Poznámky - kombinatorika a grafy I

Petr Chmel

Odhady faktoriálu

Tvrzení 1 (Triviální odhad faktoriálu pomocí n^n)**.** $\forall n \geq 1 : n^{\frac{n}{2}} \leq n! \leq (\frac{n+1}{2})^n$

Důkaz. Triviální, plyne z $(n!)^2$ a přerovnání. $\boxplus$

Lemma 1 (e^x a $1+x$)**.** $\forall x \in \mathbb{R} : 1 + x \leq e^x$

Důkaz. Derivace - zjistíme, že $1+x$ je tečnou e^x a e^x je konvexní - tedy je pod grafem. $\boxplus$

Věta 1 (Odhad faktoriálu pomocí $(\frac{n}{e})^n$)**.** $\forall n \in \mathbb{N} : e(\frac{n}{e})^n \leq n! \leq en(\frac{n}{e})^n$

Důkaz indukcí. Horní odhad: $n = 1$ - platí, ověříme dosazením.
$n \geq 2 : n! = n \cdot (n-1)! \leq ne(n-1)(\frac{n-1}{e})^{n-1} = en(\frac{n}{e})^n(\frac{n-1}{n})^n \cdot e \leq en(\frac{n}{e})^n$.
Poslední nerovnost platí, pokud $(\frac{n-1}{n})^n e \leq 1$. Upravíme: $(\frac{n-1}{n})^n e = (1-\frac{1}{n})^n e \leq (e^{-1/n})^n e = e^{-1}e = 1$.
Dolní odhad analogicky, jenom chceme přebytek ≥ 1. $\boxplus$

Důkaz s integrálem. Uvažme $\ln(n!) = \ln 1 + \ln 2 + \ldots + \ln n = \sum_{i=1}^{n} \ln(i)$ Když si nakreslíme graf, můžeme odhadnout shora pomocí $\sum_{i=1}^{n} \ln(i) \leq \int_{i}^{n+1} \ln x dx = [x \ln x - x]_1^{n+1} = (n+1)\ln(n+1) - n + 1$. Dále $n! = n \cdot (n-1)! \leq n \cdot ne^{n \ln n - n + 1} = n \cdot e^{-(n-1)} \cdot e^{n \ln n} = en(\frac{n}{e})^n$.
Podobně dolní odhad. $\boxplus$

Věta 2 (Stirlingova formule)**.** Nechť $f(n) = \sqrt{2\pi n} \cdot (\frac{n}{e})^n$. Potom $\lim_{n\to\infty} \frac{f(n)}{n!} = 1$.

Odhady binomických koeficientů

$\frac{n^k}{k^k} = \left(\frac{n}{k}\right)^k \leq \binom{n}{k} = \frac{n!}{k!(n-k)!} \leq \frac{n^k}{k!}$ pro malé hodnoty k

Tvrzení 2. Nechť $n, k \in \mathbb{N}, 1 \leq k \leq n$. Pak $\binom{n}{k} \leq (\frac{en}{k})^k$

Důkaz. Ukážeme $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k} \leq (\frac{en}{k})^k$.
Z binomické věty: $\binom{n}{0} + \binom{n}{1}x + \ldots + \binom{n}{k}x^k + \ldots + \binom{n}{n}x^n = (1+x)^n$. Pro $x > 0$:0 $\binom{n}{0} + \binom{n}{1}x + \ldots + \binom{n}{k}x^k \leq (1+x)^n$.
Vydělíme x^k: $\frac{(1+x)^n}{x^k} \geq \frac{1}{x^k}\binom{n}{0} + 1x^{k-1}\binom{n}{1} + \ldots + \binom{n}{k} \overset{\text{Z } 1 \geq x > 0}{\geq} \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k}$. Dosadíme $0 < x = \frac{k}{n} \leq 1$:
$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k} \leq \frac{(1+\frac{k}{n})^n}{(\frac{k}{n})^k} \overset{1+x \leq e^x}{\leq} \frac{(e^{\frac{k}{n}})^n}{(\frac{k}{n})^k} = (\frac{en}{k})^k$ $\boxplus$

Triviální odhad: $\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq \frac{2^{2n}}{\sqrt{2n}}$

Věta 3. Pro $n \geq 1 : \frac{2^{2n}}{2\sqrt{n}} \leq \binom{2n}{n} \leq \frac{2^{2n}}{\sqrt{2n}}$

Důkaz. Uvažme $P_n = \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)}{2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n} = \frac{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (2n-1) \cdot 2n}{(2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n)^2} = \frac{(2n)!}{2^{2n}(n!)^2} = \frac{1}{2^{2n}} \cdot \binom{2n}{n}$
Tím z věty: $\frac{1}{2\sqrt{n}} \leq P_n \leq \frac{1}{\sqrt{2n}}$.
Horní odhad: uvažme $(1-\frac{1}{2^2})(1-\frac{1}{4^2})(1-\frac{1}{6^2})\ldots(1-\frac{1}{(2n)^2}) = \frac{1 \cdot 3}{2^2} \cdot \frac{3 \cdot 5}{4^2} \cdot \frac{5 \cdot 7}{6^2} \cdot \ldots \cdot \frac{(2n-1)(2n+1)}{(2n)^2} = (2n+1)(P_n)^2 < 1$.
Poslední nerovnost plyne z toho, že jednotlivé čitatele byly kladné a menší 1. Pak $(P_n)^2 < \frac{1}{2n+1} < 2n \Rightarrow P_n < \frac{1}{\sqrt{2n}}$.
Dolní odhad: uvažme $(1-\frac{1}{3^2})(1-\frac{1}{5^2})(1-\frac{1}{6^2})\ldots(1-\frac{1}{(2n-1)^2}) = \frac{2 \cdot 4}{3^2} \cdot \frac{4 \cdot 6}{5^2} \cdot \frac{6 \cdot 8}{7^2} \cdot \ldots \cdot \frac{(2n-2)2n}{(2n-1)^2} = \frac{1}{(P_n)^2} \cdot \frac{1}{4n} < 1$.
Pak $(P_n)^2 > \frac{1}{4n} \Rightarrow P_n > \frac{1}{2\sqrt{n}}$. $\boxplus$

Ze Stirlingovy formule: $\binom{2n}{n} \approx \frac{2^{2n}}{\sqrt{\pi n}}$
Aplikace: náhodná procházka po přímce - TODO

Vytvořující funkce

Definice 1 (Vytvořující funkce)**.** Vytvořující funkce posloupnosti $(a_i)_{i=0}^{\infty}, a_i \in \mathbb{R}$ je mocninná řada $\sum_{i=0}^{\infty} a_i x^i = a(x)$.

Fakt 1 (AK vytvořující funkce - z MAI)**.** Pokud pro $(a_i)_{i=0}^{\infty}$ existuje $k \in \mathbb{R}$ t.ž. $\forall i : |a_i| < k^i$, pak $\forall x \in (-\frac{1}{k}, \frac{1}{k})$ platí, že řada $\sum_{i=0}^{\infty} a_i x^i$ konverguje absolutně. Dále výsledná funkce $a(x)$ jednoznačně určuje koeficienty, protože $a_i = \frac{a^{(i)}(0)}{i!}$.

Operace s mocninnými řadami: TODO

Definice 2 (Zobecněné kombinační číslo)**.** Pro $r \in \mathbb{R}, k \in \mathbb{Z}_0^+$ definujeme kombinační číslo $\binom{r}{k} := \frac{r(r-1)\cdot\ldots\cdot(r-k+1)}{k!}$.

Věta 4 (Zobecněná binomická)**.** Pro každé $r \in \mathbb{R}$ platí, že funkce $(1+x)^r$ je vytvořující funkcí posloupnosti $(\binom{r}{0}, \binom{r}{1}, \ldots, \binom{r}{n})$. Řada $\sum_{i=0}^{\infty} \binom{r}{i} x^i$ konverguje $\forall x \in (-1, 1)$.

Důkaz. Využitím Taylorova rozvoje $(1+x)^r$ (z analýzy).
$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \ldots, f(x) = (1+x)^r, f'(x) = r(1+x)^{r-1}, f''(x) = r(r-1)(1+x)^{r-2}$.
Vyjadřujeme, tedy $a = 0$ - $f(x) = f(0) + f'(0)(x-0) + \frac{f''(0)}{2!}(x-0)^2 + \ldots = 1 + rx + \frac{r(r-1)}{2!}x^2 + \ldots = \binom{r}{0} + \binom{r}{1}x + \binom{r}{2}x^2 + \ldots = \sum_{i=0}^{\infty} \binom{r}{i} x^i$. ⊞

Důsledek 1. Je-li $r \in \mathbb{Z}^-$: Pro $n \in \mathbb{N} : r - n, x \in (-1, 1) : \frac{1}{(1-x)^n} = (1-x)^{-n} = \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} x^i$.

Důkaz pomocí zobecněné binomické věty. $(1-x)^{-n} = \sum_{i=0}^{\infty} \binom{-n}{i}(-x)^i = \sum_{i=0}^{\infty} \frac{-n\cdot(-n-1)\cdot(-n-2)\cdot\ldots\cdot(-n-i+1}{i!} \cdot (-x)^i = \sum_{i=0}^{\infty} \frac{n\cdot(n+1)\cdot(n+2)\cdot\ldots\cdot(n+i-1}{i!} \cdot (-x)^i = \sum_{i=0}^{\infty} \binom{n+i-1}{i} \cdot (-x)^i$ ⊞

Kombinatorický důkaz. $(1-x)^{-n} = \frac{1}{1-x} \cdot \frac{1}{1-x} \cdot \ldots \cdot \frac{1}{1-x} = (1 + x + x^2 + \ldots)^n = \sum_{i=0}^{\infty} a_i x^i \overset{\text{kuličky a přihrádky}}{=} \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} x^i$ ⊞

Příklad 1 (Formule pro vyjádření Fibonacciho čísel)**.** Mějme posloupnost $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n \Leftrightarrow 0 = F_{n+2} - F_{n+1} - F_n$. Z toho nám (s pomocí obrázku - TODO) vyplyne $F(x) - xF(x) - x^2F(x) = x \Rightarrow F(x) = \frac{x}{1-x-x^2} \overset{\text{parc. zlomky}}{=} \frac{A}{x-x_1} + \frac{B}{x-x_2} = \frac{a}{1-\lambda_1 x} + \frac{b}{1-\lambda_2 x}, \lambda_i = \frac{1}{x_i}$.
Uvažme $a(x) = \frac{a}{1-\lambda_1 x} \to (a, a\lambda_1, a\lambda_1^2, \ldots) \Rightarrow a_n = a\lambda_1^n$, tedy pro $a(x), b(x) : F_n = a(x) + b(x)$.
Vypočtu $\lambda : 1 - x - x^2 = 0 \Leftrightarrow \lambda^2 - \lambda - 1 = 0 \Rightarrow \lambda_{1,2} = \frac{1\pm\sqrt{5}}{2}$.
Z předchozích: $F_n = a(\frac{1+\sqrt{5}}{2})^n + b(\frac{1-\sqrt{5}}{2})^n$. Z $F_0, F_1 : F_0 = 0 = a + b, F_1 = a(\frac{1+\sqrt{5}}{2}) + b(\frac{1-\sqrt{5}}{2})$. Z tohoto plyne $a = b = \frac{1}{\sqrt{5}} \Rightarrow F_n = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]$

Příklad 2 (Počet zakořeněných binárních stromů)**.** $b_0 = b_1 = 1, b_n = \sum_{k=0}^{n-1} b_k b_{n-k-1} \Rightarrow b_{n+1} = \sum_{k=0}^{n} b_k b_{n-k}$.
Pomocí obrázku (TODO): $b(x) = xb^2(x) + 1 \Rightarrow b(x) = \frac{1\pm\sqrt{1-4x}}{2x}$ - to by znamenalo 2 funkce. Ale rozhodneme pomocí $b(0)$ - zjistíme, že s + se v 0 dostáváme do nekonečna, což není správně. Ze zobecněné binomické věty: $\sqrt{1-4x} = (1-4x)^{\frac{1}{2}} = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k}(-4x)^k \Rightarrow$ koeficient u x^k v rozvoji odmocniny: $\binom{\frac{1}{2}}{k}(-4)^k$, tedy v celé vytvořující funkci koeficient u x^{k-1} : $\frac{-1}{2}\binom{\frac{1}{2}}{k}(-4)^k$ (nemám absolutní člen, tedy můžu dělit).
$b_k = -\frac{1}{2}\binom{\frac{1}{2}}{k}(-4)^{k+1} = (-1)^k 2^{2k+1} \frac{\frac{1}{2}\cdot\frac{-1}{2}\cdot\ldots\cdot\frac{1-2k}{2}}{(k+1)!} = 2^{2k} \frac{\frac{1}{2}\cdot\frac{3}{2}\cdot\ldots\cdot\frac{2k-1}{2}}{(k+1)!} = 2^k \frac{1\cdot3\cdot5\cdot(2k-1)}{(k+1)!} = \frac{1\cdot3\cdot5\cdot(2k-1)\cdot2^k(k!)}{(k+1)!k!} = \binom{2k}{k}\frac{1}{k+1}$, což je Catalanovo číslo.

Definice 3 (Konečná projektivní rovina)**.** Nechť X je konečná množina a $\mathcal{P} \subseteq 2^X$. Dvojice $(X, \mathcal{P})$ je konečná projektivní rovina, pokud:

1. $\exists C \subseteq X : |C| = 4, \forall p \in \mathcal{P} : |p \cap C| \leq 2$ (existence čtveřice v obecné poloze)
2. $\forall p_1, p_2 \in \mathcal{P} : p_1 \neq p_2 \Rightarrow |p_1 \cap p_2| = 1$
3. $\forall x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow \exists p \in \mathcal{P} : \{x_1, x_2\} \subseteq p$

Dále prvky X nazýváme body a prvky $\mathcal{P}$ nazýváme přímky.

Příklad 3 (Fanova rovina)**.** Obrázek - TODO

Věta 5 (Počet bodů přímky)**.** Každé dvě přímky v konečné projektivní rovině mají stejný počet bodů.

Důkaz. Mějme přímky P, Q, nejprve ukážeme $\exists x \in X : x \notin P, x \notin Q$. Vezmeme C. Pokud $|C \cap (P \cup Q)| \leq 3$, pak vezmeme $x \in X \setminus (P \cup Q)$. Jinak $C \subseteq P \cup Q$, tj. $|C \cap P| = |C \cap Q| = 2, C = \{a, b, c, d\}$. BÚNO $a, b \in P, c, d \in Q$. Pak vezmeme $\overline{ad}, \overline{bc}$. Zjevně $\exists x : \overline{ad} \cap \overline{bc} = \{x\}, x \in C$, zároveň nutně x není ani na jedné z přímek P, Q.
Nyní označme $P = \{z_1, z_2, \ldots, z_n\}$. Uvážíme přímky $\overline{xz_1}, \ldots, \overline{xz_k} : \forall i \in [k] \exists! q \in Q : \overline{xz_i} = \overline{xq}$. Tento bod označme $\varphi(z_i)$. Zjevně je toto zobrazení $\varphi : P \to Q$ prosté (jinak by neplatil 2. axiom). Analogicky umíme sestrojit prosté zobrazení $\kappa : Q \to P$, tedy $|Q| = |P|$. ⊞

Definice 4 (Řád konečné projektivní roviny)**.** Řád konečné projektivní roviny $(X, \mathcal{P})$ je $\forall P \in \mathcal{P} : |P| - 1$.

Definice 5 (Graf incidence, duální systém)**.** Graf incidence množinového systému $(X, \mathcal{S})$ je bipartitní graf na $X \cup S$, kde $(x, S) \in E \Leftrightarrow x \in S$.
Pro množinový systém $(X, \mathcal{S})$ je $(\mathcal{S}, \{\{S \in \mathcal{S} : x \in X\} : x \in X\})$ duální množinový systém (vznikne záměnou rolí bodů a přímek v grafu incidence).

Věta 6 (Duál ke KPR je KPR)**.** Duální množinový systém ke konečné projektivní množině je konečná projektivní množina.

Důkaz. Ověříme axiomy:

1. Mějme $C = \{a, b, c, d\}$ čtveřici na výchozím systému. Potom přímky $\overline{ab}, \overline{bc}, \overline{cd}, \overline{da}$ splňují axiom čtveřice.
2. Mějme dva body duálu: $P, Q \in \mathcal{P} : \exists x \in P \cap Q$, což je hledaná přímka ($\{S : x \in S\}$).
3. Mějme dvě přímky duálu: $\{S : x \in S\}, \{S : x \in S\}$. Uvažme $\overline{xy}$. ta patří do obou a je nutně jediná.

⊞

Věta 7 (Vlastnosti KPR)**.** Je-li $(X, \mathcal{P})$ konečná projektivní rovina řádu n, potom

1. $\forall x \in X : |\{P \in \mathcal{P} : x \in P\}| = n + 1$
2. $|X| = n^2 + n + 1$
3. $|\mathcal{P}| = n^2 + n + 1$

Důkaz.
1. Máme $x \in X$. Najdeme $p \in \mathcal{P} : x \in p$ (taková existuje z axiomů). p má $n + 1$ bodů. Všechny přímky procházející x musí nutně protínat p, tedy jich je $n + 1$.
2. Na každé přímce $\overline{z_i p}$ je $n+1$ bodů, z nichž $n-1$ neznáme, navíc neleží na žádné jiné z přímek. Celkem tedy máme $(n + 1) \cdot n + 1 = n^2 + n + 1$
3. Plyne z 2 a duálního systému (tj. konečná projektivní množina téhož řádu).

⊞

Věta 8 (Konečné těleso a KPR)**.** Pokud existuje konečné těleso o n prvcích, pak existuje i konečná projektivní rovina řádu n.

Důkaz. Mějme dáno $\mathbb{T}$, na $\mathbb{T}^3$ zavedeme ekvivalenci $\sim$,: $(a, b, c) \sim (\alpha a, \alpha b, \alpha c), \alpha \in \mathbb{T} \setminus \{0\}$.
Body budou třídy ekvivalence $\sim$ na $\mathbb{T}^3 \setminus \{0\}$. Těchto bodů je $\frac{n^3-1}{n-1} = n^2 + n + 1$.
Přímky budou $P_{a,b,c} = \{(x, y, z) \in X : ax + by + cz = 0, (a, b, c) \neq 0\}$.
Pozorování: $(a, b, c) \sim (a', b', c') \Rightarrow P_{a,b,c} = P_{a',b',c'} \Rightarrow$ Přímek je $n^2 + n + 1$.
Nyní stačí ověřit axiomy:

1. $C = \{(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)\}$.
2. 2 body $(x, y, z), (x'y'z')$ určují přímku $P_{a,b,c}$: dostaneme soustavu s maticí, která má hodnost 2, tedy její dimenze jádra je 1, což je námi hledaná přímka.
3. Obdobně jako 2.

⊞

Nekonečná projektivní rovina

Vytvoříme stejně jako konečnou, jen jako těleso použijeme $\mathbb{R}$. V nekonečnu jsou dva body, která jsou jeden bod, takže třeba K_5 umíme nakreslit v nekonečné projektivní rovině.

Latinské čtverce

Definice 6 (Latinský čtverec, ortogonalita LČ)**.** Latinský čtverec řádu n je tabulka o rozměrech $n \times n$ vyplněná n různými symboly tak, že se v žádném řádku ani sloupci žádný symbol neopakuje.
Dva latinské čtverce stejného řádu jsou ortogonální, pokud platí, že pro každou dvojici symbolů a, b existuje souřadnice $i, j \in [n]$ takové, že první čtverec A splňuje $A_{ij} = a$ a druhý čtverec splňuje $B_{ij} = b$.

Pozorování. Nejen existence, ale i jednoznačnost: $|[n] \times [n]| = |S \times S|$, kde S je množina symbolů.

Pozorování. Permutace řádků (sloupců) vytvoří z latinského čtverce opět latinský čtverec.

Pozorování. Je-li $\pi \in S_n$ a A je latinský čtverec, potom $\pi(A)$ je rovněž latinský čtverec.

Důsledek 2 (První řádek latinského čtverce)**.** Bez újmy na obecnosti lze v latinských čtvercích vyžadovat první řádek $1, 2, \ldots, n$.

Pozorování. Přepermutování symbolů zachovává ortogonalitu.

Důsledek 3 (Počet ortogonálních latinských čtverců)**.** Vzájemně ortogonálních latinských čtverců řádu n může být nejvýše $n - 1$.

Důkaz. Zpermutujeme první řádky na $1, \ldots, n$. Na pozici $2, 1$ nutně musejí být různé symboly z $\{2, 3, \ldots, n\}$ - těch je $n - 1$. ⊞

Pozorování. Jsou-li $L_1, \ldots, L_{n-1}$ ortogonální latinské čtverce řádu n, pak $\forall k, k', l, l' : k \neq k', l \neq l' \exists i : (L_i)_{k,l} = (L_i)_{k',l'}$.

Důkaz. Přepermutujeme čtverce tak, aby $\forall i : (L_i)_{k,l} = 1$. Podíváme se u všech čtverců na l'-tý sloupec - celkem můžu jedničku umístit na $n - 1$ pozic (1 nesmím umístit na k, l'). Zároveň 1 musí být pokaždé jinde, jinak by čtverce nebyly ortogonální. Tím pádem se musí jednou trefit do k', l' - kdyby ne: Dirichlet $\Rightarrow$ dvě místa, kde jsou dvě 1 na sobě $\Rightarrow \lightning$ ⊞

Věta 9 (Vztah konečné projektivní roviny a latinských čtverců)**.** Konečná projektivní rovina řádu n existuje $\Leftrightarrow$ existuje $n - 1$ ortogonálních latinských čtverců řádu n.

Důkaz. „$\Leftarrow$“: Dány ortogonální latinské čtverce $L_1, \ldots, L_{n-1}$.
Vytvoříme si body KPR: $X = \{r, s, L_1, \ldots, L_{n-1}, m_{1,1}, \ldots, m_{n,n}\}$. Dále vytvoříme přímky KPR čtyř typů:

1. $\{r, s, L_i, i \in [n]\}$
2. $\{r, m_{i,1}, \ldots, m_{i,n}\}$ pro $i \in [n]$
3. $\{s, m_{1,i}, \ldots, m_{n,i}\}$ pro $i \in [n]$
4. $\{L_i, m_{j,k} : (L_i)_{j,k} = \text{const}\}$

Stačí jen ověřit axiomy: Jako čtveřice bodů v obecné poloze může posloužit mj. $\{r, s, m_{11}, m_{22}\}$. Další axiomy rozborem případů: dlouhé, ale přímočaré - TODO.
„$\Rightarrow$“: Mám KPR, chci OLČ.
Zvolím si libovolnou přímku, její body si pojmenujeme (označíme) jako $r, L_1, \ldots, L_{n-1}, s$. Přímky procházející body r, s očíslujeme $1, \ldots, n/1, \ldots, n$. Zbývající body máme jednoznačně určené v mřížce. Pozice symbolů můžeme získat z přímek typu 4 jako v opačné implikaci. Zároveň ortogonalita těchto čtverců plyne z toho, že průsečík každých dvou symbolů existuje a je právě jeden. ⊞

Počet dvěma způsoby

Věta 10 (Počet hran grafu bez čtyřcyklu)**.** Graf na n vrcholech neobsahující podgraf C_4 má nejvýše $\frac{1}{2}(n^{3/2}+n)$ hran.

Důkaz. Dvěma způsoby určíme počet indukovaných cest délky 2 (vidliček) - označíme c_v.
1) $c_v \leq \binom{n}{2}$ - počet vidliček u, v, w je nejvýše počet dvojic (u, w) (z neexistence čtyřcyklu).
2) $c_v = \sum\limits_{w \in V(G)} \binom{\deg v}{2}$ - vezmeme každý potenciální prostřední vrchol a vezmeme všechny možné vidličky (dvojice výchozích hran)
Tedy

$$\sum_{w \in V(G)} \binom{\deg(w)}{2} \leq \binom{n}{2} \overset{\text{úpravy}}{\Rightarrow} \sum_{w \in V(G)} (\deg(w)-1)^2 \overset{(*)}{\leq} n^2$$

Použijeme Cauchy-Schwarzovu nerovnost ($\langle x, y\rangle \leq \|x\|\|y\|$) pro $x = (\deg(v_1)-1, \deg(v_2)-1, \ldots, \deg(v_n)-1)^T$ pro $V(G) = \{v_1, \ldots, v_n\}$ a $y = (1, 1, \ldots, 1)^T$.
Pak

$$\sqrt{n^2}\sqrt{n} \overset{(*)}{\geq} \sqrt{\sum_{w \in V(G)} (\deg(w)-1)^2} \cdot \sqrt{n} = \|x\|\|y\| \geq \langle x, y\rangle = \sum_{w \in V(G)} (\deg(w)-1) \cdot 1 = 2|E| - n$$

Tedy $2|E| - n \leq n^{3/2} \Rightarrow |E| \leq \frac{1}{2}(n^{3/2}+n)$. ⊞

Pozorování. Pro konečnou množinu X, $|X| = n$, má částečně uspořádaná množina $(2^X, \subseteq)$ antiřetězce velikosti $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Věta 11 (Spernerova)**.** Pro $|X| = n \in \mathbb{N}$ má částečně uspořádaná množina $(2^X, \subseteq)$ antiřetězce velikosti nejvýše $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Důkaz. Nechť $\mathcal{M} = \{M_1, \ldots, M_k\}$ je maximální antiřetězec. Dvěma způsoby spočteme počet dvojic (M, R), kde $M \in \mathcal{M}, R$ je řetězec a $M \in R$.
Zjevně $R := \emptyset \subseteq A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n = X, A_l \setminus A_{l-1} = \{x\}, x \in X$. Tedy permutace X jednoznačně určuje maximální řetězec.
1. $\#(M, R) \leq \#R = n!$ (Druhé složky musí být unikátní: $(M_1, R_1), (M_2, R_1) \Rightarrow M_1, M_2$ jsou porovnatelné.)
2. $\#(M, R) = \sum\limits_{M \in \mathcal{M}} |M|! \cdot (|X| - |M|)! = \sum\limits_{M \in \mathcal{M}} |M|! \cdot (n - |M|)!$.
Z toho plyne $\sum\limits_{M \in \mathcal{M}} |M|! \cdot (n-|M|)! \leq n! \Rightarrow \sum\limits_{M \in \mathcal{M}} \dfrac{|M|! \cdot (n-|M|)!}{n!} \leq 1 \Rightarrow \sum\limits_{M \in \mathcal{M}} \binom{n}{|M|}^{-1} \leq 1 \Rightarrow$
$\underset{\binom{n}{|M|}^{-1} \geq \binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1}}{\Rightarrow} \sum\limits_{M \in \mathcal{M}} \binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} \leq 1 \Rightarrow |\mathcal{M}| \binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} \leq 1 \Rightarrow |\mathcal{M}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ ⊞

Důsledek 4. Každý množinový systém na $|X| = n$ uspořádaný inkluzí má nejvýše $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ nezávislých prvků vzhledem k inkluzi.

Definice 7 (Kostra grafu)**.** Kostra grafu G je strom $T : V(T) = V(G), T \subseteq G$.
Počet koster grafu G značíme $\kappa(G)$, $\kappa(n) = \kappa(K_n)$.

Věta 12 (Cayleyho formule)**.** $\forall n \geq 2 : \kappa(n) = n^{n-2}$

Důkaz přes povykosy. Kostru si zakořeníme a její hrany očíslujeme $1, \ldots, n-1$, to odpovídá trojici (T, r, f) - strom, kořen, očíslování.
1. $\#(T, r, f) = \kappa(n) \cdot n \cdot (n-1)!$
2. $\#(T, r, f) = \prod\limits_{i=1}^{n-1} n \cdot (n-i) = n^{n-1} \cdot (n-1)!$
Tedy $n^{n-2} \cdot n! = \kappa(n) \cdot n! \Rightarrow \kappa(n) = n^{n-2}$ ⊞

Věta 13 (Počet koster podle skóre kostry)**.** Nechť $(d_1, \dots, d_n)$ je posloupnost čísel splňující $\forall i : d_i \geq$ $\wedge \sum d_i = 2n-2$. Potom koster K_n, pro něž platí $\forall i : \deg(v_i) = d_i$ je $\dfrac{(n-2)!}{(d_1-1)! \cdot \ldots \cdot (d_n-1)!}$.

Důkaz indukcí podle počtu vrcholů. Báze triviální
Indukční krok: bez újmy na obecnosti: $d_n = 1$ (v_n je nutně list). Rozebereme případy $(v_n, v_J) \in E$: koster na $n-1$ vrcholech se skóre $(d_1-1, \dots, d_{n-1})$ je z IP $\frac{(n-3)!}{(d_1-2)! \ldots (d_{n-1}-1)!}$. Analogicky pro všechny další hrany.
Pak pošet koster se stupni je $\displaystyle\sum_{i=1, d_i \neq 1}^{n-1} \frac{(n-3)!}{(d_1-1)! \cdot \ldots \cdot (d_i-2)! \ldots (d_{n-1}-1)!} =$

$$= \frac{(n-3)![d_1-1+d_2-1+\ldots+d_{n-1}-1]}{(d_1-1)! \cdot \ldots \cdot (d_{n-1}-1)!} = \frac{(n-3)!(n-2)}{(d_1-1)! \cdot \ldots \cdot (d_{n-1}-1)! \cdot (d_n-1)!} = \frac{(n-2)!}{(d_1-1)! \cdot \ldots \cdot (d_n-1)!}$$

⊞

Důsledek 5 (Cayleyho formule - II. důkaz)**.**

Důkaz. $\kappa(n) = \displaystyle\sum_{d_i \geq 1, \sum d_i = 2n-2} \frac{(n-2)!}{(d_1-1)! \cdot \ldots \cdot (d_n-1)!} \overset{k_i = d_i - 1}{=} \sum_{d_i \geq 1, \sum k_i = n-2} \frac{(n-2)!}{k_1! \cdot \ldots \cdot k_n!} \cdot 1^{k_1} \cdot 1^{k_2} \ldots \cdot 1^{k_n} \overset{\text{multinomická věta}}{=}$ $(1+1+\ldots+1)^{n-2} = n^{n-2}$ ⊞

Definice 8 (Multigraf, jeho kostra, kontrakce)**.** Multigraf je graf se smyčkami a násobnými hranami.
Kostra multigrafu je strom na $V(G)$ takový, že neobsahuje smyčky a z násobných hran vybíráme vždy nejvýše jednu.
Kontrakce hrany e v G je $G \circ e$: je-li $e = (u, v)$, sloučíme vrcholy u, v do nového vrcholu w: $N(w) := N(u) + N(v)$. Zde mohou vzniknout smyčky a násobné hrany.

Poznámka (Rekurence pro počet koster grafu)**.** $\kappa(G) = \kappa(G-e) + \kappa(G \circ e)$.

Pozorování. Pro každý multigraf H a každou hranu e různou od smyčky platí $\kappa(H) = \kappa(H-e) + \kappa(H \circ e)$.

Definice 9 (Laplaceova matice)**.** Laplaceova matice multigrafu H na vrcholech $V(H) = \{v_1, \dots, v_N\}$ je $L \in \mathbb{R}^{n \times n}$, kde $l_{i,i} :=$ # hran různých od smyček incidentních s v_i, pro $i \neq j : l_{i,j} :=$ # hran mezi v_i a v_j.

Pozorování. L je singulární (součet všech řádků je nulový vektor).

Pozorování. Pro Laplaceovu matici platí $\forall i, j \in [n] : |L^{i,i}| = |L^{j,j}|$.

Pozorování. TODO: pozorování o přičtení 1 na 1,1

Věta 14 (Počet koster)**.** Pro každý neprázdný multigraf H platí $\kappa(H) = \det(L(H)^{1,1})$.

Důkaz. Indukcí podle počtu hran. Je-li $|E(H)| = 0$, potom je graf jeden vrchol, pak $|L(H)^{1,1}| = 1$, nebo nezávislá množina, pak $|L(H)^{1,1}| = 0$.
V indukčním kroku: bez újmy na obecnosti: $(v_1, v_2) \in E(H)$ (jinak přeznačíme). Pak $L(H) = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} +$ $L(H-e) \Rightarrow L(H)^{1,1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + L(H-e)^{1,1} \Rightarrow |L(H)^{1,1}| = |(L(H)^{1,1})^{1,1}| + |L(H-e)^{1,1}| =$ $|L(H \circ e)^{1,1}| + |L(H-e)^{1,1}| \overset{\text{IP}}{=} \kappa(H \circ e) + \kappa(H-e) = \kappa(H)$. ⊞

Důsledek 6 (Cayleyho formule - III. důkaz)**.**

Důkaz. $\kappa(K_1) = \begin{vmatrix} n-1 & -1 & -1 \\ -1 & \ddots & -1 \\ -1 & -1 & n-1 \end{vmatrix} = n^{n-2}$ ⊞

Grafy

Definice 10 (Řezy a souvislosti)**.** Nechť $G = (V, E)$ je graf. Pak

- $S \subseteq V$ je vrcholový řez, pokud $G - S$ je nesouvislý
- $F \subseteq E$ je hranový řez, pokud $G - E$ je nesouvislý
- Vrcholová souvislost je $k_v = \begin{cases} \min |S| & \text{přes všechny vrcholové řezy pokud nějaké existují} \\ n-1 & \text{pro } K_n, n \geq 2 \\ 1 & \text{pro } K_1 \end{cases}$
- Hranová souvislost je $k_e = \begin{cases} \min |F| & \text{přes všechny hranové řezy} \\ 1 & \text{pro } K_1 \end{cases}$
- G je (vrcholově) t-souvislý, pokud $k_v \geq t$.
- G je hranově t-souvislý, pokud $k_e \geq t$.

Pozorování. $\forall G : G \neq K_1 : k_v, k_e \leq \min\limits_{v \in V(G)} \deg(v)$

Lemma 2. $\forall G = (V, E) : k_v(G) \leq k_e(G)$

Důkaz. Máme dán minimální F, tvoříme S.
Nechť C_1, C_2 jsou komponenty $G - F$. Pak:

1. existují $u, v : u \in C_1, v \in C_2, u, v \notin F$ - pak lze vzít vrcholy podle hran.
2. takové u, v neexistují, ale $u \in C_1, v \in C_2, (u, v) \notin F$ - pak dobře odebíráme.

   Jinak F indukuje $K_{m,n}$ - bez újmy na obecnosti $m \leq n$.
3. $m = 1$ - G je úplný, vše platí
4. $m \geq 2$ takový řez ovšem musí mít $m \cdot n$ hran, ovšem my umíme najít menší hranový řez, tedy F není minimální, což je spor.

$\boxplus$

Definice 11 (Artikulace, most)**.** Jednovrcholový řez je artikulace.
Jednohranový řez je most.

Věta 15 (Ušaté lemma)**.** G je 2-souvislý $\Leftrightarrow$ G lze vytvořit z C_k přidáváním uší, kde ucho je cesta mezi dvěma různými vrcholy.

Důkaz. „$\Leftarrow$“: indukcí - přidání ucha neporuší 2-souvislost: ať máme artikulaci - pokud je na uchu, pak to není artikulace, pokud není na uchu, byla tam už předtím.
„$\Rightarrow$“: Máme dán 2-souvislý G, najdu největší $H \subset G$, který lze z C_k vytvořit přidáváním uší. Pro spor předpokládejme $H \neq G$. Najdu si $(u, v) : u \notin H, v \in H, G - u$ souvislý. Do souseda w vrcholu u vede z H cesta - pak tato cesta + e je ucho, což je spor s maximalitou H. $\boxplus$

Poznámka (K ušatému lemmatu)**.** To je ekvivalentní tomu, že G lze vytvořit s C_3 pomocí přidání a podrozdělení hran.

Důsledek 7. G je 2-souvislý $\Leftrightarrow$ každé dva vrcholy leží na společné kružnici.

Důkaz. „$\Leftarrow$“: Má-li G artikulaci oddělující u, v, pak u, v neleží na společné kružnici - spor.
„$\Rightarrow$“: indukcí podle počtu uší. Báze je kružnice, to je zjevné.
Jinak vezmeme G najdeme ucho U a zvážíme $G - U$. Pokud $u, v \notin U$: z IP umíme najít kružnici bez ucha.
Pokud $u, v \in U$: graf byl i předtím souvislý - najdu cestu z x konce ucha do y druhého konce ucha mimo ucho - mám dvě cesty, tedy i kružnici.
Jinak bez újmy na obecnosti $u \in U, v \notin U$. Pak najdu cyklus (z IP) pro x a v a cestu z y do tohoto cyklu. Pak umím najít hledaný cyklus. ⊞

Definice 12 ((A,B)-řez)**.** O řezu $S \subseteq V(G)$ řekneme, že je (A, B)-řez, jestliže $A, B \subseteq V(G)$ a každá cesta $v \in A \to w \in B$ obsahuje vrchol z S.

Tvrzení 3 ((A,B)-řezy a disjunktní cesty)**.** Nechť $A, B \in V(G)$, kde $|A| = |B| = t$. Pokud G nemá žádný (A, B)-řez velikosti nejvýše $t - 1$, pak existuje t disjunktních cest mezi A a B.

Důkaz indukcí podle $|E(G)|$. Báze: $|E(G)| = 0 \Rightarrow E(G) = \emptyset$. Buď $A = B$, pak existuje t cest délky 0, nebo $A \neq B$, pak $A \cap B$ je (A, B)-řez velikosti $< t$, tedy nesplňujeme předpoklady a implikace platí.
IK: Zvolme $e \in E(G)$ libovolně. Uvažme $G - e$. Pokud $G - e$ nemá řez velikosti $\leq t - 1$, má z IP t cest a tedy máme hledané cesty i pro G.
Jinak má G (A, B)-řez velikosti $\leq t - 1$. Zpozorujeme, že každá $A \to B$ cesta (tj. cesta z $a \in A$ do $b \in B$) buď obsahuje vrchol z S nebo hranu e. Hranu e prochází cesty vždy ve stejném směru - bez újmy na obecnosti si ji označíme $A \to u \to v \to B$.
Označíme $S_u := S \cup \{u\}, S_v := S \cup \{v\}$. Z předchozího plyne, že S_u je (A, B)-řez v $G \Rightarrow |S_u| \geq t \Rightarrow |S_u| = t(|S| = t - 1)$, $|S_v|$ analogicky.
(1): G nemá žádný (A, S_u)-řez velikosti $\leq t-1$. Kdyby takový řez existoval, pak $\exists (A, B)$-řez velikosti $\leq t-1$, což je spor s předpoklady.
(2): $G - e$ nemá žádný (A, S_u)-řez velikosti $\leq t - 1$. Kdyby takový řez existoval, pak by v $G - e$ existovala cesta z A do S_u mimo řez.
$\overset{(1),(2),IP}{\Rightarrow} \exists\, t$ disjunktních cest z A do S_u a t disjunktních cest z S_v do B, z nichž umíme zkonstruovat t cest z A do B. ⊞

Věta 16 (Mengerova)**.** Pro každá graf G platí, že $\forall t > 0$: G je vrcholově t-souvislý $\Leftrightarrow$ mezi každými dvěma vrcholy existuje t vnitřně disjunktních cest.

Věta 17 (Ford-Fulkersonova)**.** Pro každá graf G platí, že $\forall t > 0$: G je hranově t-souvislý $\Leftrightarrow$ mezi každými dvěma vrcholy existuje t hranově disjunktních cest.

Důkaz. „$\Leftarrow$“ pro obě věty: existují cesty, tedy neexistují řezy velikosti $< t$ takové, aby přerušily T disjunktních cest, tedy graf je t-souvislý.
„$\Rightarrow$“ Mengerova věta: máme dány u, v. Pokud nesdílí hranu, vezmu $A \subseteq N(u) : |A| = t, B \subseteq N(v) : |B| = t$ - t jich lze vzít z t-souvislosti. Z předchozího tvrzení máme nalezeny cesty zadarmo.
Pokud $(u, v) \in E(G)$, hledám $t - 1$ cest v $G - e$ stejně jako výše. Stačí jen ukázat, že po odebrání jedná hrany neklesne vrcholová souvislost o více než 1, což je jednoduché pozorování.
„$\Rightarrow$“ Ford-Fulkersonova věta: převedeme hranovou na vrcholovou souvislost. Zkonstruujeme linegraf: pro dané $u, v \in V(G)$ přidáme listy $u', v' : (u', u), (v, v') \in E(G')$. Nyní vytvoříme linegraf $L(G') : V(L(G')) = E(G'), \forall e, e' \in V(L(G')) : (e, e') \in E(L(G')) \Leftrightarrow e \cap e' \neq \emptyset$ (v G).
Zpozorujeme, že $F \subseteq E(G)$ je hranový řez oddělující u, v právě když F je vrcholový řez linegrafu.
Protože G nemá malé ($\leq t - 1$) hranové řezy, $L(G')$ nemá malé vrcholové řezy $\Leftrightarrow \exists t$ vrcholově disjunktních cest v $L(G') \to \exists\, t$ hranově disjunktních cest v G. ⊞

Toky v sítích

Definice 13 (Síť, tok, velikost toku)**.** Síť je orientovaný graf s nezáporně ohodnocenými hranami a dvěma význačnými vrcholy s (stok) a z (zdroj). Formálně se jedná o čtveřici $(G, c, z, s) : z, s \in V(G), c : E(G) \to \mathbb{R}_0^+$, pak $c(e)$ je kapacita hrany.
Tok v síti (G, c, z, s) je zobrazení, které hranám přiřazuje nezáporné hodnoty nepřevyšující kapacity splňující tzv. 1. Kirchhoffův zákon. Formálně je tok $f : E(G) \to \mathbb{R}_0^+ : \forall e \in E(G) : 0 \leq f(e) \leq c(e) \wedge \forall v \in V(G) \setminus \{z, s\} :$

$\sum\limits_{u:(u,v)\in E(G)} f(u,v) = \sum\limits_{u:(v,u)\in E(G)} f(v,u)$.
Velikost toku f je $w(f) := \sum\limits_{v:(z,v)\in E(G)} f(z,v) = \sum\limits_{v:(v,z)\in E(G)} f(v,z)$.

Definice 14 (Řez v síti, kapacita řezu, elementární řez)**.** Řezem v síti (G, c, z, s) je $R \subseteq E(G)$ taková, že každá orientovaná cesta $z \to s$ obsahuje alespoň jednu hranu R.
Kapacita řezu R je $c(R) = \sum\limits_{e\in R} c(e)$.
Elementární řez je řez daný $A \subseteq V : z \in A, s \notin A$ tak, že $R_A = \{(u,v), u \in A, v \notin A\}$.

Pozorování. R_A je řez, protože každá cesta $z \to s$ alespoň jednou opustí A.

Pozorování. Každý řez R obsahuje nějaký elementární řez $R_A \subseteq R$.

Důkaz. R je řez, tedy $G \setminus R$ je nesouvislý, tedy A si zvolme komponentu $G \setminus R$ obsahující z. Pak máme hotovo. ⊞

Důsledek 8. Řezy minimální vzhledem k inkluzi jsou elementární.

Lemma 3. Je-li f tok v síti (G, c, z, s) a R_A je elementární řez, pak $w(f) = \sum\limits_{u\in A, v\notin A:(u,v)\in E(G)} f(u,v) - \sum\limits_{u\in A, v\notin A:(v,u)\in E(G)} f(v,u)$

Důkaz. $w(f) \overset{def}{=} \sum\limits_{v:(z,v)\in E(G)} f(z,v) = \sum\limits_{v:(v,z)\in E(G)} f(v,z)$. Dále $\forall u \in A : u \neq z : 0 = \sum\limits_{v:(u,v)\in E(G)} f(u,v) = \sum\limits_{v:(v,u)\in E(G)} f(v,u)$.

Sečtením těchto nerovností získáváme $w(f) = \sum\limits_{u\in A} \left[\sum\limits_{v:(u,v)\in E(G)} f(u,v) = \sum\limits_{v:(v,u)\in E(G)} f(v,u) \right] = \sum\limits_{(u,v)\in E, u,v\in A} [f(u,v) - f(u,v)] + \sum\limits_{(u,v)\in E, u\in A, v\notin A} f(u,v) - \sum\limits_{(v,u)\in E, u\in A, v\notin A} f(v,u) = \sum\limits_{u\in A, v\notin A:(u,v)\in E(G)} f(u,v) - \sum\limits_{u\in A, v\notin A:(v,u)\in E(G)} f(v,u)$ ⊞

Věta 18 (Minimaxová věta)**.** Pro každou síť platí, že velikost maximálního toku je rovna kapacitě minimálního řezu. Formálně: $\max\limits_f w(f) = \min\limits_R c(R)$.

Důkaz. Nejprve dokážeme nerovnost $\forall f, R$. Najdeme minimální $R' \subseteq R$ vzhledem k inkluzi. Z pozorování je R' elementární, tedy $R' = R_A$, z lemmatu $w(f) = \sum\limits_{u\in A, v\notin A:(u,v)\in E(G)} f(u,v) - \sum\limits_{u\in A, v\notin A:(v,u)\in E(G)} f(v,u) \leq \sum\limits_{u\in A, v\notin A:(u,v)\in E(G)} f(u,v) \leq \sum\limits_{u\in A, v\notin A:(u,v)\in E(G)} c(u,v) = c(R_A) \leq c(R)$.
Nyní ukážeme, že pokud existuje maximální tok, pak platí rovnost.

Definice 15 (Zlepšující cesta)**.** Pro cestu $P = (z = v_0, v_1, \ldots, v_k)$ definujeme hodnotu

$$\varepsilon_P = \min \begin{cases} c(v_i, v_{i+1}) - f(v_i, v_{i+1}) & \text{je-li } (v_i, v_{i+1}) \in E \\ f(v_{i+1}, v_i) & \text{je-li } (v_{i+1}, v_i) \in E \end{cases}$$

Pokud je $\varepsilon_P > 0$, pak P je zlepšující cesta.

Zpozorujeme, že pokud pro tok f existuje zlepšující cesta, není maximální, tedy jej lze zlepšit. (Případně lze rozebrat podrobněji.)
Z toho plyne, že když je f maximální, pak neexistuje žádná zlepšující cesta $z \to s$ (to je obměna pozorování).
Potom zvolíme $A := \{z\} \cup \{u \in V : \exists P : z \to u : \varepsilon_P > 0\}$, tedy $s \notin A$. Uvážíme elementární řez R_A : jeho hrany směrem ven musí mít využity veškerou kapacitu (kdyby ne, pak nemáme korektně zvolenou A) a $\forall (v,u) \in E : u \in A, v \notin A : f(v,u) = 0$ - ze stejného důvodu. Tedy $w(f) = c(R_A)$.
Jako poslední ukážeme existenci.
Pro celočíselné kapacity: $\varepsilon_P \in \mathbb{Z}_0^+$, tedy neexistuje nekonečná posloupnost zlepšujících cest.

Pro racionální kapacity: vynásobíme kapacity nejmenším společným násobkem jmenovatelů zlomků a převedeme na celočíselné kapacity.
Pro reálné kapacity: množina toků je kompaktní, velikost toku je spojitá funkce. Z analýzy: spojitá funkce na kompaktu nabývá maxima. ⊞

Systémy různých reprezentantů

Definice 16 (Množinový systém, SRR, incidenční graf)**.** Množinový systém je $\mathcal{M} = \{M_i : i \in I : M_i \subseteq X\}$, kde X, I jsou konečné množiny.
Systém různých reprezentantů pro $\mathcal{M}$ je zobrazení $f : I \to X : \forall i \in I : f(i) \in M_i \wedge f$ je prosté.
Incidentní graf pro $\mathcal{M}$ je bipartitní graf $G_{\mathcal{M}} = (V, E) : V = I \cup X, \forall i \in I, x \in X : (i, x) \in E \Leftrightarrow x \in M_i$.

Pozorování. $\mathcal{M}$ má systém různých reprezentantů $\Leftrightarrow G_{\mathcal{M}}$ má párování velikosti $|I|$, kde párování je množina navzájem disjunktních hran.

Věta 19 (Hallova)**.** $\mathcal{M}$ má systém různých reprezentantů $\Leftrightarrow \forall J \subseteq I, J \neq \emptyset : |J| \leq |\bigcup_{i \in J} M_i|$.

Důkaz. „$\Rightarrow$“: Zjevně můžu pro libovolnou $J \subseteq I$ najít $C \subseteq X : |C| = |J| \wedge \forall j \in J : \exists c \in C : c \in M_j$.
„$\Leftarrow$“: Doplníme $G_{\mathcal{M}}$ na síť tak, že přidáme $z : N(z) = I, s : N(s) = X$, orientace $z \to I \to X \to s$. Kapacity všech hran budou jednotkové.
Pak si najdeme minimální tok f a odpovídající minimální řez R.
Protože kapacity jsou celočíselné, pak $\exists$ maximální tok f s celočíselnými hranami.
Dále se podíváme na řez: libovolná cesta $z \to s$ vypadá $z - i \in I - x \in X - s$. Pokud by v řezu R byla hrana (i, x), pak lze řez upravit tak, aby (i, x) neobsahoval s pomocí jedné z hran $(z, i), (x, s)$ a zároveň tím můžu potenciálně odebrat více hran řezu. Tedy bez újmy na obecnosti R obsahuje pouze hrany výchozí ze zdroje, nebo přicházející do stoku.
Pak zvolme $A = \{i \in I : (z, i) \in R\}, B = \{x \in X : (x, s) \in R\}$.
Protože R je řez, pak neexistuje $(i, x) \in E(G) : i \in I \setminus A, x \in X \setminus B$.
Z toho plyne $\bigcup_{i \in I \setminus A} M_i \subseteq B \Rightarrow |\bigcup_{i \in I \setminus A} M_i| \leq |B|$. Z Hallovy podmínky dále plyne $|\bigcup_{i \in I \setminus A} M_i| \geq |I \setminus A|$. Dále $w(f) = |R| \cdot 1 = |A| + |B| \geq |A| + |I \setminus A| = |I|$, což je i horní omezení, jelikož existuje řez přes všechna $(z, i) \in E(G)$, jichž je $|I|$.
Tedy $w(f) = |I|$, a f je celočíselný, tedy hrany jsou ohodnoceny 1,0, tedy hrany použité v toku mezi I a X určují hledané párování. ⊞

Definice 17 (Vrcholové pokrytí)**.** Množina $C \subseteq V(G)$ je vrcholové pokrytí G, pokud $\forall e \in E(G) : e \cap C \neq \emptyset$.

Pozorování. Z Dk Hallovy věty: $A \cup B$ je vrcholové pokrytí incidenčního grafu $G_{\mathcal{M}}$.

Důsledek 9 (Königova věta)**.** V každém bipartitním grafu je velikost maximálního párování rovna velikosti nejmenšího vrcholového pokrytí.

Důsledek 10 (Obarvitelnost k-regulárního bipartitního grafu k barvami)**.** Každý k-regulární bipartitní graf je hranově k-obarvitelný, tj. hrany lze obarvit k barvami tak, že z každého vrcholu vycházejí různé barvy.

Důkaz. Indukcí podle k.
$k = 1$: Triviálně perfektní párování.
$k \geq 2$: označme si jednu partitu I, druhou X. Zadefinujeme $\mathcal{M} : M_i = N(i)$. Pak ověříme Hallovu podmínku: mějme $J \subseteq I$. Spočteme hrany vycházející z J: $k \cdot |J| = \#$ hran $\leq k \cdot |\bigcup_{i \in J} M_i| \Rightarrow |J| \leq |\bigcup_{i \in J} M_i|$, tedy Hallova podmínka platí, tedy $\mathcal{M}$ má systém různých reprezentantů. Tedy $G_{\mathcal{M}}$ má párování velikosti $|I|$. Pak párování můžu odebrat, tedy mám $(k-1)$-regulární bipartitní graf. Z indukčního předpokladu umím obarvit zbytek $k - 1$ barvami, navíc odebrané hrany obarvíme další barvou, tedy celkem lze graf obarvit k barvami. ⊞

Definice 18 (Latinský obdélník)**.** Latinský obdélník typu $k \times n, k \leq n$ je tabulka velikosti $k \times n$ vyplněná n různými symboly tak, že se v žádném řádku ani sloupci symboly neopakují.

Věta 20. Každý latinský obdélník lze doplnit na čtverec.

Důkaz. Vytvoříme bipartitní graf mezi $I = [n]$ - sloupci a $X = [n]$ takový, že $(i, x) \in E \Rightarrow x$ lze doplnit do i-tého sloupce.
Tento graf je $(n - k)$-regulární, tedy jej lze obarvit hranově pomocí $n - k$ barev, tedy máme $n - k$ párování, což je $n - k$ řádků. $\boxplus$

Definice 19 (Bistochastická a permutační matice)**.** Matice $A \in [0, 1]^{n\times n}$ je bistochastická, pokud má řádkové i sloupcové součty rovny jedné.
Matice $A \in \{0, 1\}^{n\times n}$ je permutační, pokud má řádkové i sloupcové součty rovny jedné.

Definice 20 (Konvexní obal)**.** Konvexní obal je množina všech konvexních kombinací, tedy $\{\sum_{i=1}^{n} \alpha_i x_i : \sum \alpha_i = 1 \wedge \alpha_i \geq 0 \, \forall i \in [n]\}$

Věta 21 (Birkhoff-von Neumannova)**.** Bistochastické matice tvoří konvexní obal permutačních matic (obojí stejného řádu).

Lemma 4 (O nezáporném výběru z nezáporné matice)**.** Má-li matice $A \in (\mathbb{R}_0^+)^{n\times n}$ řádkové nebo sloupcové součty stejné, pak $\exists \pi \in S_n : \forall i \in [n] : a_{i,\pi(i)} > 0$.

Důkaz lemmatu. Sestavíme $\mathcal{M}$ na $I = X = [n]$ takový, že $M_i = \{j : a_{i,j} > 0\}$. Pak $\forall J \subseteq I : \sum_{(i,j)\in E, i\in J} a_{i,j} = |J| \cdot s$. Ovšem také $\sum_{(i,j)\in E, i\in J} a_{i,j} \leq \sum_{(i',j')\in E, j\in \bigcup_{i\in J} M_i} = |\bigcup_{i\in J} M_i| \cdot s$.
Z těchto dvou (ne)rovností plyne $|J| \leq |\bigcup_{i\in J} M_i|$, tedy platí Hallova podmínka, tedy $G_{\mathcal{M}}$ má párování, které odpovídá permutaci π. $\boxplus$

Důkaz Birkhoff-von Neumannovy věty pomocí silnějšího tvrzení. Dokážeme, že pokud jsou řádkové nebo sloupcové součty nezáporné matice A rovny s, pak $A = \sum \alpha_i A_{\pi_i} : \sum \alpha_i = s, \alpha_i > 0$.
Budeme indukovat podle t - počtu nenulových prvků.
Jestliže $t = n$, pak se jedná o s-násobek permutační matice, tedy triviálně vezmeme permutaci danou touto maticí: $A = s \cdot A_\pi$.
Dále bude $t > n$. Pak z lemmatu najdu $\pi \in S_n, \alpha := \min_{i\in[n]} a_{i,\pi(i)}, \alpha > 0$. Pak z IP (alespoň jeden prvek jsme odečtením odebrali) $A - \alpha A_\pi = \sum \alpha_i A_{\pi_i}, \sum \alpha_i = s - \alpha$, tedy $A = \sum \alpha_i A_{\pi_i} + \alpha A_\pi, \sum \alpha_i + \alpha = s$ a tedy máme hledaný s-násobek konvexní kombinace. $\boxplus$

Definice 21 (Ramseyovo číslo)**.** Ramseyovo číslo $R(k, l)$ je nejmenší $n \in \mathbb{N}$ takové, že každý graf na n vrcholech splňuje buď $\alpha(G) \geq k \vee \omega(G) \geq l$, kde $\alpha(G)$ je velikost největší nezávislé množiny jako indukovaného podgrafu a $\omega(G)$ je velikost největší kliky.
Ekvivalentně můžeme uvažovat o barvení hran dvěma barvami.
$R(k, 1) = R(1, l) = 1$

Tvrzení 4 (Konečnost Ramseyova čísla)**.** $R(k, l) \leq R(k - 1, l) + R(k, l - 1)$

Důkaz. Je dán G na $R(k - 1, l) + R(k, l - 1)$ vrcholech. Pak zvolím u libovolně a označím $A := N(u), B := V(G) \setminus N[u]$ $(N[u] = N(u) \cup \{u\})$. Pak buď $|A| \geq R(k, l - 1)$ (případ 1) nebo $|B| \geq R(k - 1, l)$ (případ 2). Rozebereme jednotlivé případy:

1. Nyní $G|_A$ (graf G zúžený na A) buď obsahuje nezávislou množinu velikosti k nebo úplný podgraf velikosti $l - 1$, který rozšíříme o u na K_l.

2. Graf $G|_B$ obsahuje úplný podgraf velikosti l nebo nezávislou množinu velikosti $k - 1$. Pak ji doplníme o u na I_k.

$\boxplus$

Důsledek 11 (Horní odhad Ramseyova čísla pomocí kombinačního čísla)**.** $R(k, l) \leq \binom{k+l-2}{k-1}$

Důkaz indukcí. $R(k,1) = R(1,l) = 1$
$R(k,l) \leq R(k-1,l) + R(k,l-1) \overset{\text{IP}}{\leq} \binom{k+l-3}{k-2} + \binom{k+l-3}{k-2} = \binom{k+l-2}{k-1}$ ⊞

Věta 22 (Ramseyova věta pro grafy a r barev)**.** Pro každé $k, r \in \mathbb{N} \exists n \in \mathbb{N}$ takové, že barvíme-li hrany K_n pomocí r barev, potom vždy nalezneme k-tici vrcholů, které indukují jednobarevný úplný podgraf (K_k). Nejmenší takové n budeme značit $n_{r,k}$.

Důkaz indukcí podle r. Báze: $r = 1 : n_1, k = k$
IK: $r-1 \to r$: $n_{r,k} \leq R(k, n_{r-1,k})$. Pak $K_{R(k,n_{r-1,k})}$ obsahuje buď K_k v první barvě nebo $K_{n_{r-1,k}}$ v ostatních barvách (tj. všech kromě první) - a tento graf obsahuje z IP K_k v některé z $r-1$ barev. ⊞

Věta 23 (Ramseyova věta pro systémy p-tic)**.** Pro každé $r, p, k \in \mathbb{N} \exists n \in \mathbb{N}$ takové, že barvíme-li $\binom{[n]}{p}$ pomocí r barev, potom existuje $A \subseteq [n], |A| = k$ taková, že $\binom{A}{p}$ je jednobarevná.

Důkaz indukcí podle p. Báze: pro $p = 1$ se jedná o Dirichletův princip, pro $p = 2$ o Ramseyovu větu pro grafy.
Dále budeme nejmenší n značit jako $n_{r,p}(k)$.

Lemma 5. Pro každé obarvení p-tic množiny B velikosti $1 + n_{r,p-1}(k)$ a libovolný prvek $x \in B$ existuje $B' \subseteq B \setminus \{x\}$ taková, že $|B'| \geq k$ a všechny p-tice z $\binom{B'}{p}$ mají stejnou barvu.

Důkaz lemmatu. Mějme dáno obarvení $c : \binom{B}{p} \to [r]$. Definujeme $c' : \binom{B\setminus\{x\}}{p-1} \to [r]$ tak, že $c'(Y) := c(Y \cup \{x\}), Y \in \binom{B\setminus\{x\}}{p-1}$. Protože $|B \setminus \{x\}| = n_{r,p-1}(k)$, obsahuje hledanou monochromatickou B' z IP. ⊞

Nyní ukážeme, že $n_{r,p}(k) \leq 1 + n_{r,p-1}(1 + n_{r,p-1}(1 + n_{r,p-1}(\ldots + n_{r,p-1}(p-1)\ldots))) =: n *_{r,p} (k)$, přičemž vnořujeme $t = r(k-p) + 1$-krát.
Nyní vezmeme $B_0 := [n *_{r,p} (k)]$. To umíme spočíst, protože všude ve vzorečku používáme jen $p-1$. Mějme dané obarvení $c : \binom{B_0}{p} \to [r]$. Budeme t-krát aplikovat lemma, čímž tvoříme posloupnost $x_1, \ldots, x_t : x_i \in B_{i-1}, B_i = (B_{i-1})'$.
Z rekurence plyne $|B_t| \geq n_{r,p-1}(p-1) = p-1$. Bez újmy na obecnosti nechť $|B_t| = p-1$. K posloupnosti prvků $x_1, \ldots, x_t$ přidáme posloupnost barev $b_1, \ldots, b_t$, kde b_i je „barva vějířku určená x_i“, neboli barva $\binom{B_i}{p-1}$.
V posloupnosti $b_1, \ldots, b_t$ se z Dirichletova principu některá z barev zopakuje alespoň $(k-p+1)$-krát. Prvky x_i odpovídající této barvě nechť tvoří $C = \{x_{i_1}, \ldots, x_{i_{k-p+1}}, \ldots\}$. Potom hledaná $A := B_t \cup C$, jelikož každá p-tice obsahuje prvek z C, tedy má stejnou barvu b. ⊞

Věta 24 (Erdös-Szekeresova)**.** Pro každé k existuje n takové, že pro každou libovolnou n-prvkovou množinu bodů v $\mathbb{R}^2$ v obecné poloze nalezneme k-prvkovou podmnožinu bodů v konvexní poloze (tj. vrcholy konvexního k-úhelníku)

Důkaz. Zpozorujeme, že libovolná pětice bodů tvoří konvexní čtyřúhelník. Buď je přímo konvexní obal, nebo je konvexní obal trojúhelník - pak jsou dva body uvnitř trojúhelníku - ty tvoří přímku, která dělí $\mathbb{R}^2$ na dvě části. Vezmeme dva body, které jsou ve stejné části - ty pak s dvěma vnitřními tvoří konvexní čtyřúhelník.
Zvolíme $n = n_{2,4}(k)$, tedy barvíme čtveřice dvěma barvami. Červeně obarvím takovou čtveřici, která je v konvexní poloze a modře takovou, která v konvexní poloze není.
Z pozorování ovšem plyne, že nemůžeme najít velkou monochromatickou modrou podmnožinu - pokud má alespoň 5 bodů, pak v ní najdeme konvexní čtyřúhelník. Tedy nacházím monochromatickou červenou podmnožinu o velikosti alespoň k. Ta vytvoří ze své monochromatičnosti konvexní k-úhelník. ⊞

Tvrzení 5 (Odhady Ramseyova čísla)**.** Pro $k \geq 3$ $\sqrt{2}^k \leq R(k,k) \leq \binom{2k-2}{k-1} \leq 4^k$

Důkaz. Horní odhad máme už dokázaný, dokážeme jen dolní odhad.
Zvolíme náhodný graf na $\sqrt{2}^k$ vrcholech s $p = \frac{1}{2}$. Pek vezmeme $K \subseteq V : |K| = k$. Dále uvažme jevy A_K: $G|_K$ je klika, B_K: $G|_K$ je nezávislá množina. $p(A_K) = p(B_K) = 2^{-\binom{k}{2}}$.
Pak $p(\omega(G) \geq k \vee \alpha(G) \geq k) \leq \sum_K p(A_K) + p(B_K) = \binom{\sqrt{2}^k}{k} \cdot 2^{-\binom{k}{2}} \cdot 2 \overset{k\geq 3}{<} \frac{(\sqrt{2}^k)^k \cdot 2^{1-\binom{k}{2}}}{2^{\frac{k}{2}+1}} = 2^0 = 1.$ ⊞

Samoopravné kódy

Definice 22 (Terminologie samoopravných kódů, Hammingova vzdálenost, blokový kód)**.** Abeceda Σ je konečná množiny tzv. symbolů.
Slova jsou uspořádané n-tice symbolů.
Množina všech slov délky n se značí Σ^n.
Hammingova vzdálenost pro slova $x, y \in \Sigma^n$ je $\mathrm{dist}(x, y) := |\{i \in [n] : x_i \neq y_i\}|$ (navíc se jedná o metriku)
Blokový kód je $C \subseteq \Sigma^n$. Parametry kódu jsou $(n, k, d)_q$, kde n je délka kódu, k je dimenze kódu ($k = log_q|C|$), d je minimální vzdálenost kódu, q je velikost abecedy.

Pozorování. Kód se vzdáleností d je schopen opravit $\lfloor \frac{d-1}{2} \rfloor$ chyb.

Pozorování. Zpermutování pozic nebo symbolů na dané pozici nemění parametry kódu.

Definice 23 (Ekvivalence kódů, kombinatorická koule)**.** Kódy C, D jsou ekvivalentní, pokud $\exists \pi \in S_n : x \in C \to \pi(x) \in D$.
Kombinatorická koule se středem x a poloměrem t je $B(x, t) := \{y \text{ slovo} : \mathrm{dist}(x, y) \leq t\}$.

Pozorování (Prázdný průnik kombinatorických koulí)**.** $B(x, t) \cap B(y, t) = \emptyset \Leftrightarrow \mathrm{dist}(x, y) \geq 2t + 1$.

Pozorování (Disjunktní koule pro kód s danou vzdáleností)**.** Je-li C kód se vzdáleností d, potom $B(x, \lfloor \frac{d-1}{2} \rfloor)$ jsou navzájem disjunktní (pro x slova kódu).

Pozorování (Objem kombinatorické koule)**.** Objem kombinatorické koule je $V(t) := |B(x, t)| = \sum\limits_{i=0}^{k} \binom{n}{i}(q - 1)^i$.

Důsledek 12 (Hammingův odhad)**.** Je-li C kód opravující t chyb délky n nad $|\Sigma| = q$, potom $|C| \leq \frac{q^n}{V(t)}$

Poznámka. Kódy splňující rovnost Hammingova odhadu se nazývají perfektní.

Věta 25 (Gilbert-Varshamova mez)**.** $\forall n, d, q \exists (n, k, d)_q$ kód velikost $|C| > \frac{q^k}{V(d-1)}$

Důkaz. Budeme kód konstruovat hladově - náhodně bereme nějaké slovo a znemožníme si vzít jiné slovo z jeho okolí. Tím si zakážeme vždy nejvýše $V(d-1)$ dalších slov. $\boxplus$

Definice 24 (Lineární kód)**.** Nechť $\mathbb{T}$ je konečné těleso. Pak lineární kód je podprostor $\mathbb{T}^n$, $\Sigma = \mathbb{T}$ a slova jsou vektory. Takový kód značíme $[n, k, d]_q$. Víme $|\mathbb{T}| = \Sigma| = q \Rightarrow |C| = q^k$ (z toho, že C je podprostor).

Pozorování. $\forall x, y, z \in \mathbb{T}^n : \mathrm{dist}(x, y) = \mathrm{dist}(x + z, y + z) \stackrel{z=-y}{=} \mathrm{dist}(x - y, 0)$. Z toho plyne $D := \min\limits_{x \neq y \in C} \mathrm{dist}(x, y) = \min\limits_{x \neq y \in C} \mathrm{dist}(x - y, 0) \stackrel{C \text{ vekt. prostor}}{=} \min\limits_{x \in C} \mathrm{dist}(x, 0)$.

Definice 25 (Syndrom)**.** Pro lineární kód $C \Subset \mathbb{T}^n$ je syndrom lineární zobrazení $\mathbb{T}^n \to \mathbb{T}^{n-k}$, kde $k = \dim C$ takové, že $s(x) = 0 \Leftrightarrow x \in C$, tedy $X = \mathrm{Ker}(s)$.

Lemma 6 (O prostotě syndromu)**.** s je prosté na $B(0, t)$, pokud C má parametry $[n, k, 2t + 1]_q$.

Důkaz sporem. Nechť existují $y \neq y' \in B(0, t) : s(y) = s(y')$. Pak z linearity s: $0 = s(y) - s(y') = s(y - y') \stackrel{\text{def}}{\Rightarrow} y - y' \in C$. Protože $\forall 0 \neq x \in C : \mathrm{dist}(x, 0) \geq 2t - 1 \Rightarrow \mathrm{dist}(y - y', 0) \geq 2t - 1$, ale $\mathrm{dist}(y - y', 0) \stackrel{\triangle \text{ ner.}}{\leq} \mathrm{dist}(y, 0) + \mathrm{dist}(y', 0) \leq 2t \Rightarrow \lightning$ $\boxplus$

Tvrzení 6 (Určení x pro dané y)**.** Pokud y je přijaté slovo v lineárním kódu se syndromem s, pak se dekóduje na $x = y - s^{<-1>}(s(y))$.

Důkaz. 1. Pro $y \in B(x, t) : s(y - x) = s(y) - s(x) = s(y)$, jelikož $s(x) = 0$.
2. Pro $y \in B(x, t) : y - x \in B(0, t) \Rightarrow s^{<-1>}(s(y - x)) = y - x$.
3. $x = y - (y - x) \stackrel{2}{=} y - s^{<-1>}(s(y - x)) \stackrel{1}{=} y - s^{<-1>}(s(y))$. $\boxplus$

Definice 26 (Generující matice)**.** Generující matice kódu C má za řádky bázi C. Tedy je-li C dimenze k, pak tato matice $\in \mathbb{T}^{k\times n}$.

Důsledek 13 (O ekvivalentním kódu s generující maticí tvaru $(I|B)$)**.** Pro každý kód C existuje ekvivalentní kód takový, že jeho generující matice má tvar $(I_k|B)$. Takový tvar nazýváme standardní formou generující matice.

Důkaz. Gaussova eliminace zachovává bázi, dále můžeme přepermutovat sloupce, aby to vyšlo (máme zaručeno rank(gen. matice) $= k$ z bázovitosti). ⊞

Poznámka (Použití generujících matic pro kódování)**.** Chceme pro zprávu $z \in \mathbb{T}^k$ nějaké zakódování do C, tedy bijekci $\mathbb{T}^k$ a C.
Zprávu z zakódujeme jako $A^T z$, kde A je generující matice kódu. Zjevně $A^T z \in \mathcal{S}(A^T) = \mathcal{R}(A) = C$.
Dále syndrom s s maticí S musí splňovat $s : \mathbb{T}^n \to \mathbb{T}^{n-k}, S \in \mathbb{T}^{n-k\times n}$, $\text{rank}(S) = n-k, \forall x \in C : s(x) = Sx = 0$.
Možná volba $S = (-B^T|I_{n-k})$, potom $SA^T = -B^T I_k + I_k B^T = B^T - B^T = 0$.

Definice 27 (Duální kód a kontrolní matice)**.**
Duální kód k lineárnímu kódu C je $C^\perp := \{y : y^T x = 0 \forall x \in C\}$.
Kontrolní matice kódu C je generující matice duálního kódu $C^\perp$.

Poznámka (Shrnutí kódů a vysvětlení kontrolní matice)**.** Je-li $A = (I_k|B)$ generující matice C, pak $A^\perp = (-B^T|I_{n-k})$ je kontrolní matice.
Zároveň tato matice se nazývá kontrolní, jelikož $x \in C \Leftrightarrow A^\perp x = 0$

Tvrzení 7. Je-li $A^\perp$ kontrolní matice lineárního kódu C, pak d je minimální počet lineárně závislých sloupců $A^\top$

Důkaz. $d = \min \#$ nenulových symbolů $x \in C, x \neq 0$. $x \in C \Leftrightarrow A^\perp x = 0$, sloupce $A^\perp$ vybrané nenulovými složkami x jsou lineárně závislé. ⊞

Seznam témat