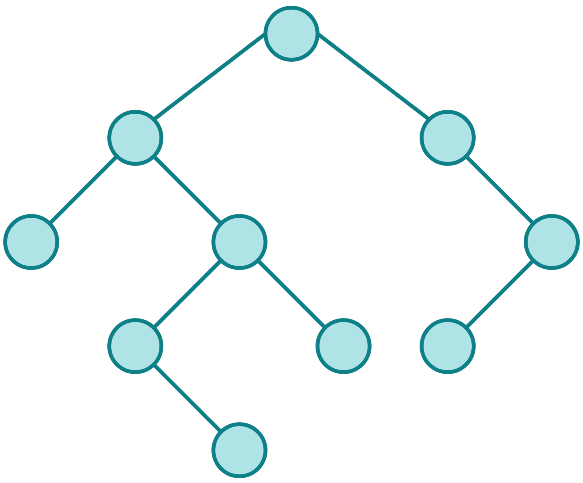
Kombinatorika a grafy

Tomáš Turek



October 21, 2023

Contents

Kombinatorika a grafy I

Většina důkazů zatím chybí.

1. Odhady

1.1 Odhady faktoriálu

Faktoriál: $n \in \mathbb{N} : n!$. Poskládání n prvků.

Tvrzení 1. $\forall n \in \mathbb{N} : n^{n/2} \le n! \le n^n$

Důkaz. Horní odhad se dá napsat jako: $n! = \prod_{i=1}^{n} i \le \prod_{i=1}^{n} n = n^n$. Dolní odhad použijeme, že $i(n+1-i) \ge n$ (to platí pro $i = 1$ a $i = n$). Potom pro $2 \le i \le \lceil \frac{n}{2} \rceil$ máme $i(n+1-i) \ge 2\frac{n}{2} = n$. Obdobný odhad je i pro $\lceil \frac{n}{2} \rceil \le i \le n$. Následně $(n!)^2 = n1 \cdot n2 \ldots 2(n-1) \cdot 1n \ge n^n$. Potom platí, že $n! \ge n^{n/2}$.

□

Věta 2. $\forall n \in \mathbb{N} : e(\frac{n}{e})^n \le n! \le en(\frac{n}{e})^n$

Důkaz. Horní odhad: Pro $n = 1$ platí $(1 = 1! \le e1\left(\frac{1}{e}\right)^1 = 1)$. Nechť $n \ge 2$.

$$n! = n(n-1)! \le ne(n-1)\left(\frac{n-1}{e}\right)^{n-1} = en\left(\frac{n}{e}\right)^n e\left(\frac{n-1}{n}\right)^n - \left(\frac{n-1}{n}\right)^n =$$

$$= e\left(1 - \frac{1}{n}\right)^n \le e\left(e^{\frac{-1}{n}}\right)^n = 1$$

Dolní odhad: Pro $n = 1$ platí $(1 = \left(\frac{1}{n}\right)^1 \le 1! = 1)$. Nechť $n \ge 2$.

$$n! = n(n-1)! \ge ne\left(\frac{n-1}{e}\right)^{n-1} = e\left(\frac{n}{e}\right)^n e\left(\frac{n-1}{n}\right)^{n-1} - \left(\frac{n-1}{n}\right)^{n-1} \ge 1$$

$$\Updownarrow$$

$$\frac{1}{e}\left(\frac{n}{n-1}\right)^{n-1} \le 1$$

$$\frac{1}{e}\left(\frac{n}{n-1}\right)^{n-1} = \frac{1}{e}\left(1 + \frac{1}{n-1}\right)^{n-1} \le \frac{1}{e}\left(e^{\frac{1}{n-1}}\right)^{n-1}$$

□

Lemma 3. $1 + x \le e^x$

Důkaz. $f(x) := e^x - (x+1)$ chceme ukázat, že $f(x) \ge 0$ pro $\forall x \in \mathbb{R}$. $f'(x) = e^x - 1 \Rightarrow (f'(x) = 0 \Leftrightarrow x = 0)$. $f''(x) = e^x$. $f''(x) = 1 > 0 \Rightarrow$ v bodě $x = 0$ je globální minimum pro $f \Rightarrow f(x) \ge 0$ pro $\forall x \in \mathbb{R}$.

□

Věta 4 (Stirlingův vzorec)**.** $n! \approx n\sqrt{2\pi n}(\frac{n}{e})^n$ $\lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}(\frac{n}{e})^n} = 1$

1.2 Binomický koeficient

Počet k-prvkových podmnožin n-prvkových množin:

$$n,k \in \mathbb{N} : \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Pozorování. *1.* $\forall n,k \in \mathbb{N} : (\frac{n}{k})^k \leq \binom{n}{k} \leq n^k$

2. největší prvek $\binom{n}{\lceil \frac{n}{2} \rceil} = \binom{n}{\lfloor \frac{n}{k} \rfloor}$

Důkaz. Empty.

□

1.2.1 Binomická věta

$$\frac{2^{2m}}{2m+1} \leq \binom{2m}{m} \leq 2^{2m}$$

Věta 5. $\forall m \in \mathbb{N} : \frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$

Užití Stirlingového vzorce: $\binom{2m}{m} \approx \frac{2^{2m}}{\sqrt{\pi m}}$. $\forall k,n \in \mathbb{N} : n > k, \binom{n}{k} \leq (\frac{en}{k})^k$.

Důkaz. Empty.

□

1.2.2 Aplikace (náhodné procházky)

n kroků a v každém bodě mám 50% že půjdu doprava anebo doleva. Střední hodnota počtu návratů do 0. X - počet návratů do 0. A_{2n} = jev po $2n$ krocích se dostanu do 0. $X = \sum_{n=1}^{\infty} I_{A_{2n}}$. $\Pr[A_{2n}] = \frac{\binom{2n}{n}}{2^2 n}$.

$$\mathbb{E}[X] = \mathbb{E}[\sum_{n=1}^{\infty} I_{A_{2n}}] = \sum_{n=1}^{\infty} \mathbb{E}[I_{A_{2n}}] =$$

$$= \sum_{n=1}^{\infty} Pr[I_{A_{2n}}] = \sum_{n=1}^{\infty} \frac{\binom{2n}{n}}{2^2 n} \geq \sum_{n=1}^{\infty} \frac{1}{2\sqrt{n}} = \infty$$

2. Vytvořující funkce

Početní metoda, kde spojitými funkcemi vyjadřujeme posloupnosti.

Definice 1. *Pro posloupnost* $(a_i)_{i=0}^{\infty}$ *je mocninnou řadou* $a(x) = \sum_{i=0}^{\infty} a_i x^i$.

Posloupnost lze převést na funkci, ale při převodu nazpátek je třeba aby posloupnost nerostal moc rychle.

Příklad.

1. $a_i = 1$ pokud $0 \leq i \leq n$ jinak $a_i = 0$. Tedy $(a_i)_{i=0}^{\infty} = (1, \dots, 1, 0, 0, \dots)$. Potom funkce je $\frac{1-x^{n+1}}{1-x}$ z geometrické řady.
2. $\forall i : a_i = 1$ to je potom nekonečná geometrická řada, takže je to $\frac{1}{1-x}$.
3. $a_i = \binom{n}{i}$ potom funkce vychází z binomické věty, takže je $(1+x)^n$.

Tvrzení 6. *Pokud pro* $(a_i)_{i=0}^{\infty} \exists k \in (R)$ *takové, že* $\forall i : |a_i| \leq k^i$*, pak pro všechna* $x \in (\frac{-1}{k}, \frac{1}{k})$ *řada* $a(x) = \sum_{i=0}^{\infty} a_i x^i$ *konverguje absolutně a na libovolném* ϵ *okolí 0 určuje i* $koeficienty_a$*, protože* $i_a = \frac{a^{(i)}(0)}{i!}$.

Obecný postup:

1. kombinatorický objekt s neznámým počtem
2. vytvořující funkce
3. rozklad na vytvořující funkce se známými koeficienty
4. určení hodnoty

Operace	Posloupnosti	Funkce
Součet	$(a_0 + b_0, a_1 + b_1, \dots)$	$(a+b)(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$
α-násobek	$(\alpha a_0, \alpha a_1, \dots)$	$\alpha a(x) = \sum_{i=0}^{\infty} (\alpha a_i) x^i$
Posun vpravo o n pozic	$(0, 0, \dots, a_0, a_1, \dots)$	$x^n a(x) \sum_{i=0}^{\infty} a_i x^{i+n}$
Posun vlevo o n pozic	$(a_n, a_{n+1}, dots)$	$\sum_{i=0}^{\infty} (a_{i+n} x^i = \frac{a(x) - \sum_{i=0}^{\infty} a_i x^i}{x^n}$
Dosazení αx	$(a_0, \alpha a_1, \alpha^2 a_2, \dots)$	$a(\alpha x) = \sum_{i=0}^{\infty} a_i + \alpha^i x^i$
Dosazení x^n	$(a_0, 0, \dots, 0, a_1, 0, \dots)$	$a(x^n) = \sum_{i=0}^{\infty} a_i x^n i$
Derivace	$(a_1, 2a_2, 3a_3, \dots)$	$a'(x) = \sum_{i=1}^{\infty} i a_i x^{i-1}$
Integrál	$(0, a_0, \frac{a_1}{2}, \frac{a_2}{3}, \dots)$	$\int_0^x a(x) \mathtt{d}x = \sum_{i=0}^{\infty} \frac{a_i}{i+1} x^{i+1}$
Součin	$(c_0, c_1, c_2, \dots)$	$a(x)b(x) = \sum_{i=0}^{\infty} (c_i) x^i$

2.1 Řešení rekurentních rovnic

Ukázka na Fibonacciho čísle. Určíme F_n jako koeficient funkce $F(x) = \sum_{i=0}^{\infty} F_i x^i$. Máme $F_{n+2} = F_{n+1} + F_n, \forall n \geq 0$. **Vynásobíme rovnici** x^n**:** $F_{n+2} x^n = F_{n+1} x^n + F_n x^n$.**Sčítáme přes** $n \geq 0$**:** $\sum_{n \geq 0} F_{n+2} x^n = \sum_{n \geq 0} F_{n+1} x^n + \sum_{n \geq 0} F_n x^n$ to se rovná:

$$\frac{F(x) - F_0 - F_1}{x^2} = \frac{F(x) - F_0}{x} + F(x)$$

teď určíme

$$F(x) = \frac{x}{1-x-x^2} = \frac{x}{(1-\frac{1+\sqrt{5}}{2}x)(1-\frac{1-\sqrt{5}}{2}} = \frac{\frac{1}{\sqrt{5}}}{1-\frac{1+\sqrt{5}}{2}x} - \frac{\frac{1}{\sqrt{5}}}{1-\frac{1-\sqrt{5}}{2}x}$$

to už lze převést

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

to je tzv. **Binetův vzorec**. Tento postup funguje pro všechny **Homogenní lineární rekurence k-tého stupně s konstantními koeficienty**, tedy typu:

$$a_{n+k} = \alpha_{k-1}a_{n+k-1} + \cdots + \alpha_0 a_n, k \in \mathbb{N}, \alpha_{k-1}, \ldots, \alpha_0 \in \mathbb{R}$$

2.2 Aplikace vytvořujících funkcí

Nadefinujeme zobecněnou **binomickou větu** pro

$$n \in \mathbb{R}, r \in \mathbb{Z}_0^+ : \binom{n}{r} := \frac{n(n-1)(n-2)\ldots(n-r+1)}{r!},$$

speciálně $\binom{n}{0} = 1$.

Věta 7 (Zobecněná binomická věta)**.** *$\forall r \in \mathbb{R}$ je $(1+x)^r$ vytvořující funkcí posloupnosti $\left(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \ldots\right)$ a řada $\sum_{i=0}^{\infty}\binom{r}{i}x^i$ konverguje pro $\forall x \in (-1,1)$.*

Důkaz. Empty.

□

Důsledek. $\forall n \in \mathbb{N}\ \forall x \in (-1{,}1)$ platí $\frac{1}{(1-x)^n} = \sum_{i=0}^{\infty}\binom{n+i-1}{n-1}x^i$.

Důkaz. Empty.

□

2.3 Aplikace - Catalanova čísla

Zakořeněný binární strom - buď je prázdný, nebo obsahuje speciální vrchol zvaný **kořen** a pár zakořeněných stromů, které tvoří **levý** a **pravý podstrom**.

$b_n =$ počet bin. zak. stromů na $n \in \mathbb{N}_0$ vrcholech, potom $b(x) = \sum_{n=0}^{\infty} b_n x^n$ je příslušná vytvořující funkce.

Věta 8. *Pro každé $n \in \mathbb{N}_0$ platí $b_n = \frac{1}{n+1}\binom{2n}{n}$. Kde se $\frac{1}{n+1}\binom{2n}{n}$ značí jako C_n a říká se mu n-té **Catalanovo číslo**.*

Důkaz. Empty.

□

Catalanova čísla mají mnoho interpretací, například počet triviálních uzávorkování s n páry závorek anebo počet triangulací.

3. Konečně projektivní roviny (KPR)

Jistá nová struktura, která je velice symetrická a vzácná. Jedná se o množinový systém (**hypergraf** - zobecnění grafu, kde hrany mohou být k-tice. Využívá se v samoopravných kódech a přichází z geometrie.

3.1 Eukleidovy axiomy

1. každé 2 body určují přímku
2. každou úsečku lzze prodloužit na přímku
3. ze zadaného bodu lze opsat kružnici procházejícím druhým zadaným bodem
4. všechny pravé úhly jsou stejné
5. bodem lze k přímce vést právě 1 rovnoběžku

Definice 2 (KPR)**.** *Konečná množina* $\mathcal{X}$ *a systém* $\mathcal{P}$ *podmnožin* $\mathcal{X}$ *tvoří KPR* $(\mathcal{X}, \mathcal{P}) =$ *(body, přímky) pokud splňuje tyto tři axiomy:*

1. $\forall x,y \in \mathcal{X}, x \neq y, \exists! P \in \mathcal{P} : \{x,y\} \subseteq P$
   - *každé 2 body určují právě jednu přímku*

2. $\forall P,Q \in \mathcal{P}, P \neq Q : |P \cap Q| = 1$
   - *každé 2 přímky se protínají právě v 1 bodě*

3. $\exists C \subseteq \mathcal{X}, |C| = 4, \forall P \in \mathcal{P} : |C \cap P| \leq 2$
   - *existují 4 body v obecné poloze*

Jako příklad je **Fanova rovina**, která má 7 přímek a 7 bodů. Jak lze vidět na obrázku 3.1.

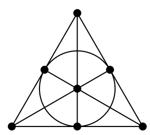


Figure 3.1: Fanova rovina

Tvrzení 9. *V KPR obsahuje každá přímka stejný počet bodů.* $\forall P,Q \in \mathcal{P} |P| = |Q|$.

Důkaz. Empty.

□

Definice 3. *Řád projektivní roviny:* $(\mathcal{X}, \mathcal{P})$ *je* $|P| - 1$ *pro* $P \in \mathcal{P}$.

Tvrzení 10. *Je-li* $(\mathcal{X}, \mathcal{P})$ *KPR řádu* n*, pak platí:*

1. *každým bodem prochází právě* $n + 1$ *přímek*
2. $|\mathcal{X}| = n^2 + n + 1$
3. $|\mathcal{P}| = n^2 + n + 1$

Důkaz. Empty.

□

3.2 Dualita KPR

"Přechod z přímek na body a z bodů na přímky."

Definice 4. ***Duální množinový systém*** *k množinovému systému* $(\mathcal{X}, \mathcal{P})$ *je* $(\mathcal{P}, \{\{P \in \mathcal{P} : x \in P\} : x \in \mathcal{X}\})$*, zkráceně* ***duál***

Tvrzení 11. *Duálem KPR řádu* n *je KPR řádu* n.

Důkaz. Empty.

□

3.3 Existence KPR

Kromě Fanovy roviny zatím neznáme žádné další příklady konečných projektivních rovin. Ale samozřejmě se ví o dalších které existují jmenovitě pro (2,3,4,5,7,8,9,11) a 12 už se neví. Domněnka je, že KPR řádu n existuje $\Leftrightarrow$ n je mocnina prvočísla. Nicméně je to pořád otevřené.

Věta 12. *Pokud existuje algebraické těleso o* n *prvcích, potom existuje KPR řádu* n.

Důkaz. Empty.

□

Konstrukce funguje nad každým tělesem a například nad $\mathbb{R}$ dává **reálnou projektivní rovinu**.

3.4 Latinský čtverec

Definice 5. *Latinský čtverec řádu* $n \in \mathbb{N}$ *je tabulka* $n \times n$ *čísel z* $\{1, \ldots, n\}$*, ve které se žádné číslo neopakuje v žádném řádku ani sloupci.*

3.4.1 Ortogonalita

Definice 6. *Latinský čtverce L, L' stejného řádu jsou* ***ortogonální****, pokud pro každé $l, l' \in \{1, \ldots, n\}$ existují $i,j \in \{1, \ldots, n\}$, takové že $L_{ij} = l, L'_{ij} = l'$. Zapisuje se jako $L \perp L'$.*

Pozorování. *Pro ortogonální latinské čtverce L, L' řádu n a pár $(l,l') \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ je pozice (l,l') s $L_{ij} = l, L'_{ij} = l'$ určena jednoznačně.*

Důkaz. Počet párů (l,l') je n^2, stejně jako počet párů (i,j).

□

Pozorování. *Je-li $L = (L_{ij})_{i,j=1}^{n}$ latinský čtverec a $\Pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ perm, tak potom $\Pi(L) := (\Pi(L_{ij})_{i,j=1}^{n}$ je latinský čtverec stejného řádu.*

Důkaz. $\Rightarrow$ BŮNO první řádek je vžzdy vzestupná řada. $\Rightarrow$ Je-li $L \perp L'$, pak $\Pi(L) \perp L'$.

□

Důsledek. Počet **navzájem ortogonálních** nanejvýš čtverců řádu $n \in \mathbb{N}$ je $n - 1$.

Důkaz. Empty.

□

Věta 13. *Konečná projektivní rovina řádu $n \geq 2$ existuje $\Leftrightarrow$ existuje $n - 1$ navzájem ortogonálních latinských čtverců řádu n.*

Důkaz. Empty.

□

4. Toky v sítích

Definice 7. *Síť je čtveřice (G, z, s, c), kde $G = (V, E)$ je orientovaný graf (tedy $V \subseteq V \times V$), $z \in V$ je **zdroj**, $s \in V$ je **stok** ($z \neq s$) a $c : E \to \mathbb{R}_0^+$. Hodnotu $c(e)$ nazýváme **kapacitou** hrany $e \in E$.*

Definice 8. *Tok v síti $(G = (V, E), z, s, c)$ je $f : E \to \mathbb{R}_0^+$ splňující následující podmínky:*

1. *$\forall r \in E : 0 \leq f(e) \leq c(e)$ (velikost toku je omezená kapacitou)*
2. ***Kirchhoffův zákon** co přitéká do vrcholu, musí odtéct, neboli:*

$$\forall u \in V \setminus \{z, s\} : \sum_{v:(u,v)\in E} f(u,v) - \sum_{v:(v,u)\in E} f(v,u) = 0$$

Definice 9. ***Velikost toku** f je $w(f) = \sum_{v:(z,v)\in E} f(z,v) - \sum_{v:(v,z)\in E} f(v,z)$.*

Tvrzení 14. *Pro každou síť existuje maximální tok.*

Důkaz. [Náčrt] Z analýzy víme, že spojitá funkce na kompaktní množině nabývá maxima. Množina $\mathcal{F} \subseteq \mathbb{R}^{|E|}$ všech toků je kompaktní funkce $w : \mathcal{F} \to \mathbb{R}$ je spojitá.

□

Definice 10. *Řez v síti (G, z, s, c) je $R \subseteq E$ taková, že každá orientovaná cesta ze zdroje z do stoku s používá aspoň jednu hranu z R.*

Speciálně hrany vycházející ze z či hrany vycházející do s tvoří řez.

Definice 11. ***Kapacita řezu** R je $c(R) = \sum_{e\in R} c(e)$.*

Řezu je jen konečně mnoho $\Rightarrow$ jistě existuje řez minimální kapacity.

Věta 15 (hlavní věta o tocích)**.** *Velikost maximálního toku = kapacita minimálního řezu, nebo-li, pro každou síť platí:* $\max\ w(f) = \min\ c(R)$*, kde f je tok a R řez.*

Definice 12 (Elementární řez)**.** *Pro $A \subseteq V$, kde $z \in A$ a $s \notin A$, nazveme množinu $R_A = \{e = (u,v) \in E : u \in A, v \notin A\}$ **elementárním řezem**. Opravdu se jedná o řez, protože pokaždé su musí nějak opustit A.*

Pozorování. *Každý řez R obsahuje elementární řez.*

Důkaz. Zvolme A jako množinu vrcholů dosažitelných po orientované cestě ze zdroje v grafu $(V, E \setminus R)$. Potom $z \in A, s \notin A$, protože R je řez $\Rightarrow R_A$ existuje $(u,v) \in R_A \Leftrightarrow u \in A, v \notin A \Rightarrow (u,v) \in R$, tedy $R_A \subseteq R$.

□

Pozorování. *Každý **v inkluzi minimální** řez R je elementární. Nebo-li $R \setminus \{e\}$ není řezem pro $\forall e \in R$.*

Důkaz. Z předchozího pozorování musí R obsahovat elementární řez $R_A \subseteq R$ a z minimality platí $R_A = R$.

□

Lemma 16. *Je-li f tok a R_A elementární řez, pak platí:*

$$w(f) = \sum_{u \in A, v \notin A, (u,v) \in E} f(u,v) - \sum_{u \in A, v \notin A, (v,u) \in E} f(v,u)$$

Důkaz. Empty.

□

Důkaz. (Věty) Empty.

□

4.1 Fordův-Fulkersonův algoritmus

```
Nastav f(e) = 0 pro ∀e ∈ E
while ∃ zlepšující cesta P do
    vylepšuj po ní tok o ϵ_P
end while
return Stávající tok f
```

Věta 17 (o celočíselnosti)**.** *Jsou-li kapacity celočíselné, pak F.F. najde max. tok po konečně mnoha krocáích a navíc má takový tok celočíselnou velikost.*

Důkaz. Tok se vždy zlepší o celé číslo $\epsilon_P >$ a $w(f) < \infty$.

□

Existují sítě s iracionálními kapacitami, kde F.F nenajde maximální tok a nekonverguje k výsledku. V síti s celočíselnými kapacitami má F.F. alg. časovou složitost $O(w(f)(|V| + |E|))$, kde f je tok. Takže je to v čase $O(|V| + |E|)$. Pokud bychom specifikovali výběr zlepšující cesty na nejkratší dostaneme **Edmondsův-Karpův algoritmus**, který má časovou složitost $0(|V| + |E|^2)$.

4.2 Königova-Egerváryho věta

Definice 13. *V grafu $G = (V,E)$ nazveme množinu $C \subseteq V$ **vrcholovým pokrytím**, pokud $C \cap e \neq \emptyset$ pro $\forall e \in E$.*

Zjistit minimální velikost vrcholové pokrytí je NP-těžká úloha.

Definice 14. ***Párováním** v G je podgraf tvořený disjunktními hranami.*

Věta 18. *(Königova-Egerváryho věta) V bipartitiním grafu je velikost min. vrcholového pokrytí rovna velikosti maximálního párování (do počtu hran).*

Důkaz. Empty.

□

4.3 Hallova věta

Definice 15. *Mějme konečné množiny X a I.* ***Množinový systém*** $\mathcal{M}$ *je* $(M_i : i \in I)$*, kde* $M_i \subseteq X$*.* ***Systém ruzných reprezentantů (SRR)*** *pro* $\mathcal{M}$ *je prosté zobrazení* $f : I \to X$ *takové, že* $\forall i \in I : f(i) \in M_i$*. Tedy* f *je výběr jednoho prvku z každé* M_i *takový, že žádný prvek nevybereme víckrát.* ***Incidenční graf*** *systému* $\mathcal{M}$ *je bipartitní graf* $G_{\mathcal{M}} = (I \cup X, E)$*, kde* $E = \{\{i,x\} : i \in I, x \in X, x \in M_i\}$*. Pokud* $\mathcal{M}$ *má SSR* $\Leftrightarrow$ $S_{\mathcal{M}}$ *obsahuje párování velikosti* $|I|$*.*

Věta 19 (Hallova věta)**.** $\mathcal{M}$ *má SSR* $\Leftrightarrow \forall J \subseteq I : |\cup_{j\in J} M_j| \geq |J|$*. Pravé části se říká* ***Hallova podmínka****, také se věta označuje jako* ***Hall's marriage theorem****.*

Definice 16. *Empty.*

S axiomem výběru by šlo dokázat variantu s konečnými M_i a nekonečnými I,X. S nekonečnými I,X to platit nemusí.

4.4 Rozšiřování latinských obdélníků

Důsledek. V každém bipartitním grafu $G = (A \cup B, E)$ s $E \neq \emptyset$ a $\mathtt{deg}_G(x) \geq \mathtt{deg}_G(y)$ pro každé $x \in A, y \in B$ existuje párování velikosti $|A|$.

Důkaz. Empty. □

Latinský obdélník typu $k \times n$ pro $k \leq n$ je tabulka s řádky s n sloupci vyplněnými symboly $1, \ldots, n$ tak, že se v žádném řádku ani sloupci žádný symbol neopakuje.

Věta 20. *Každý latinský obdélník typu* $k \times n$ *lze doplnit na latinský čtverec řádu* n*.*

Důkaz. Empty. □

5. Míra souvislosti grafu

Definice 17. *Graf je **souvislý** pokud jsou každé dva vrcholy spojené cestou, jinak je graf **nesouvislý** a je rozložen na aspoň dvě **komponenty souvislosti**.*

Nyní budeme zkoumat jak moc je graf odolný proti rozpadnutí po odebrání hrany nebo vrcholu.

Definice 18. ***Hranovým řez*** *v grafu $G = (V,E)$ je množina hran $F \subseteq E$ taková, že graf $G - F = (V, E \setminus F)$ je nesouvislý. (Také se někdy nazývá jako **separátor**.)*

Definice 19. ***Vrcholovým řezem*** *v grafu $G = (V,E)$ je množina vrcholů $A \subseteq V$ taková, že graf $G - A = (V \setminus A, E \cap \binom{V \setminus A}{2})$ je nesouvislý.*

Definice 20. ***Hranová souvislost*** *grafu $G = (V,E)$ je*

$$k_e(G) = \begin{cases} \min\{|F| : F \text{ je hranový řez v } G\} \\ k_e(G) = 1 \text{ pokud } G \equiv K_1 \end{cases}$$

Definice 21. ***Vrcholová souvislost*** *grafu $G = (V,E)$ je*

$$k_v(G) = \begin{cases} \min\{|A| : A \text{ je vrcholový řez v } G\} \\ k_v(G) = 1 \text{ pokud } G \equiv K_1 \\ k_v(G) = n - 1 \text{ pokud } G \equiv K_n, n \geq 2 \end{cases}$$

Nesouvislé grafy mají vrcholovou i hranobvou souvislost 0.

Definice 22. *Pro $r \in \mathbb{N}_0$ je graf **hranově** r**-souvislý**, pokud $k_e(G) \geq r$.*

Definice 23. *Pro $r \in \mathbb{N}_0$ je graf **vrcholově** r**-souvislý**, pokud $k_v(G) \geq r$.*

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

Lemma 21. $\forall G = (V,E) \forall e \in E : k_e(G) - 1 \leq k_e(G - e) \leq k_e(G)$ *Po odebrání hrany klesne hranová souvislost maximálně o 1.*

Důkaz. Empty.

□

Lemma 22. $\forall G = (V,E)\ \forall e \in E : k_v(G) - 1 \leq k_v(G - e) \leq k_v(G)$ *Po odebrání hrany klesne vrcholová souvislost maximálně o 1.*

Důkaz. Empty.

□

Důsledek. $\forall G = (V,E) : k_v(G) \leq k_e(G)$ Vrcholová souvislost je maximálně stejná jako hranová souvislost.

Důkaz. Empty.

□

Nerovnost může být ostrá. To lze vidět na příkaldu "motýlka". Lze vidět na obrázku ??.

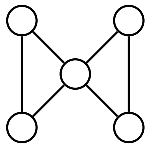


Figure 5.1: Graf "motýlek".

Věta 23 (Ford-Fulkersonova věta)**.** *$\forall G\ \forall t \in \mathbb{N} : k_e \geq t \Leftrightarrow$ mezi každými 2 vrcholy grafu $G\ \exists \geq t$ hranově disjunktních cest.*

Důkaz. Empty.

□

Varianat Fordovy-Fulkersonovy věty platí i pro vrcholovou souvislost. Tyto věty jsou známé také jako Mengerovy věty.

Věta 24 (Mengerova věta)**.** *$\forall G\ \forall t \in \mathbb{N} : k_e(G) \geq t \Leftrightarrow$ mezi každými 2 vrcholy grafu $G\ \exists \geq t$ vrcholově disjunktních cest (mimo u,v).*

Důkaz. Empty.

□

Jelikož lze zjistit tok maximální velikost v polynomiálním čase, tak máme algoritmus na zjištení $k_e(G), k_v(G)$ také v polynomiálním čase.

5.1 2-souvislost podrobněji

Definice 24. *Hranový řez velikosti 1 se nazývá **most** a vrcholový řez velikosti 1 se nazývá **artikulace**.*

Pro graf $G = (V,E)$ s $e \in E$ označme $C \div e$ graf vzniklýz G operací **podrozdělení hrany** e na cestu délky 2.

Lemma 25. *Pro každý graf $G = (V,E)$ a pro každou hranu $e \in E$ platí: G je vrcholově 2-souvislý $\Leftrightarrow G \div e$ je vrcholově 2-souvislý.*

Důkaz. Empty.

□

Věta 26 (Ušaté lemma)**.** *Graf G je vrcholově 2-souvislý $\Leftrightarrow G$ lze vytvořit z K_3 operacemi přidávání a podrozdělování hran. Proč "Ušaté lemma"? Přidání hrany a její podrozdělení odpovídám přidání cesty mezi 2 vrcholy (="přiepení ucha").*

Věta 27 (Alternativní znění)**.** *G je vrcholově 2-souvislý $\Leftrightarrow G$ lze vytvořit z cyklu přidáváním uší, protože přidávání ucha lze simulovat přidáním hrany a jejím podrozdělení.*

Důkaz. Empty.

□

6. Počítání dvěma způsoby

Metoda důkazů v kombinatorice. Určíme nějaký neznámý počet X vyjádřením počtu Z dvěma výrazy, z nichž jeden X obsahuje a druhý ne $\Rightarrow$ máme vyjádření pro X.

6.1 Cayleyho vzorec

Kolika způsoby lze vytvořit strom na vrcholech $\{1, \ldots, n\}$? Nebo-li jaká je počet koster $\kappa(n)$ grafu K_n?

Definice 25. *Kostra grafu $G = (V, E)$ je strom $T = (V, E')$ s $E' \subseteq E$.*

Věta 28 (Cayleyho vzorec)**.** *Pro každé $n \geq 1$ platí $\kappa(n) = n^{n-2}$.*

Existuje řada důkazů s velmi odlišnými myšlenkami, ukážeme si nejjednodušší založený na počítání dvěma způsoby.

Důkaz. Empty. $\square$

Věta 29. *Graf $K_n - e$ má $(n-2)n^{n-3}$ koster pro $n \geq 2$.*

Důkaz. Empty. $\square$

Počet koster $\kappa(G)$ grafu $G = (\{1, \ldots, n\}, E)$ lze určit pomocí determinantu. Uvažme **Laplacián** $L(G)$ grafu G, tedy matici $L(G) = (L_{ij})_{i,j=1}^{\infty}$, kde

$$L_{ij} = \begin{cases} \mathtt{deg}_G(i) \text{ pokud } i = j \\ -1 \text{ pokud } (i,j) \in E \\ 0 \text{ jinak} \end{cases}$$

Věta 30 (Kirchhoffova věta)**.** $\forall G : \kappa(G) = \det(L(G)^{1,1})$, *kde* $(L(G)^{1,1})$ *je Laplacián* $L(G)$ *bez 1. řádků a 1. sloupce.*

6.2 Spernerova věta

Definice 26. *Systém $\mathcal{M} \subseteq 2^{\{1,\ldots,n\}}$ podmnožin n-prvkové množiny $\{1, \ldots, n\}$ je **nezávislý**, pokud platí: $\forall A, B \in \mathcal{M}, A \neq B : A \nsubseteq B \wedge A \nsupseteq B$.*

Věta 31 (Spernerova věta)**.** *Každý nezávislý systém v $2^{\{1,\ldots,n\}}$ obsahuje $\leq \binom{n}{\lceil \frac{n}{2} \rceil}$ množin a tento odhad je těsný. Ekvivalentně: Nejdelší antiřetězec v $(2^{\{1,\ldots,n\}}, \leq)$ má právě $\binom{n}{\lceil \frac{n}{2} \rceil}$ prvků.*

Důkaz. Empty. $\square$

7. Úvod do Ramseyovy teorie

"Každý velký systém obsahuje homogenní podsystém" dané velikosti.

Definice 27. ***Obarvení*** *množiny X r barvami (zkráceně r-obarvení) je libovolné zobrazení přiřazující každému prvku z X jednu z r barev.*

Věta 32 (Dirichletův princip, Pigeonhole principle)**.** $\forall r, n_1, \ldots, n_r \in \mathbb{N}$*: obarvíme-li prvky množiny X r barvami, pak je-li $|X| \geq 1 + \sum_{i=1}^{r}(n_i - 1)$, X obsahuje n_i prvků i-té barvy.*

Důkaz. Triviální.

□

Co kdybychom chtěli obarvit dvojice?

Definice 28. *Pro $k,l \in \mathbb{N}$ buď $R(k,l)$ nejmenší $N \in \mathbb{N}$ takové, že každé 2-obarvení (BÚNO: červené a modré obarvení) $E(K_N)$ obsahuje červené K_k nebo modré K_l jako podgraf.*

Věta 33 (Ramseyova věta pro 2 barvy)**.** $\forall k,l \in \mathbb{N} : R(k,l)$ *je konečné. Dokonce* $R(k,l) \leq \binom{k+l-2}{k-1} = \binom{k+l-2}{l-1}$.

Důkaz. Empty.

□

Určit Ramseyovská čísla $R(k,l)$ přesně je velice obtížné (už pro malé případy). Známá čísla $R(3,3) = 6$, $R(4,4) = 18$.

Věta 34. $\forall k \geq 3 : R(k,k) > 2^{k/2}$

Důkaz. Empty.

□

Rozšíření Ramseyovy věty na více barev a také na barvení p-tic vrcholů.

Definice 29. *Pro čísla $p,r,n_1, \ldots, n_r \in \mathbb{N}$ (p - velikost barevných množin, r - počet barev, n_i - velikost 1-barevných podstruktur, které chceme najít) definujeme **Ramseyovo číslo** $R_p(n_1, \ldots, n_n)$ jako nejmenší $N \in \mathbb{N}$ takové, že pro každou množinu X s $|X| \geq N$ a každé r-obarvení množiny $\binom{X}{p}$ existuje $i \in \{1, \ldots, n\}$ a $Y \subseteq X$ takové, že $|Y_i| = n_i$ a všechny p-tice z $\binom{Y}{p}$ mají i-tou barvu.*

Věta 35 (Ramseyova věta pro p-tice)**.** *Pro každé $p,r,n_1, \ldots, n_n$ je $R_p(n_1, \ldots, n_n)$ konečné.*

Důkaz. Empty.

□

7.1 Aplikace - Erdösova-Szekeresova věta

Definice 30. *P = konečná množina bodů v rovině $\mathbb{R}^2$. P je v **obecné poloze**, pokud neobsahuje 3 body na přímce. P je v **konvexní poloze**, pokud tvoří množinu vrcholů konvexního mnohoúhelníku.*

Lemma 36. *Každá množina 5 bodů v $\mathbb{R}^2$ v obecné poloze obsahuje 4 body v konvexní poloze.*

Důkaz. Empty.

□

Věta 37 (Erdösova-Szekeresova věta)**.** *Pro každé $r \in \mathbb{N}$ existuje nejmenší $ES(r) \in \mathbb{N}$ takové, že každá konečná množina $s \geq ES(r)$ body v $\mathbb{R}^2$ b obecné poloze obsahuje r bodů v konvexní poloze.*

Důkaz. Empty.

□

Erdösova-Szekeresova domněnka je že $\forall r \geq 2 : ES(r) = 2^{r-2} + 1$. Zatím se zná, že to je dolní odhad a horní jako $\leq 2^{r+o(r)}$.

Věta 38 (Nekonečná verze Ramseyovy věty)**.** *Pro každé p,$r \in \mathbb{N}$ a pro každé r-obarvení množiny $\binom{\mathbb{N}}{p}$ existuje nekonečná $A \subseteq \mathbb{N}$ taková, že všechny její p-tice mají v daném r-obarvení stejnou barvu.*

Důkaz. Empty.

□

Nekonečná verze implikuje konečnou. Dá se dokázat sporem, my si ji ukážeme pro $n_1 = \cdots = n_n = n$.

Lemma 39 (Königovo lemma)**.** *V každém zakořeněném stromě, který má nekonečně mnoho vrcholů ale jen konečné stupně existuje nekonečná cest začínající v kořeni.*

Důkaz. (implikace konečné věty) Empty.

□

8. Samoopravné kódy

Definice 31. ***Abeceda*** *Σ = konečná množina symbolů,* ***slovo*** *délky n = posloupnost n symbolů, Σ^n = množina všech slov délky n.*

Definice 32. ***Hammingova vzdálenost****: $x,y \in \Sigma^n : d(x,y) = |i \in \{1,\ldots,n\} : x_i \neq y_i|$, neboli počet pozic, kde se x a y liší. d je metrika a tedy (Σ^n, d) je metrický prostor.*

Definice 33. ***(Blokový) kód*** *je $C \subseteq \Sigma^n$ a prvky C jsou* ***kódova slova****. Pomocí C umíme opravit $\leq t$ chyb, pokud $\forall y \in \Sigma^n \exists$nanejvys 1 slovo$x \in C$t.ž.$d(x,y) \leq t$.*

Definice 34. *Parametry kódu:*

1. *délka = n,*
2. *velikost abecedy $q = |\Sigma|$,*
3. *dimenze $k = \log_q |C|$,*
4. *vzdálenost $d = \min_{x,x' \in C, x \neq x'} d(x,x')$.*

Kód s parametry n,k,d,q značíme $(n,k,d)_q$.

V kódu s parametry $(n,k,d)_q$ dokážeme opravit $\leq \lfloor \frac{d-1}{2} \rfloor$ chyb. Množiny slov ve vzdálenosti $\leq \lfloor \frac{d-1}{2} \rfloor$ od kódových slov jsou navzájem disjunktní. Pokud $d \leq n$, tak dokážeme opravit $\leq \lfloor \frac{n-1}{2} \rfloor$.

Příklad. 1. opakovací kód: každý symbol n-krát zopakujeme, paramtery: $(n,1,n)_q$

2. charakteristický vektory KPR
   - kódová slova P - {0,1} - vektor, kde na pozici x je 1 $\leftrightarrow x \in P$
   - $(X, \mathcal{P})$ - KPR řádu n
   - parametry: $(n^2+n+1, \log_2(n^2+n+1), 2n)_2$
   - $|X| = n^2+n+1$ a $|C| = |\mathbb{P}| = n^2+n+1$
   - $d = 2n$
   - 2 kódove slova sdílí jednu jedničku, na zbytku se liší na $2n$ pozicích
3. hadamardovy kódy
   - hadamardova matice řádu n je $H \in \{-1,1\}$, kde $H \cdot H^T = n \cdot I_n$
   - každý 2 různy řádky se liší na $n/2$ pozicích
   - zvolme $C = \{\text{řádky}H\} \cup \{-\text{řádky}H\}$
   - parametry: $(n, 1+\log_2(n), \frac{n}{2})_2$

$$H_1 = 1$$

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Sylvestrova konstrukce hadamardovy matice:

$$H_{n+1} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

Hadamardova domněnka: pro $\forall k \in \mathbb{N} \exists$ hadamardova matice řádu $4k$

Kódy C, C' jsou ekvivalentní, pokud se liší jen pořadím pozic. $\exists \Pi \in S_n : X = (x_1, \ldots, x_n) \in C \leftrightarrow \Pi(X) = (X_{\Pi(1), \ldots, X_{\Pi(n)} \in C}$. Pro jaké parametry existuje kód?

Definice 35. *Kombinatorická koule je středem $X \in \Sigma^n$ a poloměrem t je $B(X,t) = \{y \in \Sigma^n : d(x,y) \leq t\}$.*

Lemma 40. *Je-li C kód se vzdáleností $2t+1$, pak $\forall X,X' \in C : B(X,t) \cap B(X',t) = \emptyset$.*

Důkaz. Sporem - $\exists z \in B(x,t) \cap B(x',t) \implies d(x,x') \leq d(x,z) + d(x',z) \leq t + t = 2t$, kde $d(x,x')$ je $\geq 2t+1$, takze celkove je $2t+1 \leq 2t$.

□

Věta 41 (Hammingův odhad). $\forall$ *kód C s parametrama $(n,k,d)_q$ platí, že $|C| \leq \frac{q^n}{V(t)}$.*

Důkaz. $d = 2t+1 \implies$ koule okolo kódovych slov s poloměrem t jsou disjunktní. $\implies |C| \cdot |V(t)| \leq |\Sigma^n| \implies |C| \leq \frac{|\Sigma^n|}{|V(t)|} = \frac{|q^n|}{|V(t)|}$.

□

Definice 36. ***Perfektní kód*** *= kód s parametry $(n,k,2t+1)_q$ a s $|C| = \frac{q^n}{V(t)}$.*

Opakovací kód s $q = 2$ a lichou delkou.

Věta 42 (Gilbertův - Varshalův odhad). *$\forall n,q,d \in \mathbb{N} : \exists$ kód C s parametry $(n,k,d)_q$, kde $|C| \geq \frac{q^n}{V(d-1)}$.*

Důkaz. Stačí iterativně odebírat slova z Σ^n spolu se slovy v Hammingové vzdálenosti $\leq d-1$. Proces skončí po $\geq \frac{q^n}{V(d-1)}$ krocích, protože odebírané koule jsou nanejvýš disjunktní.

□

Definice 37. ***Linearní kódy*** *- jako abecedu použít konečné těleso $\mathbb{K} = \Sigma^n$. Podprostor vektorového prostoru $\mathbb{K}^n$ s parametry n,k,d,q značíme $[n,k,d]_q$.*

Příklad.

1. opakovací kódy nad $\mathbb{Z}_p$ [nejsou linearní]
2. charakteristický vektory KPR [nejsou linearní]
3. hadamardovy kódy [obecně ne, ze Sylvestrovy konstrukce ano]

8.1 Lineární kódy

Víme, že každé těleso $\mathbb{K}$ odpovídá Galoisovu tělesu $\mathbb{F}_q$. $\forall x,y,z \in \mathbb{K}^n : d(x,y) = d(x+z, y+z) = d(x-y,0)$. $\Rightarrow$ minimální vzdálenost d se rovná $\min_{x,y \in C, x \neq y}\{d(x-y,0) = \min_{x \in C, x \neq 0}\{d(x,0)\}\}$. $\Rightarrow$ ke zjištění d není třeba zkoumat všechny dvojice, stačí počítat nenulové složky kódových slov. Výhodou lineárních kódů je úsporný popis, namísto všech q^r prvků kódu stačí uvést r prvků nějaké jeho báze.

Definice 38. ***Generující matice*** *kódu C = matice $M \in \Sigma^{r \times n}$ jejíž řádky tvoří bázi kódu C. V prostoru $\mathbb{F}_q^n$ definujeme* ***skalární součin*** *$< x,y >= \sum_{i=1}^{n} x_i y_i$ pro $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$. Nejedná se o klasický skalární součin podle klasické definice, protože neplatí $< x,x >= 0 \Leftrightarrow x = 0$ (třeba $x = (1,1,0,0)$ nad $\mathbb{F}_2^4$).*

Definice 39. ***Duálním kódem*** *k lineárnímu kódu C je jeho ortogonální doplněk.*

$$C^{\perp} = \{x \in \mathbb{F}_q^n :< x,y >= 0 \text{ pro každé } y \in C\}$$

Z povahy našeho skalárního součinu nemusí platit $C \cap C^{\perp} = \{0\}$. Platí $\dim(C^{\perp}) + \dim(C) = n$ a $(C^{\perp})^{\perp} = C$. Generující matice $M^{\perp}$ kódu $C^{\perp}$ se nazývá **kontrolní matice**. Řádky kontrolní matice určují lineární rovnice, které musí každé slovo z C splňovat (a naopak každý vektor z $\mathbb{F}_q^n$, který je splňuje, je kódovým slovem v C). Nebo-li $C = \{x \in \mathbb{F}_q^n : M^{\perp}x = 0\}$.

Mějme lineární kód C s parametry $[n,r,d]_q$.

8.1.1 Kódování lineární kódy

Ze vstupního slova $z \in \mathbb{F}_q^n$ chceme vytvořit kódové slovo $x \in C \subseteq \mathbb{F}_q^n$. Nechť $M \in \mathbb{F}_q^{r \times n}$ je generující matice kódu C. Pro každý lineární kód existuje ekvivalentní kód, jehož generující matice má tvar:

$$\begin{pmatrix} Ir & B \end{pmatrix}$$

Kde výška je r a šířka n. Říká se jí **standardní forma**. Stačí generující matici upravit Gaussovou eliminací a popřípadě zpermutovat sloupce. $\Rightarrow$ BŮNO: Matice M je ve standardní formě. Jako kódové slovo zvolíme $x = M^{\top} z \in C$. $\Rightarrow$ x má na prvních r souřadnicích slovo z (**indormační symboly**) a na zbylých $n-r$ souřadnicích obsahuje **kontrolní symboly**.

$$\begin{pmatrix} I_r \\ B^{\top} \end{pmatrix} \begin{pmatrix} z \end{pmatrix} \begin{pmatrix} z \\ . \end{pmatrix}$$

8.1.2 Dekódování lineárních kódů

Po odeslání $x \in C$ bylo přijato $y \in \mathbb{F}_q^n$. Příjemce zná pouze y a chce najít kódové slovo, které je mu nejblíž. Nechť $M^{\perp}$ je kontrolní matice kódu C, pokud je matice Mve standardní formě pak:

$$M^{\perp} = \begin{pmatrix} -B\top & I_{n-r} \end{pmatrix}$$

kde šířka je r a výška $n-r$, protože pak $M^{\perp}M^{\top} = -B^{\top}I_r + I_{n-r}B^{\top} = 0$. Jako **syndrom slova** $y \in \mathbb{F}_q^n$ nazveme součin $M^{\perp}y$, protože $C = \{x \in \mathbb{F}_q^n : M^{\perp}x = 0\}$, tak máme určené lineární zobrazení $S : \mathbb{F}_q^n \to \mathbb{F}_q^{n-r}$ splňující $C = Ker(S)$. Zobrazení S nazveme **syndrom**. Zobrazení S je na, protože platí $\dim(Ker(S)) + \dim(Im(S)) = \dim(\mathbb{F}_q^n)$, kde $Im(S)$ je obraz S.

Lemma 43. *Zobrazení S je prosté na $B(0,t)$ kde $t = \lfloor \frac{d-1}{2} \rfloor$.*

Důkaz. Empty.

□

Podle lemma tedy k $S \restriction B(0,t)$ existuje inverzní zobrazení $S^{-1} : S(B(0,t)) \to B(0,t)$. S^{-1} není lineární, ale jde popsat tabulkou s q^{n-k} prvky z $B(0,t)$ a v této tabulce je pro každý syndrom slova uloženo nějaké slovo s minimální vahou a s daným syndromem.

Co víme:

1. Pro $y \in B(x,t)$ máme $S(y-x) = S(y) - S(x) = S(y)$ (díky linearitě a toho že $x \in Ker(S)$). Neboli y a vzniklá chyba $y-x$ mají stejný syndrom.

2. Pro $y \in B(x,t)$ máme $y - x \in B(0,t)$ a tedy $y - x = S^{-1}(S(y-x))$. Neboli vzniklou chybu jde vyjádřit pomocí S.

3. $x = y - (y-x) = y - S^{-1}(S(y-x)) = y - S^{-1}(S(y))$ nezávisý na x, pro dané y pomocí syndromu $S(y)$ dokážeme určit kódové slovo x, ze kterého vzniklo, nastalo-li $\leq t$ chyb.

8.1.3 Jak dekódovat

Pro přijaté slovo $y \in \mathbb{F}_q^n$ spočítat $x = y - S^{-1}(M^{\perp}y)$, kde $M^{\perp}$ je kontrolní matice a zobrazení S^{-1} máme připravené jako tabulku. Nastane-li $\leq t$ chyb, je x kódové slovo, ze kterého y vzniklo.

Tvrzení 44. *Vzdálenost d kódu C = minimální počet lineárně závislých sloupců kontrolní matice $M^{\perp}$.*

Důkaz. Víme, že d = minimální počet nenulových symbolů v nenulovém slově x z C. $x \in C \Leftrightarrow M^{\perp}x = 0$ tedy sliupce $M^{\perp}$ vybrané nenulovými složkami x jsou lineárně závislé.

□

8.2 Hammingovy kódy

Příklad lineárních kódů, které jsou dokonce perfektní. Jejich nevýhodou je, že nedokáží opravit příliš mnoho chyb. Například nad tělesem $\mathbb{F}_2$. Mějme parametr $r = 3$. Generující matice:

$$M = \begin{pmatrix} & - & l_1 & - \\ I_{2^r-r-1} & - & l_2 & - \\ & - & l_3 & - \end{pmatrix}$$

Kde l_i jsou všechny nenulové vektory z $\mathbb{F}_2^r$ různé od vektorů kanonické báze. Kontrolní matice:

$$M^\perp = \begin{pmatrix} | & | & | & & \\ l_1 & l_2 & l_3 & & I_r \\ | & | & | & & \end{pmatrix}$$

Parametry matic jsou r a $2^r - r - 1$. Dva vektory z $\mathbb{F}_2^r \setminus \{0\}$ jsou lineárně závislé $\Leftrightarrow$ jsou totožné $\Rightarrow$ minimální počet lineárně závislých sloupců v $M^\perp$ je 3 a podle tvrzení 13.2. je vzdálenost kódu 3. $\Rightarrow$ jedná se o kód s parametry $[2^r, 2^r - r - 1, 3]_2$, takže opraví ≤ 1 chybu

Příklad. Pro $r = 3$ dostaneme kód s parametry $[7,4,3]_2$. Jedná se o kód sestavený z Fanovy roviny přidáním počátku a doplňků.

Hommingovy kódy jsou perfektní: stačí ukázat, že Hammingův odhad $|C| \leq \frac{q^n}{V(t)}$ je těsný. $t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = 1$. $V(t) = V(1) = \sum_{i=0}^{t} = (q-1) = 1 + (2^r - 1) = 2^r$. $\frac{q^n}{V(1)} = \frac{2^{@^r-1}}{2^r} = 2^{2^r-r-1}$. $|C| = 2^r = 2^{2^r-r-1}$ takže Hammingův je skutečně pro Hammingovy kódy těsný.

Lepší reprezentace funkce S^{-1}. Tabulka reprezentující S^{-1} má pouze $2^{n-r} =$ $= 2^{2^r-1-(2^r-r-1)} = 2^r = n+1$ prvků. Ve skutečnosti tabulku vůbec nepotřebujeme. Zpermutujeme-li sloupce a řádky $M^\perp$ pak, aby i-tý sloupec byl binárním zápisem čísla i, pak $S(y)$ určuje pozici na níž nastala chyba. $\Rightarrow$ lze dékodovat tak, že pokud $S(y) = 0$, pak $x = y$, jinak je $S(y)$ binárním zápisem čísla i a pak $x =$ slovo vzniklé z y výměnnou bitu, který je v y na pozici i.

Kombinatorika a grafy II

9. Párování v grafech

Definice 40. ***Párování*** *v grafu $G = (V,E)$ je množina hran $M \subseteq E$ taková, že každý vrchol z G je obsažen v nejvýš jedné hraně v M. $\mu(G) :=$ velikost největšího párování v grafu G.*

Definice 41. ***Vrcholové pokrytí*** *v grafu $G = (V,E)$ je množina vrcholů $T \subseteq V$ t.ž. každá hrana obsahuje aspoň jeden vrchol z T. $\tau(G) :=$ velikost nejmenšího vrcholového pokrytí v grafu G.*

Cvičení. *Nechť $G = (V,E)$ je bipartitni graf s partitami $A,B, |A| \leq |B|$, souvislý. Jaké nerovnosti (nebo rovnosti) platí mezi $\mu(G), \tau(G), |A|$:*

- $\mu(G) \leq |A|$
- $\mu(G) = \tau(G)$ *(plyne z König-Egarvaryho vety)*

Pozorování. $\mu(G) \leq \tau(G)$ *v libovolném grafu G.*

Cvičení. *Dokažte:*

1. $\exists G : \mu(G) \neq \tau(G)$
   - *$K4$ s tím že uprostřed je vrchol (má $\mu(G) = 2$ a $\tau(G) = 3$)*
2. $\forall G : \tau(G) \leq 2\mu(G)$
   - *v nejhorším případě vezmu oba vrcholy všech hran z M*

Definice 42. ***Volný vrchol****: vrchol nesousedící s žádnou hranou z M.* ***volná střídavá cesta****: cesta spojující dva volné vrcholy na níž se střídají párovácí($\in M$) a nepárovácí($\notin M$) hrany.*

Lemma 45. *Nechť M je párování v G. Potom M je největší párování v $G \Leftrightarrow$ v G neexistuje volná střídající se cesta pro M.*

Důkaz. $\Rightarrow$ Pokud v G existuje VSC pak lze tyto hrany přehodit. Potom je to spor s tím, že je největší. $\Leftarrow$ Nechť M není největší potom existuje N větší párování než M. Uvažme graf s hranami $M \cup N$. Každá komponenta grafu je buď:

1. izolovaná hrana v $M \cap N$
2. kružnice sudé délky, kde se střídají M a N
3. cesta na níž se střídají M a N

Protože $|N| > |M|$ v $M \cup N$ musí být komponenta K, která má víc hran z N než z M. K je cesta liché délky, která začíná a končí hranou z N, tedy K je VSC pro M. $\square$

Definice 43. ***Kytka*** *v grafu G a párování M je podgraf tvořený* ***stonkem*** *S a* ***květem*** *K, kde S je cesta sudé délky mezi dvěma vrcholy x a y, kde x je volný a $y \in K$, navíc na S se střídají párovací a nepárovací hrany. K je lichá kružnice, která neobsahuje žádný vrchol z S a střídají se na ni párovací a nepárovací hrany (u y má dvě nepárovací hrany).*

Může nastat že $x = y$ a $S = \{x\}$.

Pozorování. *Hrany z květu jsou nepárovací. Jinak by se nejednalo o párování.*

Definice 44. ***Kontrakce*** *květu K nahradí K jedním vrcholem y, smaže všechny hrany indukované K a každou hranu $\{u,v\}$, kde $u \in K$ a $v \notin K$ nahradí hranou $\{y,v\}$. Označme $G.K$ graf vzniklý z G kontrakcí květu K, $M.K$ pak párování vznikle z M odstraněním všech hran K.*

Lemma 46. *Nechť M je párování v grafu G obsahující kytku se stonkem S a květem K. Potom M je největší párování v $G \Leftrightarrow M.K$ je největší párování v $G.K$.*

Nebo-li: *M má VSC v $G \Leftrightarrow M.K$ má VSC v $G.K$.* Navíc z VSC v $M.K$ v $G.K$ lze v polynomiálním čase najít VSC v M a G.

Proof. $\Rightarrow$ (v alternativním znění) Nechť P je VSC v $M.K$. Potom:

1. $y \in P \Rightarrow P$ je i VSC v M
2. y je vnitřní vrchol v P, potom lze nahradit obloukem z K (jsou dva oblouky, protože je tam celkově lichý počet hran, tak jedna cesta musí být lichá a druhá sudá, tudíž to lze spojit)
3. y je koncový vrchol v P, potom y musí být volný, tudíž $x = y$, poté prakticky stejný postup jako u 2.

$\Leftarrow$ G má VSC $\Rightarrow$ $G.K$ má VSC, pokud S má délku 0, to jest y je volný vrchol. Následně to pak už není cesta ale sled. Začnu tedy z konce cesty a poprvé co se dostanu do y tak skončím. $M \triangle S$: Párování v G vznikne tak, že se na S prohodí párovací a nepárovací hrany.

Pozorování: V $M \triangle S$ je květ K kytka se stonkem délky 0. Pozorování: $|M \triangle S| = |M|$.

G má VSC $\Rightarrow G.K$ má VSC, navíc S má délku 0. (G,M) má VSC $\Leftrightarrow (G, M \triangle S)$ má VSC $\Rightarrow (G.K, (M \triangle S).K)$ má VSC $\Leftrightarrow (G.K, M.K)$ má VSC. □

Lemma 47. *Pokud NajdiVSCneboKytku napíše "M je největší", tak M je největší.*

Proof. Pokud M není největší, tak obsahuje VSC $v_0 v_1 \dots v_k \in V$, dokážeme indukci podle i, že každý z vrcholů $v_0 \dots v_k$ dostal přidělenou hladinu $h(v_i)$ splňující $h(v_i) \equiv i \mod 2$. Pro $i = 0$ v_0 je volný, tedy $h(v_0) = 0$. Hotovo. Pro $i > 0$, i liché, indukční předpoklad je $h(v_{i-1})$ je sudá: tak z algoritmu buď už v_i měla lichou $h(v_i)$ nebo ji dostala. (Kdyby sudá, tak vyhodí VSC nebo Kytku.) Pro $i > 0$ i je sudé, indukční předpoklad, že $h(v_{i-1})$ je lichá: tak obdobně bude $h(v_i)$ sudé. Jistě k je liché, tedy $h(v_k)$ je lichá, ale v_k je volný vrchol, tedy $h(v_k) = 0$ a to je spor. □

Definice 45. ***Perfektní párování*** *v grafu G je párování v němž každý vrchol sousedí s právě jednou párovací hranou.*

Algorithm 1 NajdiVSCneboKytku

Require: Graf $G = (V,E)$ párování M
Ensure: Buď VSC P pro (G,M), nebo kytka $S \cup K$ v (G,M), nebo "M je největší párování v G".

Používáme frontu vrcholů ‘F‘, pro každý vrchol $x \in V$ máme hladinu $h(x) \in \mathbb{N}_0$ a rodiče $r(x) \in V$.
Na začátku ‘F‘ $= \emptyset, h(x)$ a $r(x)$ jsou nedefinované.
for každý volný vrchol x **do**
    Zařaď x do ‘F‘, $h(x) = 0$.
end for
Dokud ‘F‘ $\neq \emptyset$: odebereme x z ‘F‘.
if $h(x)$ je lichá. Nechť y je vrchol spojený s x hranou M. **then**
    Pokud $h(y)$ není definovaná: $h(y) = h(x) + 1$, $r(y) = x$, zařaď y do ‘F‘.
    Pokud $h(y)$ je sudá: to nemůže nastat
    if (1.3) Pokud $h(y)$ je lichá: Px = cesta $x, r(x), r(r(x)), \dots,$ Py je cesta $y, r(y), r(r(y)), \dots$ obě cesty vedou až do volného vrcholu. **then**
        Pokud $Px \cap Py = \emptyset$ tak potom $Px \cup Py \cup \{x,y\}$ je **VSC**, konec.
        Pokud $Px \cap Py \neq \emptyset$ našli jsme **kytku** $Px \cap Py \cap \{x,y\}$, konec.
    end if
else Pokud $h(x)$ je sudá. Pro každý y t.z. $\{xy\} \notin M$:
    Pokud $h(y)$ není definovaná: $h(y) = h(x) + 1$, $r(y) = x$, vlož y do ‘F‘.
    Pokud $h(y)$ je lichá, tak nedělej nic.
    Pokud $h(y)$ je sudá: najdi VSC nebo kytku jako v 1.3,konec.
end if
Pokud dojdeme do stavu, že $F = \emptyset$, napiš "M je největší", konec.

Algorithm 2 ZvětšiPárování

Require: G,M
Ensure: párování M' v G, $|M'| > |M|$ nebo "M je největší"

Procedura NajdiVSCneboKytku(G,M)
M je největší, tak konec
VSC, invertuji a zvětši M, konec
if Kytka **then**
    ZvětšiPárování(G.K,M.K)
    $M.K$ je největší, potom i M je největší
    M' je větší párování v $G.K$ než $M.K$: $M^* := M' \cup (\frac{|k|-1}{2}$ hran květu) tak aby to šlo.
end if

Algorithm 3 Algoritmus pro hledání největšího párování

Require: G
Ensure: největší párování v G

$M :=$ libovolné párování (buď prázdné, nebo hladově nějaké)
Opakuj ZvětšiPárování(G,M) dokud to jde. **return** Vypiš nalezéné párování.

Pozorování. *Perfektní párování je největší párování.*

Pozorování. *Ne každý graf má perfektní párování (trojúhelník).*

Definice 46. ***Lichá komponenta*** *grafu G je komponenta s lichým počtem vrcholů.* ***odd***(G) *:= počet lichých komponent v G. Pro graf $G = (V,E)$ a množinu $S \subseteq V$: $G - S = (V \setminus S, E \cap \binom{V \setminus S}{2})$.*

Věta 48 (Tutte)**.** *Pro každý $G = (V,E)$ platí G má perfektní párování $\Leftrightarrow \forall S \subseteq V$: $odd(G - S) \leq |S|$. Druhá část se nazývá Tutteova podmínka.*

Důkaz. $\Rightarrow$ Nechť G má perfektní párování M. Pro spor, nechť $\exists S \subseteq V : \mathrm{odd}(G-S) > |S|$. Potom ale z každé liché komponenty $G - S$ vede aspoň jedna hrana z M do S, tudíž $\mathrm{odd}(G - S) \leq |S|$ a to je spor. $\Leftarrow$ Nechť G splňuje Tutteovu podmínku. Pozorování: $\mathrm{odd}(G) = 0$, jinak spor $S = \emptyset$. Chci dokázat, že G má perfektní párování a to pomocí indukce podle $|\binom{V}{2} \setminus E|$.

Pro $|\binom{V}{2} \setminus E| = 0$: G je úplný graf, navíc $\mathrm{odd}(G) = 0$. Tudíž zjevně má perfektní párování. Pro $|\binom{V}{2} \setminus E| > 0 : S := \{x \in V : \deg(x) = |V| - 1\}$. Rozliším dva případy:

1. Každá komponenta $G - S$ je úplný graf: G snadno najdu perfektní párování, díky tomu, že $\mathrm{odd}(G - S) \leq |S|$.

2. Existuje komponenta Q grafu $G - S$, která není úplná. V Q lze najít dva nesousední vrcholy x,y, které mají společného souseda z Q. Protože $z \notin S, \exists w : w$ nesousedí se z. Označme $G_1 = (V, E \cup \{xy\}), G_2 = (V, E \cup \{zw\})$.

Pozorování G_1, G_2 splňují Tutteovu podmínku. Pak z indukčního předpokladu G_1 má perfektní párování M_1 a G_2 má M_2. Pokud M_1 neobsahuje hranu $\{xy\}$, tak M_1 je perfektní párování v G. Tak je to hotové.

Pokud ale $\{xy\} \in M_1$ tak podobně předpokládám, že $\{zw\} \in M_2$. Uvažme graf $H = (V, M_1 \cup M_2)$: každá komponenta H je buď hrana patřící $M_1 \cap M_2$, nebo sudá kružnice na níž se střídají hrany z M_1 a M_2. V každé komponentě H neobsahující hranu $\{xy\}$ můžu vrcholy spárovat pomocí hran M_1. Nechť C je komponenta H obsahující $\{xy\}$. Pokud C neobsahuje $\{zw\}$, vrcholy spáruji pomocí M_2, hotovo. Ve zbylém případu v C použijeme jednu z hran $\{xy\}, \{zw\}$ a zbytek lze spárovat pomocí $M_1 \setminus \{xy\}$ a $M_2 \setminus \{zw\}$. Tedy G má perfektní párování.

□

Definice 47. *Graf je d-**regulární**, pokud všechny jeho vrcholy mají stupeň d.*

Definice 48. *Graf je (vrcholově) k-**souvislý**, pokud má aspoň $k + 1$ vrcholů a nemá vrcholový řez velikosti $< k$.*

Lemma 49. *Nechť $G = (V,E)$ je graf, jehož každý vrchol má lichý stupeň, nechť $A \subseteq V$ je množina liché velikosti. Potom G obsahuje lichý počet hran z A do $V \setminus A$.*

Důkaz. $S = 2k +$ ven je součet stupňů v A. Ten musí být lichý. $2k$ je pro každou hranu, která má oba vrcholy v A. Tudíž *ven* musí být liché.

□

Věta 50 (Petersen)**.** *Každý 3-regulární a 2-souvislý graf má perfektní párování.*

Důkaz. Nechť $G = (V,E)$ je 3-regulární a 2-souvislý graf. Tvrdíme: $\forall S \subseteq V$: $\operatorname{odd}(G-S) \leq |S|$. Pro $S = \emptyset$ Tutteova podmínka platí: $|V|$ je sudá (z principu sudosti grafů) a taky souvislý $\Rightarrow$ $\operatorname{odd}(G) = 0$. $S \neq \emptyset, l :=$ $\operatorname{odd}(G-S)$ nechť $Q_1, \ldots, Q_l$ jsou liché komponenty $G - S$. Nechť p je počet hran mezi S a $Q_1 \cap \cdots \cap Q_l$. Pozorování: $p \leq 3|S|$ - plyne z toho, že je 3-regulární. Pozorování: z každé Q_i vedou aspoň 2 hrany do S to plyne z toho, že je G 2-souvislý, jinak by existovala artikulace. Pozorování: z každé Q_i vedou aspoň 3 hrany do S. To plyne z lemma. $\Rightarrow p \geq 3l \Rightarrow l \leq |S|$. A ještš použít Tutteovu větu.

$\square$

10. Kontrakce a minory

Definice 49. *Nechť $G = (V,E)$ je graf, $e = \{x,y\} \in E$ pak* ***kontrakce*** *hrany e je operace, která vrcholy x,y nahradí jedním vrcholem v_e a pro každý vrchol $z \in V \setminus \{x,y\}$ sousedící s x nebo y se hrany $\{xz\},\{yz\}$ nahradí $\{v_e z\}$. Výsledek se značí $G.e$.*

Lemma 51 (o kontrahovatelné hraně)**.** *V každém 3-souvislém grafu $G = (V,E)$, který není izomorfní K_4 existuje hrana $e \in E$ taková, že $G.e$ je opět 3-souvislý graf.*

Tvrzení 52. *Pro každou hranu $e = \{xy\} \in E$ existuje vrchol $z \in V \setminus \{x,y\}$ takový, že $G - \{x,y,z\}$ je nesouvislý, navíc každý z vrcholů $\{x,y,z\}$ má aspoň jednoho souseda v každé komponentě $G - \{x,y,z\}$.*

Důkaz. Víme, že $G.e$ není 3-souvislý, navíc $|V(G.e)| \geq 4$ jinak je to K_4, tedy existuje v $G.e$ vrcholový řez R velikosti nejvýše 2. Jistě $v_e \in R$ jinak by R byl řez v $G> R \neq \{v_e\}$ jinak by $\{x,y\}$ byl řez v G. Tedy $R = \{v_e,z\}$ a $\{x,y,z\}$ je řez v G. Kdyby např. x neměl žádného souseda v nějaké komponentě C grafu $G - \{x,y,z\}$, tak $G - \{y,z\}$ je nesouvislý, spor s tím, že G má být 3-souvislý.

□

Důkaz. Pro spor nechť $G = (V,E)$ je protipříklad. Volme $e = \{x,y\} \in E$ a vrchol $z \in V$, komponentu C grafu $G - \{x,y,z\}$ tak, aby C mělo co nejméně vrcholů. Nechť w je vrchol C sousedící se z. Pro hranu $f = \{z,w\}$ použiji pomocné tvrzení: $\exists v \in V \setminus \{z,w\} : G - \{z,w,v\}$ je nesouvislý a každá jeho komponenta obsahuje vrchol sousedící s w. Nechť D je komponenta $G - \{z,v,w\}$ neobsahující x ani y. Tedy $D \subseteq C \setminus \{w\} : D$ obsahuje souseda w, ten musí být uvnitř C, žádná cesta uvnitř D neobsahuje x,y,z,w tedy D je uvnitř jediné komponenty $G - \{x,y,z\}$, tedy D je uvnitř C, tedy i uvnitř $C \setminus \{w\}$. To je spor s minimalitou C.

□

Věta 53 (Tutteova charakterizace 3-souvislých grafů)**.** *Graf $G = (V,E)$ je 3-souvislý $\Leftrightarrow \exists$ posloupnost grafů $G_0,G_1,\ldots,G_k$, kde:*

1. $G_0 \cong K_4, G_k \cong G$.
2. $\forall i = 1,\ldots,k : G_i$ *obsahuje hranu $e = \{x,y\}$ spojující dva vrcholy x,y stupně* ≥ 3, $\deg(x) = \deg(y) = 3$ *a* $G_{i-1} \cong G_i.e$.

Proof. "$\Rightarrow$" Opakovaná aplikace lemma o kontrahovatelné hraně.

"$\Leftarrow$" Nechť $G_0,\ldots,G_k$ splňuje podmínky na pravé straně. Dokážeme, že všechny grafy $G_0,\ldots,G_k$ jsou 3-souvislé. Indukcí pdole i dokážeme, že G_i je 3-souvislý. $i = 0 : K_4$ je 3-souvislý. $i > 0$ předpokládáme, že G_{i-1} je 3-souvislý, pro spor nechť G_i není 3-souvislý, $\exists u,v \in V(G_i) : G_i - \{u,v\}$ je nesouvislý, navíc $\exists e = \{x,y\} \in E(G_i) = G_i.e = G_{i-1}$. Případy:

1. $\{u,v\} \cap \{x,y\} = \emptyset$ G_{i-1} pak není 3-souvislý. Spor.
2. $\{u,v\} = \{x,y\}$ pak G_{i-1} je 1-souvislý. Spor.

3. $|\{u,v\} \cap \{x,y\}| = 1$ BŮNO: $x = u$: nelze, protože $\deg(y) \geq 3$, tedy komponenta $G_i - \{u,v\}$ obsahující y má aspoň 2 vrcholy, tedy $G_i.e = G_{i-1}$ má řez $\{v, v_e\}$. Spor.

□

Definice 50. *Graf H je **minor** rafu G pokud H lze vyrobit z G posloupností mazání hrany, kontrakce hrany, mazání vrcholu. Značení: $H \leq_m G$.*

Definice 51. *Graf F je **dělení** grafu H, pokud F vznikne z H tak, že se každá hrana $\{x,y\} \in E(H)$ nahradí cestou délky ≥ 1.*

Definice 52. *Graf H je **topologický minor** grafu G, pokud G obsahuje nějaké dělení grafu H jako podgraf. Značení $H \leq_t G$.*

Definice 53. *Graf H je **indukovaný podgraf** grafu G, pokud je H podgraf grafu G a zároveň má všechny hrany původního grafu indukované vrcholům grafu H. Značení $H \leq_i G$. H je **podgraf** grafu G. Značení $H \subseteq G$.*

Pozorování. *Platí implikace $H \leq_i G \Rightarrow H \subseteq G \Rightarrow H \leq_t G \Rightarrow H \leq_m G$. Ale neplatí žádná opačná implikace.*

Lemma 54. *$H = (V_H, E_H)$ je graf, $V_H = \{x_1, x_2, \ldots, x_k\}, G = (V_G,E_G)$ je graf. Potom $H \leq_m G$ iff G obsahuje k disjunktních souvislých neprázdných podgrafů $B_1, B_2, \ldots, B_k$ takových, že pokud $\{x_i, x_j\} \in E_H$, tak G obsahuje aspoň jednu hranu spojující vrchol B_I s vrcholem B_j.*

Důkaz. Danou vlastnost si označíme jako vlastnost p. "$\Leftarrow$" Zkontrahuji všechny hrany v B_i. Nadbytečné hrany a vrcholy odstraním. "$\Rightarrow$" Nechť $H \leq_M G$, tj. existuje posloupnost grafů $G_0, G_1, \ldots ,G_p$, kde $H \cong G_0, G_p \cong G$ a pro $\forall i = 1, \ldots , p : G_{i-1}$ vznikne z G_i smazáním hrany nebo vrcholu anebo kontrakcí hrany. Dokážeme indukcí podle $i = 0, \ldots , p$, že G_i má vlastnost p. $i = 0 : \forall j = 1, \ldots ,k : \{x_j\} = B_j$. $i > 0$ předpokládejme G_{i-1} splňuje vlastnost p. Pak přidáním vrcholu nebo hrany - nic neděláme, zůstávají stejné. Dekontrakce hrany. Pokud není v B_j tak hotovo (zůstane stejné). Pokud ale je v B_j tak oba nové vrcholy přidáme do B_j a ostatní stejné.

□

Definice 54. *Pro uspořádání $\leq$ a množinu grafů $F = \{F_1, F_2, \ldots\}$ označím $\mathcal{F}orb_{\leq}(F) := \{G \text{ graf}, \forall H \in F : H \not\leq G\}$. (Plyne ze slova Forbidden, nebo-li zakázané.)*

Definice 55. *Třída grafů $\mathcal{G}$ je **uzavřená** vůči uspořádání $\leq$ pokud $\forall G \in \mathcal{G}\ \forall H \leq G : H \in \mathcal{G}$.*

Pozorování. *Třída $\mathcal{G}$ se dá přepsat jako $\mathcal{F}orb_{\leq}(F)$ pro nějakou množinu F iff $\mathcal{G}$ je uzavřená vůči $\leq$.*

Fakt. *Rovinné grafy jsou uzavřené vůči $\subseteq, \leq_i, \leq_t, \leq_m$.*

Připomenutí: $G = (V,E)$ rovinný, souvislý, má nakreslení mající f stěn, potom $|V| - |E| + f = 2$. Pokud $|V| \geq 3$ tak $|E| \leq 3|V| - 6$. Pokud $|V| \geq 4$ a G neobsahuje trojůhelník jako podgraf, tak $|E| \leq 2|V| - 4$.

Věta 55 (Kuratowski, Wagner)**.** *Pro graf $G = (V,E)$ je ekvivalentní:*

1. G je rovinný,

2. $G \in \mathcal{F}orb_{\leq_t}(K_5,K_{3,3})$*,*

3. $G \in \mathcal{F}orb_{\leq_m}(K_5,K_{3,3})$*.*

Proof. $1 \Rightarrow 2$: G je rovinný $\Rightarrow$ každý topologický minor je rovinný $\Rightarrow K_5 \nleq_t G \wedge K_{3,3} \nleq_t G \Rightarrow G \in \mathcal{F}\mathrm{orb}_{\leq_t}(K_5,K_{3,3})$.

$1 \Rightarrow 3$: Obdobně jako předchozí.

$3 \Rightarrow 2$: $H \leq_t J \Rightarrow H \leq_m J$ a taky $H \nleq_m J \Rightarrow H \nleq_t J$. $J \in \mathcal{F}\mathrm{orb}_{\leq_m}(H) \Rightarrow J \in \mathcal{F}\mathrm{orb}_{\leq_t}(H)$ nebo-li $\mathcal{F}\mathrm{orb}_{\leq_m}(H) \subseteq \mathcal{F}\mathrm{orb}_{\leq_t}(H)$.

$2 \Rightarrow 3$: Připomenutí: Pro graf H s maximálním stupněm ≤ 3. $H \leq_t G \Leftrightarrow H \leq_m G$. A taky $K_5 \leq_m H \Rightarrow ((K_5 \leq_t H) \vee (K_{3,3} \leq_t H))$. Pak dokážeme obměnu $(\neg 3 \Rightarrow \neg 2)$ $K_5 \leq_m G \vee K_{3,3} \leq_m G \Rightarrow K_5 \leq_t G \vee K_{3,3} \leq_m G \Rightarrow G \notin \mathcal{F}\mathrm{orb}(K_5,K_{3,3}$.

$3 \Rightarrow 1$ Indukcí podle $|V|$. $|V| \leq 4$: Jistě G ke rovinný. Předpoklad, že $|V| \geq 5$ a $G \in \mathcal{F}\mathrm{orb}_{\leq_m}(K_5,K_{3,3})$. Nechť k je vrcholová souvislost. Rozlišíme případy:

1. $k = 0$: každá komponenta je dle indukčního předpokladu rovinná $\Rightarrow G$ je rovinný.

2. $k = 1$: Lze rozdělit graf G na dva grafy G_1, G_2 podle dané artikulace x. S tím, že oba grafy mají i daný vrchol x. Podle IP jsou oba grafy rovinné, navíc jdou nakreslit tak, že x bude vždy na vnější stěně (pomocí projekce na sféru), potom je můžeme "slepit" dohromady a máme stále rovinný graf.

3. $k = 2$ Obdobně rozdělím graf na G_1, G_2 a z nich vytvořím $G_1^+ := G_1 \cup \{xy\}$ a $G_2^+ := G_2 \cup \{xy\}$. Následně tvrdím: $G_1^+, G_2^+ \in \mathcal{F}\mathrm{orb}_{\leq_m}(K_5,K_{3,3})$. G_1 i G_2 obsahuje cestu P_1 a P_2 z x do y (jinak by x nebo y obsahovalo řez).

   - $G_1^+ \leq_m G$ (dokonce $G_1^+ \leq_m G1 \cup P_2 \subseteq G$).
   - $G_1^+ \in \mathcal{F}\mathrm{orb}_{\leq_m}(K_5,K_{3,3})$ kdyby např. $K_5 \leq_m G_1^+ \leq_m G$, tak $K_5 \leq_m G$ a to je spor. Dle IP G_1^+ i G_2^+ jsou rovinné, oba se dají nakreslit tak, že hrana $\{xy\}$ je na vnější stěně. Následně pak slepím G_1^+ a G_2^+ a popřípadě smažu hranu $\{xy\}$ a získám rovinný graf.

4. $k \geq 3$: G je 3-souvislý: Fakt: v rovinném nakreslení 2-souvislého grafu je každá stěna ohraničená kružnicí. A taky lemma o kontrahovatenlné hraně: $\exists e = \{xy\} \in E$ taková, že $G.e$ je 3-souvislý, tedy $G.e - v_e$ je 2-souvislý.

   - Pozorování: $G.e - v_e = G - \{x,y\}$. Dle IP $G.e$ je rovinný. Zvolme rovinné nakreslení $G.e$. V $G.e - v_e$ je stěna, z níž byl smazán v_e ohraničená kružnicí C. Do stěny ohraničné C nakreslíme vrchol x. Každý soused v_e v grafu $G.e$ leží na C, tedy každý soused x v grafu G různý od y leží na C. Označme $N_C(x)$: sousedé x na C a podobně $N_C(y)$. Teď rozdělme případy.
     (a) $|N_C(x) \cap N_C(y)| \geq 3$: to nelze, $C \cup \{x,y\}$ indukují dělení K_5.
     (b) $\exists a_1,a_2 \in N_C(x), b_1, b_2 \in N_C(y)$: $|\{a_1,a_2,b_1,b_2\}| = 4$ leží na C v pořadí a_1, b_1, a_2, b_2: to taky nelze, pak je tam $K_{3,3}$.
     (c) Nenastane ani jedna z předchozích možností. Vrcholy $N_c(x)$ rozdělí C na cesty $P_1,P_2,\ldots,P_k, \exists j : N_C(y) \subseteq P_j$.

□

Kombinatorika a grafy III

11. Structural graph theory

Definition 1. *$H \leq_t G$ means that subdivision of H is a subgraph of G, also known as **topological minor**.*

Definition 2. *$H \leq_m G$ means that H is a **minor** of G.*

Definition 3. *$H \subseteq G$ means that H is a **subgraph** of G.*

Definition 4. *$H \sqsubseteq G$ means that H is a **induced subgraph** of G.*

Theorem 1 (Kuratowski)**.**

$$K_5, K_{3,3} \not\leq_t G \Leftrightarrow G \text{ planar}$$

$$K_5, K_{3,3} \not\leq_m G \Leftrightarrow G \text{ planar}$$

Definition 5. *$\chi(G)$ means that G has a coloring of size $\chi(G)$.*

Observation. *$C_3, C_5, C_7, \dots \not\subseteq G \Leftrightarrow \chi(G) \leq 2$ which holds also for $\sqsubseteq$.*

Observation. *$C_3 \not\leq_m G \Leftrightarrow G$ is a forest also holds for $\leq_t$.*

Definition 6. *$Forb_{leq}(\mathcal{F}) = \{G|(\forall F \in \mathcal{F})F \not\leq G\}$*

We will try to show $\mathcal{G} = Forb_{\leq_m}(\mathcal{F})$. If $G \in \mathcal{G}$ then all minors of G belong to $\mathcal{G}$.

Observation. *If $\mathcal{G} = Forb_{\leq}(\mathcal{F})$ then $\mathcal{G}$ is $\leq$-closed. Which means that $\forall G,G'$ if $G \in \mathcal{G}$ and $G' \leq G$ then $G' \in \mathcal{G}$.*

Lemma 56. *Let $\leq$ be a partial ordering of graphs. If a class $\mathcal{G}$ of graphs is $\leq$-closed, then there exist $\mathcal{F}$ s.t. $\mathcal{G} = Forb_{\leq}(\mathcal{F})$.*

Proof. $\mathcal{F} = \{F : F \not\leq G\}$. ☐

Definition 7. *F is **minimal $\leq$-obstruction** for $\mathcal{G}$ if $F \notin \mathcal{G}$ but for every $F' \lneq F$ and $F' \in \mathcal{G}$.*

Lemma 57. *Let $\leq$ be an ordering og graphs **without infinite decreasing chains**. If $\mathcal{F}$ is $\leq$-closed, then $\mathcal{G} = Forb_{\leq}(\{F : F$ is a minimal $\leq$ -obstruction for $\mathcal{G}\})$.*

Proof. $G \notin \mathcal{G}$ is min $\leq$-obstruction or $\exists G' \lneq G : G \notin \mathcal{G} \Rightarrow G'$ is obstruction or we continue and because we don't have **without infinite decreasing chains** we will eventually end. ☐

If $\mathcal{G}$ is $\leq_m$-closed, then there exists a **finite** $\mathcal{F}$ such that $\mathcal{G} = Forb_{\leq_m}(\mathcal{F})$.

Theorem 2 (Robertson-Seymor)**.** *For every F there exists an algorithm that for input graph G decides whether $F \leq_m G$ in time $O_F(|G|^3)$.*

Definition 8. *For graph $G = (V,E)$ we define $|G| = |V|$ and $||G|| = |E|$. Also for some $U \subseteq V$ $G[U]$ is a induced subgraph of G that has only vertices from U. Then $N_G(v)$ stands for the neighborhood of vertex v in graph G.*

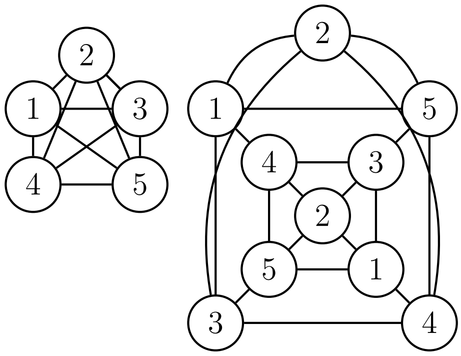


Figure 11.1: Example of G and G' as covers.

Definition 9. *G' is a **cover** of G if $(\exists f : V(G') \to V(G))\forall v \in V(G')$ for $N_{G'}(v)$ is a bijection with $N_G(f(v))$.*

Example. We may see an example 11.1:

$$\{G\text{"}\exists \text{ planar } G' \text{ cover of } G\}$$
$$\Updownarrow$$
$$F_1, \ldots, F_n \not\leq_m G$$

Contrary we take $\mathcal{G} = \{G : (\forall uv \in V(G)U \neq v, \deg(u) \geq 5, \deg(v) \geq 5)(\exists X \subseteq E(G) : |X| \leq 1)u$ and v are in different component of $G - X\}$ which is $\leq_t$-closed. But take these graphs:

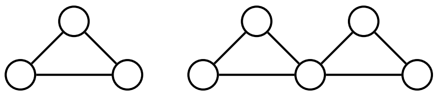


Figure 11.2: Obstructions.

Where each one of them is an obstruction. And we could create much more of them.

Now we take a look at some nice properties of graphs if we forbid some graphs as a minors.

$$\begin{array}{rcl}
K_1 \not\leq_m G & \Leftrightarrow & V(G) = \emptyset \\
K_2 \not\leq_m G & \Leftrightarrow & E(G) = \emptyset \\
K_3 \not\leq_m G & \Leftrightarrow & G \text{ is a forest} \\
 & & G \text{ is obtained from } K_1, K_2 \text{ by clique sums} \\
K_4 \not\leq_m G & \Leftrightarrow & G \text{ is obtained from } K_1, K_2, K_3 \text{ by clique sums}
\end{array}$$

Definition 10. *Graph G can be obtained from G_1 and G_2 by **clique-sum** if the intersection that these graphs have in G form a clique. In other way it is that we bind together two graphs by identifying their vertices and edges in the same size clique.*

Observation. *If G is obtained from G_1 and G_2 by a clique-sum then:*

$$K_m \leq_m G \Leftrightarrow K_m \leq_m G_1 \vee K_m \leq_m G_2$$

Lemma 58. *If $K_k \leq_m G$ and G is the clique-sum of G_1 and G_2 then $K_k \leq_m G_1 \vee K_k \leq_m G_2$.*

Lemma 59. *If G is not 3-connected then there exist $G_1, G_2 \lneq_m G$ s.t. G is a clique-sum of G_1 and G_2.*

Proof. If G is not connected then it is done since it is a clique sum on K_0. If G is connected, but not 2-connected then it is a clique-sum on K_1 since there exist a articulation. If G is 2-connected then there must be two vertices which splits the graph. And these two vertices form a K_2 as a minor. That is because we split G to two parts where we leave the major one side and add a edge to these two vertices, which we can do because they need to have a path between them so we contract all the edges alongside the path. □

Definition 11. *$\delta(G)$ is a minimum degree of a graph G.*

Theorem 3. *If G is K_4-minor-free then G is obtained from $K_{\leq 3}$'s by clique-sums.*

Proof. By induction on $|V(G)|$.

(a) If G is not 3-connected. G is a clique-sum of G_1,$G_2 \lneq_m G$. Since $K_4 \nleq_m G_1$ and $K_4 \nleq_m G_2$ we use induction hypothesis and we are done.

(b) If G is 3-connected. If $|V(G)| \leq 3$, then $G = K_{\leq 3}$, wlog $|V(G)| \geq 4$. $\delta(G) > 1 \Rightarrow G$ contains a cycle. Let C be a shortest cycle in G. C is induced in G 3-connected $\Rightarrow G \neq C$ so $\exists v \in V(G) \setminus V(C)$. By Merger's theorem there exists three paths from v to C intersecting only in v. That gives us K_4 as a minor of the graph. Which is contradiction.

□

$$K_5 \nleq_m G \quad \Leftrightarrow \quad G \text{ is obtained from planar graphs and } W_8 \text{ by clique sums}$$

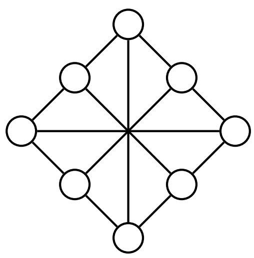


Figure 11.3: W_8 graph.

Observation. *If G is a clique-sum of G_1 and G_2 then*

$$\chi(G) \leq \max(\chi(G_1), \chi(G_2))$$

Proof. We just need to match the coloring of the cliques. Other than that we don't have any problem. □

11.1 Hadwiger's conjecture

K_t-minor-free graphs are $(t-1)$ colorable.

$$\begin{array}{lll} K_1 \not\leq_m G & \chi \leq 1 & \delta \leq 0 \\ K_2 \not\leq_m G & \chi \leq 2 & \delta \leq 1 \\ K_3 \not\leq_m G & \chi \leq 3 & \delta \leq 2 \\ K_4 \not\leq_m G & \chi \leq 4 & \delta \leq 5 \\ K_5 \not\leq_m G & \chi \leq 5 & \end{array}$$

Theorem 4. *$\exists f$ every K_t-minor-free graph G has $\delta(G) \leq f(t)$.*

The function is somewhere near $f(t) = (1{,}6 \cdots + O(1))t\sqrt{\log t}$. But we won't show this result. Instead we will show $f(t) = O(t^2)$. Before we continue it is better to remind ourselves **chordal graph** and **elimination ordering** (known as PES).

Definition 12 (Chordal decomposition of G)**.** *$V(G) = \mathcal{P}_1 \dot\cup \mathcal{P}_2 \dot\cup \ldots \dot\cup \mathcal{P}_n \dot\cup$ and*

1. *$(\forall i) G[\mathcal{P}_i]$ is connected.*
2. *"$\mathcal{P}_i$'s form elimination ordering" Precisely: $(\forall i \in [n])(forall j_1,j_2 < i)$ if G has an edge between $\mathcal{P}_i$ and $\mathcal{P}_{j_1}$ and also between $\mathcal{P}_i$ and $\mathcal{P}_{j_2}$ then it also has an edge between $\mathcal{P}_{j_1}$ and $\mathcal{P}_{j_2}$.*

Definition 13. *Chordal partition is **geodesic** if $(\forall i)(\exists v_i \in \mathcal{P}_i)$ s.t. if $v_1, \ldots, v_t < i$ are the indices s.t. G has an edge between $\mathcal{P}_i$ and $\mathcal{P}_{j_1}, \mathcal{P}_{j_2}, \ldots, \mathcal{P}_{j_t}$ then $v_1, \ldots, v_t \in \mathcal{P}_i$ s.t. v_i has a neighbor in $\mathcal{P}_{j_1}, \mathcal{P}_{j_2}, \ldots, \mathcal{P}_{j_t}$ and $G - \bigcup_{j<i} \mathcal{P}_j$ contains shortest paths from v_i to $v_1, \ldots, v_t$ which cover all vertices in $\mathcal{P}_i$.*

Theorem 5. *Every graph has a geodesic chordal partition.*

Before we show us a proof we will take a look at a simple application. If G is K_k-minor-free last part has neighbours in $t \leq k-2$ parts (otherwise it will have K_k as a minor). Then we may take a look at a $\deg(v) \leq (k-2) + (k-2)(k-2)3 \leq 3k^2$. Thus getting the upper bound $\delta(G) \leq 3k^2$.

Definition 14. *Part is called **terminal** if there is no edge from any vertex in that part going to some vertex in one of the parts on the right.*

Proof. Let $\mathcal{P}$ be a chordal decomposition of G into parts satisfying both properties of definition of chordal decomposition (i) abd (ii) and geodesity (iii) for all non-terminal parts.

This can be easily done by creating parts based on the components of connectivity. For them all properties hold, since they are all connected and "chordal" property is also satisfied since there are no edges. Also all of them are terminal (iii) doesn't have to be satisfied.

Now we proof by that by choosing $\mathcal{P}$ with largest number of parts. Lets say that there is a part that does not satisfy (iii). This means that it is terminal part. Lets take vertex from the part and find the shortest paths to the vertices that are connected to some of the parts to the left. Now we put vertices to separate components and these components will make a new parts. We will also remove all these vertices from the origin part. Note that all properties are satisfied. (i) is trivial. (ii) If there are any vertices from the new parts to other parts then they are to the ones which are already connected to the origin part, which satisfied (ii) before so it is fine. Also (iii) is satisfied.

The thing is that we created $\mathcal{P}$ with larger number of parts which is contradiction. $\square$

Observation. $H \leq_t G \Rightarrow H \leq_m G$

Observation. $\Delta(H) \leq 3 : H \leq_m G \Rightarrow H \leq_t G$

Lets remind ourselves a table and add some new thinks.

$$
\begin{array}{lcl}
K_1 \not\leq_t G \Leftrightarrow K_1 \not\leq_m G & \Leftrightarrow & V(G) = \emptyset \\
K_2 \not\leq_t G \Leftrightarrow K_2 \not\leq_m G & \Leftrightarrow & E(G) = \emptyset \\
K_3 \not\leq_t G \Leftrightarrow K_3 \not\leq_m G & \Leftrightarrow & G \text{ is a forest} \\
 & & G \text{ is obtained from } K_1, K_2 \text{ by clique sums} \\
K_4 \not\leq_t G \Leftrightarrow K_4 \not\leq_m G & \Leftrightarrow & G \text{ is obtained from } K_1, K_2, K_3 \text{ by clique sums} \\
K_5 \not\leq_t G \not\Leftrightarrow K_5 \not\leq_m G & \Leftrightarrow & G \text{ is obtained from planar graphs and } W_8 \text{ by clique sums}
\end{array}
$$

Well technically $K_5 \not\leq_t G \Rightarrow K_5 \not\leq_m G$ but the other way around is what doesn't work $K_5 \not\leq_m G \not\Rightarrow K_5 \not\leq_t G$. For that we can see an example 11.4. We may see that $\mathcal{G} = \{G : G \text{ has } \leq 4 \text{ vertices of degree } \geq 4\}$ these graphs are so that $K_5 \not\leq_t G$.

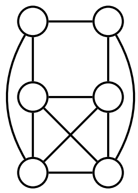


Figure 11.4: A counter example.

11.2 Hájos conjecture

If we remember Headwiger's conjecture then Hájos conjecture is the same only with topological minors. Thus it is that $K_t \leq_t G \Rightarrow \chi(G) \leq t - 1$. This is actually true for $t < 4$ but it is false for $t \geq 7$ and 5,6 are open questions.

Theorem 6. $\exists f_m(k) = O(k\sqrt{\log k})$ *Every K_k-minor-free graph G satisfies $\delta(k) \leq f_m(k)$.*

We won't proof this, but we will proof something similiar, that is for topological minors.

Theorem 7. $\exists f_t(k) = O(k^2)$ *Every G s.t. $K_k \lneq_t G$ satisfies $\delta(G) \leq f_t(k)$.*

The corollary to this is that $\chi)G_{\leq} f_t(k) + 1$. We will proof this theorem, but to do that we need to do some steps beforehand.

Firstly imagine that the enemy gives you a graph and you need to prove that. But the enemy is kind enough to give you a graph H with connectivity $>> k^2$. We could apply Merger's theorem. Though this will only give certain number of vertex disjoint paths from one vertex to another. We would more likely have this many paths between more pairs of sources and targets.

Definition 15. *Graph G is k-**linked** if $|V(G)| \geq 2k$ and $\forall s_1, s_2, \ldots, s_k, t_1, t_2, t_k$ distinct vertices of G. G contains pairwise vertex-disjoint paths $P_1, P_2, \ldots, P_k$. When P_i has ends s_i and t_i.*

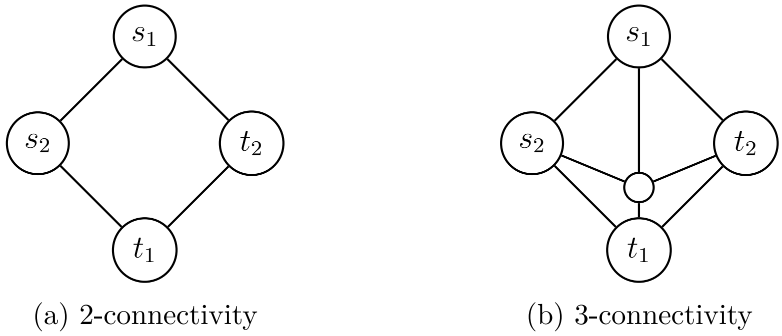


Figure 11.5: A counter example to 2-linked graphs.

We may see that there exist a graph that is 2-connected and yet not 2-linked. You may see this on the picture 11.5a. Also not even 3-connected graph has to be 2-linked. Which is also on the picture 11.5b (though we can change the vertex inside for any planar graph). We could continue and end up with that not even 5-connectivity forces 2-linked.

Observation. *Every k-linked graph is $(2k-1)$ connected.*

Proof. That is simply because we put all the s_i, t_i for $i \in [k-1]$ to the edge cut and then choose s_k in the left part and t_k in the right part then we can see that it is indeed $(2k-1)$-connected. ☐

Theorem 8. *If G is $2k$-connected, $K_{4k} \leq_m G$ then G is k-linked.*

Proof. Next week... ☐

Corollary. If G is $\max(2k, f_m(4k)+1)$-connected then G is K-linked.

Proof. We use the theorem to get that $\delta > f_m(4k)$ thus $K_{4k} \leq_m G$. ☐

Also we can say $\exists f_l(k) = O(k\sqrt{\log k})$. If G is $f_l(k)$-connected then G is k-linked.

Corollary. If G is $f_l\left(\frac{k(k-1)}{2}\right)$-connected then $K_k \leq_t G$.

Proof. To see this we choose k vertices and for every one of them $k-1$ neighbors. Then we give s_i and t_i to every single one of these vertex so that every neighborhood has pair with all others. Then we find such paths between them. ☐

Lemma 60. *If $\bar{d}(G) \geq 4d$ then G contains a $(d+1)$-connected subgraph H of minimum degree $2d+1$.*

Proof. Let H be a minimal subgraph of G s.t. $|V(H)| \geq 2d$ and $|E(H)| > 2d(|V(H)|-d)$. We may see that $|V(H)| > 2d$ that is if it has $2d$ vertices then

$$\frac{2d^2-d}{2} = \binom{2d}{2} > |E(H)| > 2d^2$$

which is a contradiction.

Then we also have that $\delta(H) \geq 2d+1$. If we have $\delta(H) \leq 2d$ we may remove the certain vertex. But we need to show that given properties still hold. We will split the graph to two parts $|A|, |B| \geq 2d+2 > 2d$. Then

$$\begin{aligned}
|E(G)| &\leq |E(A)| + |E(B)| \\
(1) &\leq 2d(|V(A)| - d) + 2d(|V(A)| - d) \\
&= 2d(|V(A)| + |V(B)| - 2d) \\
&= 2d(|V(H)| - |V(A \cap B)| - 2d) \\
|E(G)| &> 2d(|V(H)| - d)
\end{aligned}$$

Where (1) is due to the minimality of H. The thing is with the last two lines we get that $|A \cap B| > d$. $\square$

Proof. This actually is enough for the theorem to be proven since the enemy doesn't have to be kind anymore. $\square$