathrm{Var}[X]}{t^2}$.*

Důkaz. Nechť $Y = (X - \mathbb{E}[X])^2$. Pak dle markovovy nerovnosti $P[Y \geq t^2] \leq \frac{\mathbb{E}[Y]}{t^2} = \frac{\mathrm{Var}[X]}{t^2}$. Avšak to je též $P[\sqrt{Y} \geq t]$. □

Odhad středního binomického koeficientu. Mějme binom $\binom{2m}{m}$. Je dobře známo, že je $\theta(\frac{4^m}{\sqrt{m}})$. Ukážeme nerovnost $\binom{2m}{m} \geq \frac{4^m}{4\sqrt{m}+2}$.

Důkaz. Uvažujme $2m$ náhodných veličin $X_1, \ldots, X_{2m}$, které jsou nezávislé a nabírají hodnot 0 nebo 1 s pravděpodobností $1/2$. Nechť X je jejich součet. Pak $\mathbb{E}[X] = m$ a $\mathrm{Var}[X] = m/2$.

Použijeme čebyšeovu nerovnost, $P[|X - \mathbb{E}[X]| \geq \sqrt{m}] \leq (m/2)/\sqrt{m}^2 = 1/2$. Pak taktéž $P[|X - \mathbb{E}[X]| < \sqrt{m}] \geq 1/2$. Uvažujme parametr k : $|k| < \sqrt{m}$. Potom $P[X = m + k] = \binom{2m}{m+k} \cdot 1/2^{2m} \leq \binom{2m}{m} 1/2^{2m}$.

Tudíž $1/2 \leq P[|X - \mathbb{E}[X]| < \sqrt{m}] = \sum_{k=-\lfloor\sqrt{m}\rfloor}^{\lfloor\sqrt{m}\rfloor} P[X = m + k] \leq (2\sqrt{m} + 1)\binom{2m}{m} 1/4^m$. Úpravou nerovnice již dostaneme výsledek. □

Práhové funkce. Uvažujme parametr $p \in [0,1]$, k němu graf $G(n,p)$ a náhodnou veličinu X značící počet trojúhelníků v G. Pak $\mathbb{E}[X] = \binom{n}{3}p^3 \in \Theta(n^3p^3)$. V závislosti na p, dostaneme alespoň 1 trojúhelník v $G(n,p)$?

První případ: $p = o(1/n)$. Pak $\mathbb{E}[X] \to 0$, a tedy $P[X \geq 1] \to 0$.

Druhý případ: $p = \omega(1/n)$. Pak $\mathbb{E}[X] \to \infty$. Platí ale, že $P[X \geq 1] \to 1$?

Definice. Říkáme, že grafová vlastnost $\mathcal{P}$ je monotónní, pokud pro každý pár grafů G, H, kde H je podgraf G platí: Pokud H splňuje vlastnost $\mathcal{P}$, pak G ji splňuje taky.

Funkci $r : \mathbb{N} \to [0,1]$ nazveme práhovou funkci pro monotónní grafovou vlastnost $\mathcal{P}$, pokud platí:

1. Pokud $p(n) = o(r(m))$, pak $\lim P[G(n,p(n)) \text{ splňuje } \mathcal{P}] = 0$.
2. Pokud $p(n) = \omega(r(m))$, pak $\lim P[G(n,p(n)) \text{ splňuje } \mathcal{P}] = 1$.

Věta 19. *Funkce $1/n$ je práhovou funkcí pro obsažení trojúhelníku.*

Lemma 20. *Nechť $X_1, X_2, \ldots$ je posloupnost nezáporných náhodných veličin takových, že $\lim_{n\to\infty} \frac{\mathrm{Var}[X_n]}{\mathbb{E}^2[X_n]} = 0$. Pak $\lim_{n\to\infty} P[X_n > 0] = 1$.*

Důkaz. $P[|X_n - \mathbb{E}[X_n]| \geq \mathbb{E}[X_n]] \leq \frac{\mathrm{Var}[X_n]}{\mathbb{E}^2[X_n]}$ dle Čebyšeovy nerovnosti. Taktéž $P[X_n = 0] \leq \frac{\mathrm{Var}[X_n]}{\mathbb{E}^2[X_n]}$. Proto $\lim_{n\to\infty} P[X_n = 0] \leq \lim_{n\to\infty} \frac{\mathrm{Var}[X_n]}{\mathbb{E}^2[X_n]} = 0$. To je opačná událost k $P[X_n > 0]$. □

Důkaz věty. Pro $p \in o(1/n)$ jsme již dokázali, ukážeme pro $p \in \omega(1/n)$. Nechť T_i je indikátor pro $G(n,k)$ obsahující i-tý trojúhelník. Pak $T = \sum T_i = \Theta(n^3p^3)$ je počet trojúhelníků.

Rozptyl $\mathrm{Var}[T] = \sum_{i,j} \mathrm{Cov}[T_i, T_j]$. Pokud trojúhelníky i, j nesdílí hranu, pak jejich kovariance je 0. Tudíž $\mathrm{Var}[T] \leq \sum_{i,j} \mathbb{E}[T_iT_j]$. Pokud $i = j$, pak $\mathbb{E}[T_i^2] = \mathbb{E}[T_i] = p^3$, pro $i \neq j$ sdílející hranu $\mathbb{E}[T_iT_j] = p^5$.

Celkem máme $\Theta(n^3)$ trojúhelníků a $\binom{n}{4}\binom{4}{2} \in \Theta(n^4)$ párů sdílejících hranu. Tudíž $\mathrm{Var}[T] \in \mathcal{O}(n^3p^3 + n^4p^5)$.

Nyní $\frac{\mathrm{Var}[T]}{\mathbb{E}^2[T]} \in \mathcal{O}(n^{-3}p^{-3} + n^{-2}p^{-1}) \in o(1)$. Dle předchozího lemmatu nakonec $P[T > 0] \to 1$. □

Definice. Nechť H je graf s v vrcholy a e hranami, pak *hustotou* H rozumíme hodnotu $\rho(H) = e/v$.

Řekneme, že H je *vyvážený*, jestliže pro každý podgraf $H' \leq H$ platí $\rho(H') \leq \rho(H)$.

Věta 21. *Nechť H je vyvážený graf. Pak funkce $n^{-1/\rho(H)}$ je prahovou funkcí pro obsažení H v $G(n,p)$.*

Důkaz. Označme $v = |V(H)|, e = |E(H)|, \rho = e/v$. Nechť $a_1, \ldots, a_v$ jsou vrcholy H. Pro uspořádanou v-tici $\beta = (\beta_1, \ldots, \beta_v)$ vrcholů $G(n,p)$ označíme A_β jev, že $b_i b_j \in E(G(n,p))$ kdykoliv $a_i a_j \in E(H)$. Indikátor A_β označíme X_β.

Součet $X = \sum_\beta X_\beta$ je kladný právě, když $G(n,p)$ obsahuje kopii H. Pak $\mathbb{E}[X] = \sum_\beta \mathbb{E}[X_\beta] = \sum_\beta p^e \in \Theta(n^v p^e)$.

Uvažujme případy podle nastavení p. Pokud $p(n) \in o(n^{-v/e})$, pak $\mathbb{E}[X] \to 0$, proto i $P[X > 0] \to 0$ dle Markova.

Nyní předpokládejme $p(n) \in \omega(n^{-v/e})$, chceme spočítat $\mathrm{Var}[X] = \sum_{\beta,\gamma} \mathrm{Cov}[X_\beta, X_\gamma]$. Pokud β, γ sdílejí nejvýše jeden vrchol, pak X_β, x_γ jsou nezávislé.

Předpokládejme, že β, γ sdílejí právě $t \in \{2, \ldots, v\}$ vrcholů. Potom $\mathrm{Cov}[X_\beta, X_\gamma] \leq \mathbb{E}[X_\beta X_\gamma]$. Ve sdílené části je nejvýše $t\rho$ hran z kopie H pro β i γ díky balancovanosti H. Celkový počet hran je alespoň $2(e - e') + e' \geq 2e - t\rho = 2e - te/v$. Proto $\mathrm{Cov}[X_\beta, X_\gamma] \leq p^{2e-te/v}$. Takových párů je navíc $\Theta(n^{2v-t})$.

Tudíž $\mathrm{Var}[X] \leq \mathcal{O}(\sum_{t=2}^{v} n^{2v-t} p^{2e-te/v}) = \mathcal{O}(\sum_{t=2}^{v} (n^v p^e)^{2-t/v})$. Nyní $\frac{\mathrm{Var}[X]}{\mathbb{E}^2[X]} = \mathcal{O}(\sum_{t=2}^{v} (n^v p^e)^{-t/v}) \to 0$, protože $p(n) = \omega(n^{-v/e})$. Podle lemmatu pak $P[X > 0] \to 0$. □

Definice. Pro kladné celé n označuje $\nu(n)$ počet prvočísel dělících n.

Věta 22 (Hardy, Ramannujan)**.** *Nechť f je funkce na kladných celých číslech taková, že $f(n) \to \infty$. Pak počet $x \in \{1, \ldots, n\}$ s vlastností $|\nu(x) - \log\log n| > f(n)\sqrt{\log\log n}$ je $o(n)$.*

Pro důkaz použijeme fakta z teorie čísel:

1. $\sum_{p \leq n, p \text{ prvočíslo}} 1/p = \log\log n + \mathcal{O}(1)$.
2. Počet prvočísel v $[n]$ je $\mathcal{O}(n/\log n)$.

Důkaz. Zvolíme x z $[n]$ rovnoměrně náhodně. Pro p prvočíslo zvolíme X_p indikátor, že $p \mid x$. Pak $\sum_p X_p = \nu(x)$.

$\mathbb{E}[X_p] = \frac{\lfloor n/p \rfloor}{n} = 1/p + \mathcal{O}(1/n)$, $\mathbb{E}[\sum X_p] = \log\log n + \mathcal{O}(1)$.
$\mathrm{Var}[\sum X_p] = \sum_{p,q} \mathrm{Cov}[X_p, X_q]$, rozdělíme na dva případy. Pro $p = q$: $\mathrm{Cov}[X_p, X_q] \leq \mathbb{E}[X_p^2] = \mathbb{E}[X_p]$, pak $\sum_p \mathrm{Var}[X_p] = \log\log n + \mathcal{O}(1)$.

Pro $p \neq q$ je $\mathrm{Cov}[X_p, X_q] = \mathbb{E}[X_p X_q] - \mathbb{E}[X_p]\mathbb{E}[X_q]$. $\mathbb{E}[X_p X_q] = \frac{\lfloor n/pq \rfloor}{n}$. $\mathrm{Cov}[X_p, X_q] \leq \frac{\lfloor n/pq \rfloor}{n} - \frac{\lfloor n/p \rfloor}{n} \cdot \frac{\lfloor n/q \rfloor}{n} \leq 1/np - (1/p - 1/n)(1/q - 1/n) \leq 1/n(1/p + 1/q)$. Pak $\sum_{p \neq q} \mathrm{Cov}[X_p, X_q] \leq 1/n \sum_{p \neq q} (1/p + 1/q) \leq 1/n\mathcal{O}(n/\log n) \cdot 2\sum_p 1/p \in \mathcal{O}(\log\log n/\log n) \to 0$.

Podle Čebyšeovy nerovnosti proto $P[|\nu(X) - \mathbb{E}[X]| \geq f(n)\sqrt{\log\log n}] \leq \frac{\mathrm{Var}[X]}{f^2(n)\log\log n} \in \mathcal{O}(1/f^2(n)) \to 0$. □

Lovász Local Lemma. Mějme špatné události $B_1, \ldots, B_n$ u kterých chceme, aby nenastaly všechny: $\bigcup B_i$ není Ω. Příkladem jsou Ramseyovy věty. Možnosti, jak počítat:

1. Pokud podle Union Bound $P[\bigcup B_i] \leq \sum P[B_i] < 1$, pak jsme hotovi, navíc B_i nejsou nezávislé.
2. Pokud události jsou nezávislé a $P[\bigcap B_i^C] = \prod P[B_i^C] > 0$, pak $P[\bigcap B_i] < 1$.

Našim cílem bude nějak využít omezenou nezávislost na odhady pravděpodobnosti.

Definice. Nechť $A, B_1, \ldots, B_k$ jsou náhodné jevy. Pak A je vzájemně nezávislý na $B_1, \ldots, B_k$, když $\forall J \subseteq [k] : P[A \bigcap_{j \in J} B_j] = P[A]$.

Jevy $B_1, \ldots, B_k$ jsou vzájemně nezávislé právě, když $\forall i \in [k] : B_i$ je nezávislý na zbylých B_j.

Definice. Nechť $B_1, \ldots, B_k$ jsou jevy a D je orientovaný graf o $V(D) = [k]$. Pak D je graf závislostí jevů $B_1, \ldots, B_k$ právě, když $\forall i \in [k] : B_i$ je nezávislý na $\{B_j \mid ij \notin E(D) \wedge i \neq j\}$.

Příklad. Pokud jevy $B_1, \ldots, B_k$ jsou vzájemně nezávislé, pak prázdný graf na k vrcholech je jejich graf závislostí.

Lemma 23 (LLL symetrické)**.** *Nechť $B_1, \ldots, B_k$ jsou náhodné jevy, kde $\forall i\, P[B_i] \leq p$, existuje graf závislostí s výstupním stupněm nejvýše d a $4pd \leq 1$ ($ep(d+1) \leq 1$). Pak $P[\bigcap B_i^C] > 0$.*

Uvažme extrémní případy. Když $d = 0$, dostáváme vzájemně nezávislé jevy, pak lemma platí vždy. Pokud $d = k - 1$, pak $4p(k-1) \leq 1$, což je varianta $\sum P[B_i] \leq pk < 1$.

Věta 24. *Nechť $\mathcal{H}$ je hypergraf takový, že každá hrana má alespoň k vrcholů a protíná nejvýše d ostatních hran. Pokud $e(d+1) \leq 2^{k-1}$, pak $\mathcal{H}$ je 2-obarvitelný.*

Důkaz. Uvažme náhodně zvolené obarvení $f : V(\mathcal{H}) \to \{0, 1\}$. Pro hranu $e \in E(\mathcal{H})$ mějme jev $B_e = \{f : |f(e)| = 1\}$ – hrana e je jednobarevná. Chceme $P[\bigcap B_e^C] > 0$.

Pravděpodobnost $P[B_e] = 2/2^l \leq 2^{1-k}$, kde l je počet vrcholů v e. Nyní mějme graf D, pro který $V(D) = E(\mathcal{H})$ a $ef \in E(D)$ právě, když $e \cap f \neq \emptyset$. Tento graf má maximální stupeň nejvýše d.

Podle definice je D graf závislosti, pokud $\forall e \in E(\mathcal{H}) : B_e$ je nezávislý na $\{B_f \mid e \neq f \wedge e \cap f = \emptyset\}$. To platí, protože B_e závisí pouze na hodnotách $f(v)$ pro $v \in e$, zatímce B_f závisí pouze na ostatních hodnotách.

Podle LLL, pokud $e2^{1-k}(d+1) \leq 1$, existuje korektní 2-obarvení. □

Podobná věta lze dokázat pomocí Union Bound, pokud zapomeneme na d a omezíme počet hran pod 2^{k-1}. Rozdílem je, že v této variantě máme globální podmínku oproti lokální podmínky protínání $\leq d$.

Routing v grafech. Chceme propojit s_i do t_i v grafu pro $i \in [n]$ hranově disjunktními cestami. Pro každé i máme F_i seznam m cest mezi s_i a t_i. Víme, že $\forall i \neq j\, \forall P \in F_i$ nejvýše k cest ve F_i sdílí hranu s P.

Věta 25. *Pokud $8nk/m \leq 1$, pak existuje $P_i \in F_i$ pro každé i takové, že $P_1, \ldots, P_n$ jsou hranové disjunktní.*

Důkaz. Pro každé i zvolme $P_i \in_u F_i$ náhodně rovnoměrně nezávisle. Pro $i \neq j$ mějme špatný jev $B_{i,j}$, kde P_i, P_j sdílí hranu, $P[B_{i,j}] \leq k/m$, jelikož $P[B_{i,j} \mid P_i = P]$ pro $P \in F_i$ je počet cest ve F_j protínajících P děleno $|F_j|$, což je nejvýše k/m.

Nyní uvažujme graf $D = (V, E)$, kde vrcholy odpovídají $\binom{n}{2}$ a $E = \{\{A, B\} \mid A \neq B, A \cap B \neq \emptyset\}$. Chceme, aby $B_{i,j}$ je nezávislý na $B_{k,l}$ tak, že k, l, i, j jsou po dvou různé. To platí, protože cesty jsou disjunktní. Jedná se proto o graf závislostí. Jeho maximální stupeň je $d = 2n - 2$.

Potom podle LLL, pokud $4pd \leq 4 \cdot 2n \cdot k/m \leq 8kn/m \leq 1$, existuje routing. □

Věta 26. *Nechť D je konečný orientovaný graf s δ^+ minimálním výstupním stupněm a Δ^- maximálním vstupním stupněm. Pokud $k \in \mathbb{N}$ a $k \leq \delta^+/(1 + \log(1 + \delta^+\Delta^-))$, pak D obsahuje orientovaný cyklus délky dělitelné k.*

Důkaz. Najdeme funkci $f : V(D) \to [k]$ takovou, že $\forall u \exists v \in N^+(u)$ takový, že $f(v) = f(u) + 1 \bmod k$. Abychom f našli, můžeme předpokládat, že $\forall v : \deg^+(v) = \delta^+$. Pak pro každý vrchol zvolíme $f(v)$ uniformně nezávisle náhodně.

Uvažujme jev $B_u : \forall v \in N^+(u) : f(v) \neq f(u) + 1 \bmod k$. Pak $P[B_u] = (1 - 1/k)^{\delta^+}$. Nyní chceme najít d v grafu závislosti, abychom splnili $ep(d + 1) \leq 1$.

Nechť $G_u = \{w : N^+(u) \cap (N^+(w) \cup \{w\}) = \emptyset\}$ a pro graf závislosti D máme $V = V(D)$ a $E = \{uw \mid w \neq u, w \notin G_u\}$. Pak $d = \delta^+\Delta^-$. Tudíž chceme, aby platilo $e(1-1/k)^{\delta}(\delta\Delta+1) \leq 1$. Pro volbu k ve větě máme vyhráno.

Proč to je graf závislosti? ... □

Lemma 27 (LLL, obecná verze)**.** *Nechť $B_1, \ldots, B_n$ jsou (špatné) jevy, D graf závislosti a $x_1, \ldots, x_n \in [0, 1]$. Pokud $P[B_i] \leq x_i \prod_{B_iB_j \in E(D)}(1 - x_j)$, potom $P[\bigcap B_i^C] > 0$.*

Důkaz, že obecná ⇒ symetrická. Máme $B_1, \ldots, B_n, D, p, d$, kde $ep(d+1) \leq 1$. Zvolíme $x_i = 1/(d + 1) < 1$, pokud $d \neq 0$. Kdyby platilo $d = 0$, pak D nemá hranu a jevy jsou nezávislé.

Pak $x_i \prod(1 - x_j) = 1/(d+1)(1 - 1/(d+1))^{\deg^+(B_i)} \geq 1/(d+1) \cdot 1/e \geq p \geq P[B_i]$. Proto podle obecného LLL jsme hotovi. □

Obvyklý důkaz je nekonstruktivní, ale algoritmická verze existuje: volíme náhodné proměnné, v případě nastání špatného jevu převzorkujeme proměnné, které jej ovlivňují.

Chernoffovy meze. Nechť $X_1, \ldots, X_\epsilon\{0,1\}$ jsou náhodné veličiny zvolene uniformně nezávisle. Uvažme $S_n = \sum_{i=1}^{n} X_i$. Potom $\mathbb{E}[S_n] = \sum \mathbb{E}[X_i] = n/2$. (Jedná se o rozdělení $Bin(n, 1/2)$.)

Příklad. Uvažme $\Delta(G(n, 1/2))$. Pro každý vrchol $v : \deg(v) \sim Bin(n-1, 1/2)$. Tudíž $\mathbb{E}[\deg(v)] = (n-1)/2$.

Nyní $P[\deg(v) > (n-1)/2 + t] < f_n(t)$, pokud $f_n(t) < 1/n^2$, pak $P[\Delta > (n-1)/2 + t] \leq n \cdot f_n(t) < 1/n$. Chceme tedy dostat $f_n(t)$ co nejníže.

Věta 28. *Nechť $Y_1, \ldots, Y_n \in \{+1, -1\}$ jsou uniformně náhodné nezávislé proměnné, $T_n = \sum_{i=1}^{n} Y_i$ a $t \geq 0$. Potom $P[T_n \geq t] < e^{-t^2/2n}$ a $P[T_n \leq -t] < e^{-t^2/2n}$.*

Výraz $e^{-t^2/2n}$ můžeme rovněž zapsat jako $e^{-t^2/2\sigma^2}$, kde $\sigma = \sqrt{n} = \sqrt{\mathrm{Var}[T_n]}$. Speciálně tedy $P[T_n \geq s\sigma] \leq e^{-s^2/2}$.

Vraťme se k příkladu. Pokud $Y_i = 2X_i - 1$, pak $T_n = 2S_n - n$ a speciálně $P[S_n > n/2 + t] = P[T_n/2 > t] < e^{-2t^2/n}$. Podobně, $P[\deg(v_1) > (n-1)/2 + t] < e^{-2t/(n-1)}$. To bude pod $1/n^2$, když zvolíme $t > \sqrt{n-1}\sqrt{\log n}$.

Podle Čebyševovy nerovnosti dostáváme $P[|T_n - \mathbb{E}[T_n]| > s\sigma] \leq 1/s^2$. Chernoffovy meze nám dávají $\leq 2e^{-s^2/2}$.

Důkaz. $T_n \geq t$ je ekvivalentní $e^{\lambda T_n} \geq e^{\lambda t}$ pro $\lambda > 0$. Pak $P[T_n \geq t] = P[e^{\lambda T_n} \geq e^{\lambda t}] \leq \mathbb{E}[X]/e^{\lambda t}$ (podle Markova).

$\mathbb{E}[X] = \mathbb{E}[e^{\lambda \sum Y_i}] = \mathbb{E}[\prod e^{\lambda Y_i}] = \prod \mathbb{E}[e^{\lambda Y_i}] = ((e^{\lambda} + e^{-\lambda})/2)^n = \cosh^n \lambda$. Odhadneme $\cosh \lambda \leq e^{\lambda^2/2}$. Proto $\mathbb{E}[X] \leq e^{\lambda^2 n/2}$.

Nakonec tedy $P[T_n \geq t] \leq e^{\lambda^2 n/2 - \lambda t}$. Chceme minimalizovat výraz přes λ. Když zvolíme $\lambda = t/n$, dostáváme správnou mez.

Druhou mez dokážeme analogicky pro $-Y_i$. □

Kombinatorický rozpor. Mějme množinu X velikosti n a $\mathcal{S} \subseteq P(X)$. Chceme obarvit X dvěma barvami vyrovnaně.

Definujme $c : X \to \{-1, 1\}$ a nevyrovnanost $S \in \mathcal{S} : c(S) = \sum_{x \in S} c(x)$ a rozpor $\mathrm{disc}(\mathcal{S}, c) = max_{S \in \mathcal{S}} |c(S)|$ a $\mathrm{disc}(\mathcal{S}) = \min_c \mathrm{disc}(\mathcal{S}, c)$.

Tvrzení 29. *Nechť $|X| = n, |\mathcal{S}| = m$. Potom $\mathrm{disc}(\mathcal{S}) \leq \sqrt{2n \log(2m)}$. Pokud $\forall s \in \mathcal{S} : |S| \leq s$, pak $\mathrm{disc}(\mathcal{S}) \leq \sqrt{2s \log(2m)}$.*

Důkaz. Chceme, aby existovalo c takové, že $\mathrm{disc}(\mathcal{S}, c) \leq \sqrt{2s\log(2m)} = t$. Zvolme $c : X \to \{-1, 1\}$ náhodně. Dále chceme: $\forall S \in \mathcal{S} : |c(S)| \leq t$.

Uvažujme špatný jev $B_S = \{c \mid |c(S)| > t\}$. Pak $P[B_S] \leq P[|c(S)| \geq t] = P[|\sum_{x\in S} c(x)| \geq t]$. Sčítáme $|S|$ nezávislých veličin, každá ± 1. Proto $P[B_S] < 2e^{-t^2/2|S|} \leq 2e^{t^2/2s} = 2e^{-\log 2m} = 1/m$.

Pak $P[B_s] < 1/m$, a proto $P[\bigcup_{s\in\mathcal{S}} B_s] < 1$. □

Věta 30 (Chernoffovy meze (aditivní))**.** *Mějme nezávislé náhodné proměnné $X_1, \ldots, X_n$, $0 \leq X_i \leq 1$ a $X = \sum_{i=1}^n X_i$, $\sigma^2 = \mathrm{Var}[X]$. Potom $P[X \geq \mathbb{E}[X] + t]$ a $P[X \leq \mathbb{E}[X] - t]$ je ostře menší $e^{-t^2/2(\sigma^2+t/3}$.*

Věta 31 (Chernoffovy meze (multiplikativní))**.** *Mějme nezávislé náhodné proměnné $X_1, \ldots, X_n$, $X_i \in \{0, 1\}$ a $X = \sum_{i=1}^n X_i$, $\mu = \mathbb{E}[X]$. Potom $P[X \geq (1+\delta)\mu < (e^\delta/(1+\delta)^{1+\delta}))^\mu$ a $P[X \geq (1-\delta)\mu < (e^{-\delta}/(1-\delta)^{1-\delta}))^\mu$.*

První tvar lze zjednodušit na $e^{-\mu\delta^2/3}$ pro $\delta \in (0, 1)$, druhý na $e^{-\mu\delta^2/2}$.

Důkaz. Chceme ukázat $P = P[e^{tX} \geq e^{t(1+\delta)\mu}] \leq \mathbb{E}[e^{tX}]/e^{t(1+\delta)\mu}$ podle Markova pro $t > 0$. Pak $\mathbb{E}[e^{tX}] = \mathbb{E}[e^{\sum tX_i} = \prod \mathbb{E}[e^{tX_i}]$. Označme $p_i = P[X_i = 1]$. Dostaneme $\mathbb{E}[e^{tX_i}] = e^t p_i + e^0(1-p) = 1 + p(e^t - 1) \leq e^{p_i(p^t-1)}$.

Tudíž $P \leq (e^{e^t-1}/e^{t(1+\delta)})^\mu$. Pokud dosadíme $t = \log(1+\delta)$, dostaneme hledaný tvar. □

Důsledek 32. *$P[|X - \mu| > \delta\mu] < 2e^{c_\delta \mu}$, kde c_δ je konstanta závislá na δ.*

Důsledek 33. *Pokud $R \geq 6\mu$, pak $P[X \geq R] \leq 2^{-R}$.*

Důkaz. Zvolme $\delta = R/\mu - 1 \geq 5$. Pak $P[X \geq R] = P[X \geq (1+\delta)\mu] \leq (e^{\delta+1}/(1+\delta)^{1+\delta})^\mu = (e/(1+\delta))^(1+\delta)\mu$. Navíc $(1+\delta)/e \geq 6/e \geq 2$. □

Routování v hyperkrychli.

Budeme modelovat přenos informací v počítačových sítí, kterou budeme uvažovat jako graf. Jak rychle se přenese informace? Pokud graf je úplný, je vše rychlé, ale jaksi to chce hodně drátů. Nás bude zajímat graf hyperkrychle $G = Q_n : V(G) = \{0,1\}^n, E(G) = \{xy \mid d_H(x,y) = 1\}$.

Navíc každý paket může procházet nejvýše jednou hranou najednou a každá hrana pojme nejvýše jeden paket.

Bit Fixing Algoritmus
Vstup: $a, b \in V(Q_n)$
Výstup $a - b$ cesta

Pro $i = 1, \ldots, n$: Pokud $a_i \neq b_i$, vypiš $(b_1, \ldots, b_i, a_{i+1}, \ldots, a_n)$.

Takový algoritmus je jistě nezajímavý a trvá $\mathcal{O}(N)$. Co když chceme posílat více paketů najednou?

Budeme chtít permutační routování, tedy permutaci $\pi : V \to V$, kde chceme poslat paket $v \to \pi(v)$, a to najednou.

Triviální postup je sekvenčně, pak máme čas $\mathcal{O}(Nn)$. Existuje dolní odhad $\sqrt{N}$ pro špatnou permutaci. Jistě existuje lepší způsob.

Dvou fázový algoritmus (TPA)
Vstup: π
Výstup: Routovací schéma

Zvol náhodné $f : V \to V$. V první fázi použij BFA na dopravení paketu $v \to f(v)$, v druhé pak pošli $v \to \pi(v)$, vše paralelně.

Motivace je následující: Je to nejhůře dvakrát pomalejší, ale hlavně nastane nějaká randomizace, která může zachránit špatné permutace (podobně jako u Quicksortu).

Věta 34. *Pro každou permutaci π na V platí:*
$P[$*TFA routuje v* $\mathcal{O}(\log N)$ *paralelních krocích*$] \geq 1 - \mathcal{O}(1/N)$.

Důkaz. Analyzujme fázi 1. Označme náhodnou veličinu $X(e)$ jako počet paketů procházejících hranou e. Dále p bude přípustná cesta $e_1, \ldots, p_m$ a $T(p) = \sum_{i=1}^{m} X(e_i)$.

👁 První fáze zabere nejvýše $\max_p T(p)$ paralelních kroků.

Cílem je $P[\exists P : T(P) \geq 30n] \leq 1/N$. Zvolme fixní $P = v_0, v_1, \ldots, v_m$. Paket z a do náhodného $f(a)$ je aktivní ve v_{i-1}, pokud dosáhne v_{i-1} a

může pokračovat do v_i. Definujme H_a jako indikátor, jenž je 1 právě, když paket z a je aktivní v nějakém v_{i-1}. Pak $H = \sum_{a \in V} H_a$ součet nezávislých veličin.

Střední hodnota $\mathbb{E}[H] = \sum \mathbb{E}[H_a]$, kde $\mathbb{E}[H_a] \leq \sum_{i=1}^{n} P[a \text{ je aktivní ve } v_{i-1}]$. Nechť $v_{i-1} = (b_1, \ldots, b_{j-1}, a_j, \ldots, a_n)$ a $v_i = (b_1, \ldots, b_{j-1}, b_j, a_{j+1}, \ldots, a_n)$. Prvních $j-1$ bitů je stejných, jako $f(a)$, bity od $j+1$-tého se shodují s a.

Tedy $P[a \ldots v_{i-1}] \leq 2^{j-1}$ a rovná se 0, pokud v_{i-1}, a se neshodují v bitech $j+1, \ldots, n$. Proto $\mathbb{E}[H] = m \leq n$.

Podle Chernoffa pak $P[H \geq 6n] \leq 2^{-6n}$. Dále $P[T(P) \geq 30n] \leq P[H \geq 6n] + P[T(P) \geq 30n \mid H < 6n]$. Vyrobíme si $36n$ hodu mincí, potřebujeme alespoň $6n$ úspěchů. Proto podmíněná pravděpodobnost je nejvýše $P[Bin(36n, 1/2) < 6n] \leq e^{18n(2/3)^2/2} = e^{-4n} \leq 2^{-3n-1}$.

Celková pravděpodobnost je proto nejvýše 2^{-3n}. Pak pravděpodobnost, že existuje špatná cesta, je maximálně $2^{-3n} \cdot \#P \leq 2^{-3n} \cdot 2^{2n} = 1/N$. □

Markovovy řetězce.

Definice. Stochastický proces $X = \{X(t) \mid t \in T\}$ je množina náhodných veličin, kde $X(t) = X_t$ je stav X v času t.

Pokug $\text{rng}(X_t)$ je spočetný, je tento proces diskrétním prostorem. Pokud T je spočetná, říká se tomu diskrétní čas.

Definice. $X_0, X_1, \ldots$ je množina náhodných proměnných, pak X je markovovský řetězec, pokud $P[X_t = a_t \mid X_0 = a_0, X_1 = a_1, \ldots, X_{t-1} = a_{t-1}] = P[X_t = a_t \mid X_{t-1} = a_{t-1}]$ pro každé $t \in \mathbb{N}$.

Této vlastnosti se často říká *memoryless property.*

Často budeme uvažovat speciální případ, kde $\text{rng}\, X_0, \text{rng}\, X_1, \cdots \subseteq \mathbb{N}$. Pak můžeme Markovovský řetězec X definovat jako orientovaný graf $D = (V, E, w)$ pro $V \subseteq \mathbb{N}, E \subseteq V^2, w : E \to \mathbb{R}$. Smyčky mohou existovat a pro každý vrchol musí být součet vah přes výstupní hrany právě 1.

V takovém grafu pak X odpovídá nějaké náhodné procházce.

Číslo $P_{i,j}$ bude značit $P[X_t = j \mid X_{t-1} = i]$. Budeme předpokládat, že $P_{i,j}$ nebude záležet na čase. Z toho pak můžeme utvořit čtvercovou matici přechodu P.

Distribuční vektor $p(t) = (p_0(t), p_1(t), \dots)$, kde $p_i(t) = P[X_t = i]$ popisuje distribuci náhodné veličiny čase t.

👁 $p(t+1) = p(t) \cdot P$.

Důkaz. Podívejme se na $p_j(t+1)$. To jest $P[X_{t+1} = j] = \sum_i P[X_{t+1} = j \mid X_t = i] P[X_t = i] = \sum_i P_{i,j} p_i(t) = p(t) \cdot P$. □

Uvažme $P^m_{i,j} = P[X_{t+m} = j \mid X_t = i]$. Pokud časy se nemění, pak $P^m_{i,j} = (P^m)_{i,j}$ (lze dokázat iterací předchozího pozorování).

2-SAT. Mějme $\varphi = C_1 \wedge C_2 \wedge \dots$ formuli v CNF takovou, že každá klauzule C_i má nejvýše dva literály. Dále n je počet proměnných.

Obecný SAT je NP-úplný, na druhou stranu 2-SAT je polynomiální. Ukážeme si algoritmus založený na Markovovských řetězcech:

1. Zvol nějaké ohodnocení A_0
2. Opakuj nejvýše $2mn^2$ krát:
   (a) Pokud φ je splněná, skonči kladně
   (b) Zvol C_i nesplněnou ohodnocením a změň ohodnocení náhodné proměnné literálu.
3. Skonči záporně

Věta 35. *Pokud φ není splnitelná, pak algoritmus vždy funguje, jinak funguje s pravděpodobností alespoň $1 - 2^{-m}$.*

Důkaz. Pokud φ není splnitelná, pak vždy algoritmus projde smyčkou a odpoví správně. Jinak si zafixujeme jedno splňující ohodnocení A^*.

Označme A_t jako ohodnocení a X_t jako počet proměnných shodujících se s A^* v čase t.

Pokud $X_t = n$, pak jistě končíme. Pokud $X_t = 0$, pak jistě $X_{t+1} = 1$. Pokud $1 \leq X_t < n$, uvažme nesplněnou $C_i = x_1 \vee x_2$. Tudíž v A_t $x_1 = x_2 = 0$. Naopak v A^8 platí $x_1 = 1$ nebo $x_2 = 1$ nebo obojí.

Pokud v A^* platí $x_1 = x_2 = 1$, pak $X_{t+1} = X_t + 1$. Když pro A^* platí $x_1 = 0, x_2 = 1$, pak $X_{t+1} = \pm 1$ s pravděpodobností $1/2$. Tudíž $P[X_{t+1} = j+1 \mid X_t = j] \geq 1/2$ a $P[X_{t+1} = j-1 \mid X_t = j] \leq 1/2$.

Definujme $Y_0, Y_1, \ldots$ pesimistický odhad X_t tak, že $Y_0 = X_0$, $P[Y_{t+1} = 1 \mid Y_t = 0] = 1$ a $P_[Y_{t+1} = j \pm 1 \mid Y_t = j] = 1/2$. To je již Markovovský řetězec s popisující náhodnou procházku na přímce z bodu 0 do bodu n. Zajímá nás $\mathbb{E}[\min t : Y_t = n]$.

Označme $h_j = \mathbb{E}[\text{počet kroků k dosáhnutí } Y_t = n \mid Y_0 = j]$. Potom $h_0 = 1 + h_1$, $h_n = 0$ a $h_j = 1 + (h_{j-1} + h_{j+1})/2$. Dostáváme $h_j = n^2 - j^2$.

$\mathbb{E}[\min t : X_t = n] \leq \mathbb{E}[\min t : Y_t = n] \leq h_0 = n^2$. Tudíž $P[\min(t : X_t = n) \geq 2n^2] \leq 1/2$.

Nyní si rozdělíme proces na m bloků velikosti $2n^2$. Každý blok si můžeme představit jako nezávislý výpočet. Pravděpodobnost, že první blok selže je nejvýše $1/2$. Stejná pravděpodobnost selhání je i pro ostatní bloky. To nám dává pravděpodobnost selhání 2^{-m}. □