

Diskrétní a spojitá optimalizace

poznámky

Tomáš Sláma
10. 1. 2022

*Toto PDF bylo automaticky vygenerováno (5. prosince 2025) z webové stránky
<https://slama.dev/poznamky/diskretni-a-spojita-optimalizace>,
která je preferovaný způsob jak dokument číst. Za případné chyby způsobené převodem se omlouvám.*

Obsah

Úvodní informace	2
Diskrétní optimalizace	2
Matroidy	2
Grafy a matroidy	3
Řádové funkce	4
Hladový algoritmus	7
Operace na matroidech	9
Dualita matroidu	11
Perfektní párování	12
Generující funkce magic	14
Poštáci a cestující	16
Spojité optimalizace	17
Zkouška	17
Diskrétní část	17
Spojité část	17
Odkazy	17
Poděkování	17

Úvodní informace

Tato stránka obsahuje moje poznámky z přednášky Martina Loebla a Milana Hladíka z akademického roku 2021/2022 | MFF (MFF UK). Pokud by byla někde chyba/nejasnost, nebo byste rádi něco přidali, tak stránku můžete upravit [pull requestem](#) (případně mi dejte vědět na mail).

Diskrétní optimalizace

Matroidy

Definice (matroid) je dvojice $(X, \mathcal{S})$, kde X je konečná množina, $\mathcal{S} \subseteq 2^X$ splňující

1. $\emptyset \in \mathcal{S}$
 2. **dědičnost:** $(\forall A \in \mathcal{S}) A' \subseteq A \implies A' \in \mathcal{S}$
 3. **výměnný axiom:** $(\forall U, V \in \mathcal{S}) |U| > |V| \implies (\exists u \in U \setminus V) V \cup \{u\} \in \mathcal{S}$
 - $(3') : A \subseteq X \implies$ všechny maximální $(\subseteq)$ podmnožiny A v $\mathcal{S}$ mají stejnou velikost
- prvkům $\mathcal{S}$ říkáme **nezávislé množiny**
 - **maximálním** nezávislým množinám (co do inkluze) říkáme **báze**

Poznámka: Při definici matroidu je dobré si představit graf. X je tu množina hran a $\mathcal{S}$ všechny acyklické podgrafy. Pak podmínka dědičnosti říká, že acyklické podgrafy jsou rovněž acyklické a axiom $3'$ to, že maximální kostry (co do inkluze) mají stejnou velikost.

Lemma (stejná definice) Axiomy $(1, 2, 3)$ a $(1, 2, 3')$ definují stejný objekt.

Důkaz: $(3) \implies (3')$ sporem:

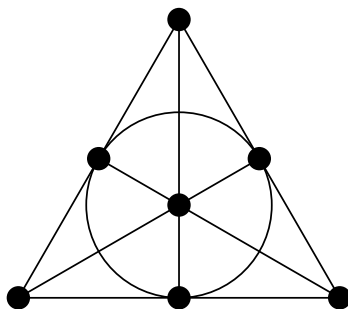
- nechť platí (3) ale existuje $A \subseteq X$ t. ž. pro nějaké $U, V \subseteq \mathcal{S}$ platí $U, V \subseteq A$, U, V jsou do inkluze maximální ale $|U| > |V|$
- díky (3) $(\exists u \in U \setminus V)$ t. ž. $V \cup \{u\} \in \mathcal{S}$, což je spor s maximalitou V .

Důkaz: $(3') \implies (3)$ sporem:

- nechť $U, V \in \mathcal{S}$ a $|U| > |V|$ a V je maximální (negace výměnného axiomu)
- definujme $A = U \cup V \subseteq X$; pak V je maximální ale $|U| > |V|$, což je spor

Příklad:

1. **vektorový matroid:**
 - nechť M je matice nad tělesem $\mathbb{F}$ s řádky C
 - $\mathcal{V}_M = (C, \mathcal{S})$, kde
 - $A \in \mathcal{S} \iff A \subseteq C$ je lineárně nezávislá v $\mathbb{F}$
 - $3'$ vyplývá přímo ze Steinitzovy věty o výměně, zbytek přímo z definice
2. **grafový matroid:**
 - mějme graf $G = (V, E)$
 - $\mathcal{M}_G = (E, \mathcal{S})$, kde
 - $A \in \mathcal{S} \iff A \subseteq E$ a A je acyklická
 - $(1) : \emptyset \in \mathcal{S}$
 - $(2) : \text{podmnožina acyklické je rovněž acyklická}$
 - $(3) : \text{počítání přes to, kolik hran je v komponentách souvislosti}$
3. **Fanova rovina:**
 - za X uvažíme body Fanovy roviny a za báze trojprvkové množiny bodů neležící na jedné přímce (v rámci Fanovy roviny – kružnice uprostřed je také přímka)

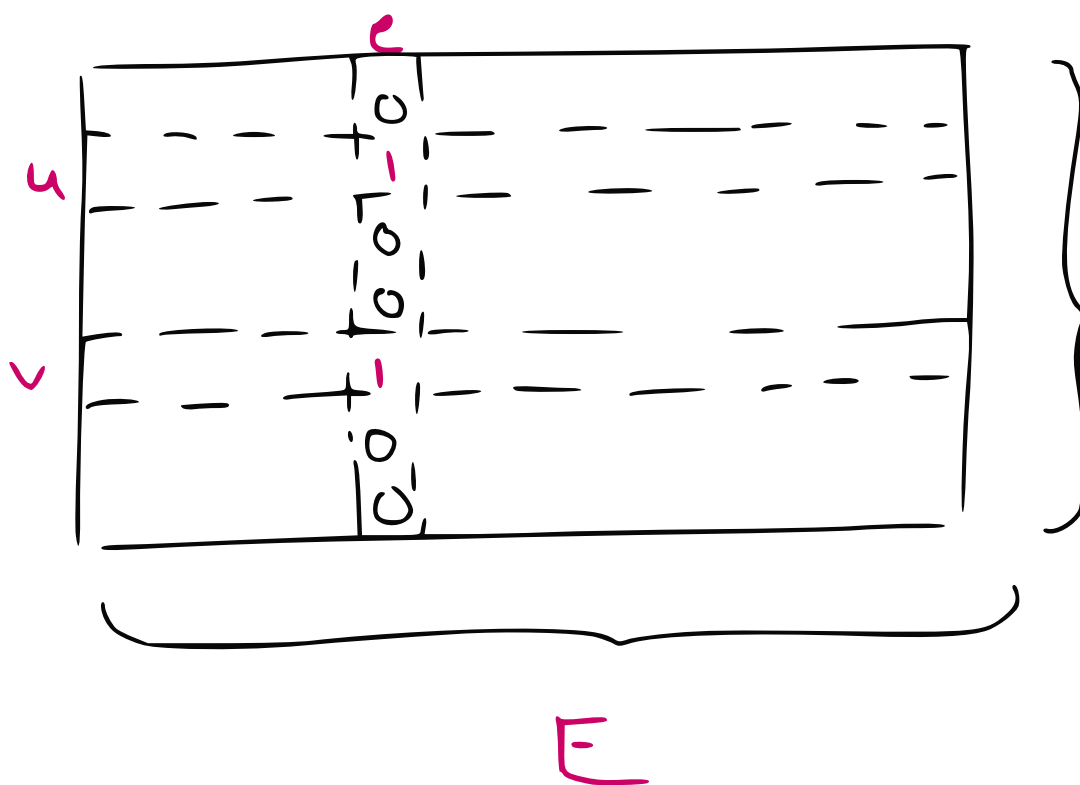


Grafy a matroidy

Definice (sudá podmnožina hran) podmnožina hran $E' \subseteq E$ je sudá, právě když $H = (V, E')$ má pouze sudé stupně.

Definice (matice incidence) grafu $G = (V, E)$ je matice $I_G \in \mathbb{F}_2^{|V| \times |E|}$ t.ž.

$$(I_G)_{v,e} = \begin{cases} 1 & v \in e \\ 0 & \text{jinak} \end{cases}$$



Definice (jádro matice incidence) pro matici incidence I_G definujeme jádro jako

$$\text{Ker}_{\mathbb{F}_2} I_G = \left\{ \mathbf{x} \in \mathbb{F}_2^{|E|} \mid I_G \mathbf{x} = \mathbf{0} \right\}$$

Definice (charakteristický vektor) mějme nosnou množinu X a podmnožinu $A \subseteq X$. Charakteristický vektor A je $\chi_A \in \{0, 1\}^{|X|}$ t.ž.

$$(\chi_A)_k = \begin{cases} 1 & k \in A \\ 0 & k \notin A \end{cases}$$

(☹☹): řádek matice incidence I_G indexovaný vrcholem w je roven $\chi_{\underbrace{N(w)}_{\text{okolí}}}$

(☹☹) (**prostor cyklů**) jádro matice můžeme ekvivalentně vyjádřit jako

$$\text{Ker}_{\mathbb{F}_2} I_G = \left\{ x \in \mathbb{F}_2^{|E|} \mid x = \chi_{E'} \text{ pro } E' \text{ sudou} \right\}$$

Tuto množinu rovněž nazýváme **prostor cyklů**.

Řádové funkce

Definice (řádová funkce) mějme systém podmnožin $(X, \mathcal{S})$, $\mathcal{S} \subseteq 2^X$ a $A \subseteq X$. Pak řádovou funkci $r : 2^X \mapsto \mathbb{N}$ definujeme jako **velikost maximální podmnožiny patřící do $\mathcal{S}$** :

[1]

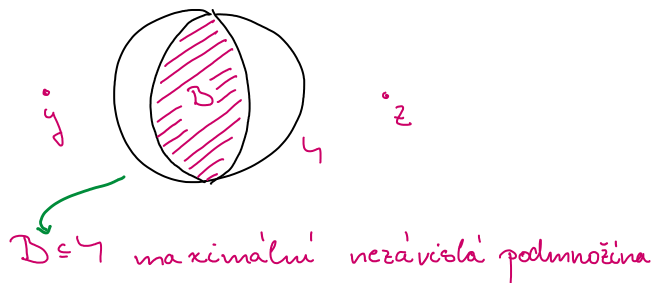
$$r(A) = \max \{ |X| \mid X \in 2^A \wedge X \in \mathcal{S} \}$$

Věta (řádová funkce matroidu) funkce $r : 2^X \mapsto \mathbb{N}$ je řádová funkce nějakého matroidu nad X právě tehdy, když platí:

- (R1): $r(\emptyset) = 0$
- (R2): $r(Y) \leq r(Y \cup \{y\}) \leq r(Y) + 1$
- (R3): $r(Y \cup \{y\}) = r(Y \cup \{z\}) = r(Y) \implies r(Y) = r(Y \cup \{y, z\})$

Důkaz ($\Rightarrow$) ukážeme přímo:

- (R1): max. nezávislá podmnožina $\emptyset$ je $\emptyset$ a $|\emptyset| = 0$
- (R2): z definice řádové funkce a dědičnosti matroidu
- (R3): nechť B je max. nez. podm. Y a $\tilde{B}$ je max. nez. podm. $Y \cup \{y, z\}$ t.ž. $B \subseteq \tilde{B}$



Pokud $|B| = |\tilde{B}|$, pak platí R3

- jinak $B \subsetneq \tilde{B}$, BUNO například $y \in \tilde{B}$
– $B \cup \{y\}$ je nezávislá a $r(Y) < r(Y \cup \{y\})$ a předpoklad implikace v R3 neplatí

Důkaz ($\Leftarrow$) z X konstruujeme matroid s řádovou funkcí r . Matroid definujeme jako

$$\mathcal{M} = (X, \mathcal{S}) \quad \text{t.ž.} \quad A \in \mathcal{S} \iff |A| = r(A)$$

Ukážeme, že $(X, \mathcal{S})$ je matroid:

1. $\emptyset \in \mathcal{S}$ (triviálně)
2. pro spor předpokládejme, že dědičnost neplatí
 - existuje tedy $A \in \mathcal{S}$, $A' \subseteq A$ ale $|A'| > r(A')$ (menší nemůže být z definice řádové funkce, jelikož je pro množinu definována jako velikost nějaké její podmnožiny)

$$\begin{aligned} r(A) &\leq r(A') + |A \setminus A'| & \text{R2} \\ &< |A'| + |A \setminus A'| \\ &= |A| \implies A \notin \mathcal{S} \end{aligned}$$

[1] V řeči grafů chceme pro libovolnou množinu hran (prvků podmnožin) vrátit největší acyklický podgraf (prvek matroidu).

3. pro spor předpokládejme, že $\exists U, V \in \mathcal{S}$ t.ž. $|U| > |V|$ ale $\forall x \in U \setminus V : V \cup \{x\} \notin \mathcal{S}$
- přes R3 získáváme ($\forall x, y \in U \setminus V$):

$$\begin{aligned} r(V) &= r(V \cup \{x\}) = r(V \cup \{y\}) \\ &\Rightarrow r(V \cup \{x, y\}) \\ &\Rightarrow r(V \cup (U \setminus V)) = r(U \cup V) \geq r(U) = |U| \end{aligned} \quad \text{R3}$$

Poznámka (alternativní znění důkazu 2) díky R2 víme, že odebráním prvku z A se může $r(A)$ buď o 1 snížit, nebo zůstat stejný. Zůstat stejný být však nemůže (z definice řádové funkce), musí se tedy o 1 snížit a v tom případě je rovněž v $\mathcal{S}$.

Věta (řádová funkce a submodularita) $r : 2^X \mapsto \mathbb{N}$ je řádová funkce matroidu $\iff$

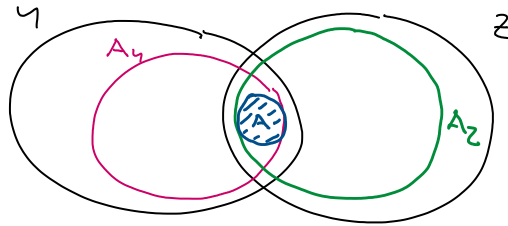
- (R1') : $\forall Y \in X : 0 \leq r(Y) \leq |Y|$
- (R2' – monotonie) : $Z \subseteq Y \subseteq X \implies r(Z) \leq r(Y)$
- (R3' – submodularita) : $r(Y \cup Z) + r(Y \cap Z) \leq r(Y) + r(Z)$

Důkaz ($\Rightarrow$ R1' a R2')

- (R1') : mějme $Y \subseteq X$
 - $r(Y) \geq 0$ (funkce je definována na $\mathbb{N}$)
 - $r(Y) \leq |Y|$ (max. nezávislá množina je z definice menší než její množina)
- (R2') : přímo vylývá z R2 ($r(A) \leq r(A \cup \{x\})$)

Důkaz ($\Rightarrow$ R3')

- A – maximální nezávislá množina v $Y \cap Z$
- A_Y – maximální nezávislá množina v Y t.ž. $A \subseteq A_Y$ (nějaká taková existuje)
- A_Z – maximální nezávislá množina v Z t.ž. $A \subseteq A_Z$ (nějaká taková existuje)

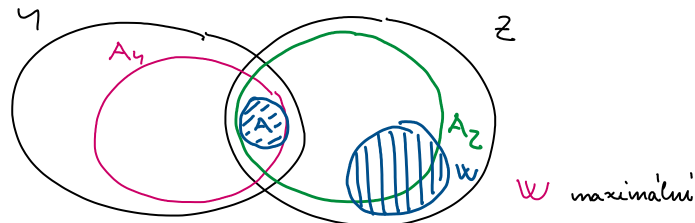


Máme

$$\begin{aligned} r(Y) + r(Z) &= |A_Y| + |A_Z| && \text{definice} \\ &= |A_Y \cap A_Z| + |A_Y \cup A_Z| && \text{inkluzi/exkluzi} \\ &\geq r(Y \cap Z) + |A_Y \cup A_Z| && A \subseteq A_Y \cap A_Z \end{aligned}$$

K důkazu tvrzení zbývá ukázat, že $|A_Y \cup A_Z| \geq r(Y \cup Z)$.

(☹☹): A_Y nemůže být rozšířené více než $A_Z \setminus Y$ prvky na nezávislou množinu v $Y \cup Z$



- pro spor předpokládejme, že $W \subseteq Z \setminus Y$ maximální, $A_Y \cup W$ je nezávislá a $|W| > |A_Z \setminus Y|$; pak ale $|W \cup A| > |A_Z|$, což je spor s maximalitou A_Z

Nyní můžeme dokončit důkaz:

$$\begin{aligned} r(Y \cup Z) &\leq |A_Y| + |A_Z \setminus Y| \\ &\leq |A_Y \cup A_Z| \end{aligned}$$

Důkaz (matroid $\Leftarrow$ R1', R2', R3') ukážeme R1, R2, R3

- (R1): dokazujeme $r(\emptyset) = 0$
 - nechť pro spor $r(\emptyset) > 0$; pak $|\emptyset| \geq r(\emptyset) > 0$, což je spor
- (R2): dokazujeme $r(Y) \leq r(Y \cup \{y\}) \leq r(Y) + 1$
 - mějme $Y \subseteq X$, $y \in X$ a $y \notin Y$ (jinak platí triviálně)
 - * první nerovnost (z monotonie):

$$Y \subseteq Y \cup \{y\} \implies r(Y) \leq r(Y \cup \{y\})$$

* druhá nerovnost (ze submodularity):

$$r(Y \cup \{y\}) + \overbrace{r(Y \cap \{y\})}^0 \leq r(Y) + r(\{y\}) \leq r(Y) + 1$$

- (R3): dokazujeme $r(Y \cup \{y\}) = r(Y \cup \{z\}) = r(Y) \implies r(Y) = r(Y \cup \{y, z\})$
 - z monotonie dostáváme první část: $Y \subseteq Y \cup \{y, z\} \implies r(Y) \leq r(Y \cup \{y, z\})$
 - nyní použijeme submodularitu na $A = Y \cup \{y\}$, $B = Y \cup \{z\}$
 - * předpokládáme, že $y \neq z$ a že $x, y \notin Y$, jinak platí triviálně

$$r(\underbrace{Y \cup \{y, z\}}_{A \cup B}) + r(\underbrace{Y}_{A \cap B}) \leq r(\underbrace{Y \cup \{y\}}_A) + r(\underbrace{Y \cup \{z\}}_B)$$

* pokud tedy platí $r(Y \cup \{y\}) = r(Y \cup \{z\}) = r(Y)$, tak dostáváme druhou část:

$$r(Y \cup \{y, z\}) \leq r(Y)$$

(☹☹): matroidy jsou systémy podmnožiny, kde řádová funkce je **monotonní** a **submodulární**.

Definice (marginální hodnota) Mějme množinu X a funkce $f : 2^X \mapsto \mathbb{N}$. Pak $\forall x \in X$ definujeme $\Delta f_x : 2^X \mapsto \mathbb{Z}$:

$$T \subseteq X \implies \Delta f_x(T) = f(T \cup \{x\}) - f(T)$$

[2]

Věta (marginální hodnota a submodularita) $f : 2^X \mapsto \mathbb{N}$ je submodulární $\iff \forall x \in X : \Delta f_x$ je nerostoucí

- nerostoucí myslíme následně: $T' \subseteq T, x \notin T \implies \Delta f_x(T') \geq \Delta f_x(T)$
 - menším množinám záleží (oproti větším) víc na přidání prvku, který nemají

Důkaz: Je-li f nerostoucí, pak $\forall U, y, z$ platí

$$\underbrace{f(U \cup \{y, z\}) - f(U \cup \{y\})}_{\Delta f_z(U \cup \{y\})} \leq \underbrace{f(U \cup \{z\}) - f(U)}_{\Delta f_z(U)}$$

Tedy f je nerostoucí $\iff \forall U \subseteq X$ a $y, z \in X \setminus U$ platí

$$f(\underbrace{U \cup \{y\}}_A) + f(\underbrace{U \cup \{z\}}_B) \geq f(\underbrace{U \cup \{y, z\}}_{A \cup B}) + f(\underbrace{U}_{A \cap B}) \quad *$$

To je skoro submodularita!

Důkaz ($\Rightarrow$) platí přímo z definice submodularity (prostě tam dosadíme)

Důkaz ($\Leftarrow$) dokazujeme $* \implies$ submodularita. Chceme

$$f(Y) + f(Z) \geq f(Y \cup Z) + f(Y \cap Z)$$

- definujeme $S = Y \cap Z$, $A = Y \setminus S$ a $B = Z \setminus S$, pak
 - $Y = S \cup A$
 - $Z = S \cup B$
 - $Y \cup Z = S \cup A \cup B$

[2] „Jak cením přidání x , když mám T .“

$$- Y \cap Z = S$$

- zkonstruujeme $f(Y)$ a $f(Z)$ z $f(S)$ za pomoci posloupností marginálních hodnot:

- rozepišme definici marginální hodnoty jako $f(X \cup \{y_1\}) = f(X) + \Delta f_{y_1}(X)$
 * dvojím rozepsáním dostaneme:

$$f(X \cup \{y_1, y_2\}) = f(X \cup \{y_1\}) + \Delta f_{y_2}(X \cup \{y_1\}) = f(X) + \Delta f_{y_1}(X) + \Delta f_{y_2}(X \cup \{y_1\})$$

- * opakovaným rozepsáním pro $Y = \{y_1, y_2, \dots, y_k\}$ dostaneme:

$$f(X \cup Y) = f(X) + \sum_{i=1}^k \Delta f_{y_i}(X \cup \{y_1, \dots, y_{i-1}\})$$

- zafixujeme pořadí prvků v $A \cup B$: $a_1, a_2, \dots, a_k$ $ABNO(A = \{a_1, \dots, a_r\})B = \{a_{r+1}, \dots, a_k\}$, potom:

$$f(Y) = f(S \cup A) = f(S) + \sum_{i=1}^r \Delta f_{a_i}(S \cup \{a_1, \dots, a_{i-1}\})$$

$$f(Z) = f(S \cup B) = f(S) + \sum_{i=r+1}^k \Delta f_{a_i}(S \cup \{a_{r+1}, \dots, a_{i-1}\})$$

$$f(Y \cup Z) = f(S \cup A \cup B) = f(S) + \sum_{i=1}^k \Delta f_{a_i}(S \cup \{a_1, \dots, a_{i-1}\})$$

- pro každé $i = 1, \dots, r$ platí, že $S \cup \{a_1, \dots, a_{i-1}\} \subseteq S \cup \{a_1, \dots, a_{i-1}\} \cup \{a_{r+1}, \dots, a_k\}$, takže:

$$\Delta f_{a_i}(S \cup \{a_1, \dots, a_{i-1}\}) \geq \Delta f_{a_i}(S \cup \{a_1, \dots, a_{i-1}, a_{r+1}, \dots, a_k\})$$

- stejně pro každé $i = r+1, \dots, k$ máme:

$$\Delta f_{a_i}(S \cup \{a_{r+1}, \dots, a_{i-1}\}) \geq \Delta f_{a_i}(S \cup \{a_1, \dots, a_{i-1}\})$$

- součtem obou stran dostaneme:

$$\begin{aligned} f(Y) + f(Z) &= f(S \cup A) + f(S \cup B) \\ &= f(S) + \sum_{i=1}^r \Delta f_{a_i}(S \cup \{a_1, \dots, a_{i-1}\}) \\ &\quad + f(S) + \sum_{i=r+1}^k \Delta f_{a_i}(S \cup \{a_{r+1}, \dots, a_{i-1}\}) \\ &\geq f(S) + \sum_{i=1}^k \Delta f_{a_i}(S \cup \{a_1, \dots, a_{i-1}\}) + f(S) \\ &= f(S \cup A \cup B) + f(S) \\ &= f(Y \cup Z) + f(S) \end{aligned}$$

Hladový algoritmus

Definice (úloha kombinatorické optimalizace) je dán množinový systém $(X, \mathcal{S})$ a váhová funkce $w : X \mapsto \mathbb{Q}$.
Úloha kombinatorické optimalizace je najít $A \in \mathcal{S}$ t.ž.

$$w(A) = \sum_{v \in A} w(v) = w^T \chi_A$$

je **maximální** (χ_A je charakteristický vektor A , který je 1 pro $v \in A$ a 0 jindy).

Příklad:

1. maximální párování v G
2. minimální Hamiltonovská kružnice
3. minimální hranový řez

Algoritmus (hladový) necht' že $w_1 \geq \dots \geq w_n$ a $m = \max \{i \in X \mid w_i \geq 0\}$; pak:

1. nastav $J = \emptyset$
2. pro $i = \{1, \dots, n\}$
 - je-li $J \cup \{i\} \in \mathcal{S}$, pak i přidej do J
3. vrať J

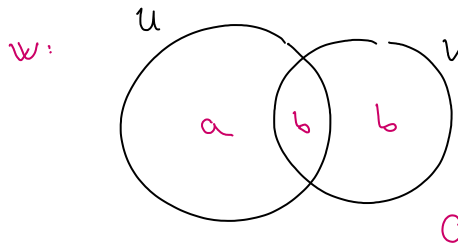
(☹☹): algoritmus je polynomiální (pro rozumné předpoklady na reprezentaci matroidu).

(☹☹): pro výše uvedené příklady nemusí algoritmus vrátit optimální řešení.

Věta (hladový algoritmus na matroidech) necht' $(X, \mathcal{S})$ je dědičný množinový systém a $\emptyset \in \mathcal{S}$. Pak hladový algoritmus vyřeší správně úlohu kombinatorické optimalizace pro **každou funkci** $w \iff (X, \mathcal{S})$ je matroid.

Důkaz ($\Rightarrow$) obměnou: necht' $(X, \mathcal{S})$ není matroid $\implies$ HA nefunguje. Zkonstruujeme $w : X \mapsto \mathbb{Q}$, na které algoritmus selže.

Jelikož $(X, \mathcal{S})$ není matroid, tak neplatí 3, 3' a tedy $\exists U, V \in \mathcal{S}, |U| > |V|$ a U, V jsou max. nezávislé množiny. Pak definujeme w následně (pro $b, a \in \mathbb{Q}, b > a > 0$):



V takovém případě hladový algoritmus najde U , ikdyž V je větší.

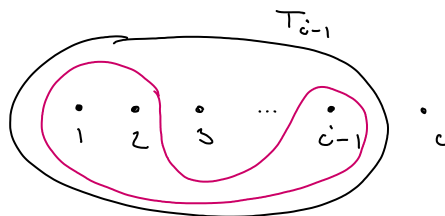
Důkaz ($\Leftarrow$) nejprve dokážeme pomocné lemma.

Lemma: mějme $w_1 \geq \dots \geq w_n, m \leq n$ maximální t.ž. $w_m > 0$, množiny $T_i \subseteq \{0, 1\}^i$ a z' je **charakteristický vektor výsledku HA** (rozumíme tím, že je to 0/1 vektor podle toho, které prvky HA vybral s tím, že jsou seřazené podle w). Pak $\forall i$ platí

$$z'(T_i) = \sum_{i \in T_i} z'_i = r(T_i)$$

Důkaz: Ukážeme, že HA najde v každém kroku největší nezávislou množinu z uvažovaných prvků.

Pro spor necht' $\exists i$ t.ž. $z'(T_i) < r(T_i)$. Vezměme nejmenší takové i :



Platí, že $z'(T_{i-1}) = r(T_{i-1})$ (jelikož i je nejmenší protipříklad). Pokud HA další prvek přidá, tak je vše v pořádku a $z'(T_i) = r(T_i)$ platí. Jinak to znamená, že $z'(T_i)$ je co do inkluze maximální množina v T_i , což je spor s 3'.

Nyní k původnímu důkazu: označíme z^* charakteristický vektor optima. Pak

$$\begin{aligned}
w^T z^* &= \sum w_i \cdot z_i^* \\
&= \sum w_i (z_i^*(T_i) - z_i^*(T_{i-1})) & T_0 = \emptyset, * \\
&= \sum \underbrace{(w_i - w_{i+1})}_{\geq 0} z_i^*(T_i) + \underbrace{w_m}_{> 0} z_m^*(T_m) & ** \\
&\leq \sum (w_i - w_{i+1}) r(T_i)_i + w_m r(T_m) \\
&= \sum (w_i - w_{i+1}) z'(T_i)_i + w_m z'(T_m) & \text{lemma výše} \\
&= w^T z'
\end{aligned}$$

* rovnost $z_i^* = z_i^*(T_i) - z_i^*(T_{i-1})$ platí, protože $z_i^*(T_i)$ se zvýší právě tehdy, když charakteristický vektor získá novou 1 (konkrétně tu na pozici z_i^*).

** tohle vypadá magicky, ale dává to smysl – $z^*(T_i)$ v jednom cyklu smyčky přičítáme a ve druhém odčítáme, tak jsme to jen posunuli do $w_i - w_{i+1}$, navíc také započteme poslední část součtu, na který se nedostane. Navíc právě v tomhle kroku používáme **předpoklad setřizenosti**.

Jelikož navíc triviálně $w^T z^* \geq w^T z'$ (je to optimum), tak věta platí.

Důsledek (grafy) poštvání HA na grafový matroid vrátí maximální (minimální pro $-w$) kostru. Poštvání na duál vrátí maximální množinu hran, kterou když odstraníme tak graf zůstane souvislý.

Důsledek (lineární programy) necht (X, S) je matroid a $w \in \mathbb{Q}^X$. Pak HA vyřeší následující lineární program

$$\max \sum_{i \in X} w_i z_i$$

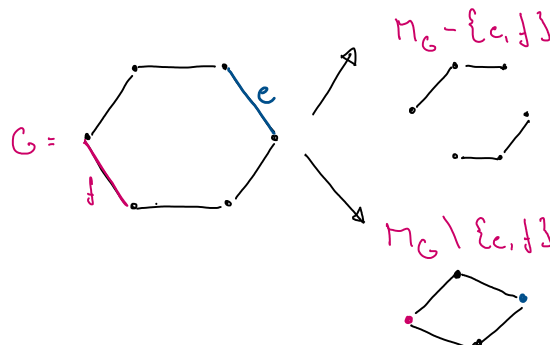
za podmínek $z(A) \leq r(A), z \geq 0$ pro $\forall A \subseteq X$

Operace na matroidech

Součet – pro matroidy $\mathcal{M}_\infty = (X_1, \mathcal{S}_1), \mathcal{M}_\epsilon = (X_2, \mathcal{S}_2), X_1 \cap X_2 = \emptyset$

$$\mathcal{M}_1 + \mathcal{M}_2 = (X = X_1 \cup X_2, \{A \in X \mid A \cap X_1 \in \mathcal{S}_1 \wedge A \cap X_2 \in \mathcal{S}_2\})$$

Příklad (mazání a kontrakce v grafovém matroidu)



Sjednocení – zobecnění součtu. Definice je stejná, ale nepředpokládáme různé X_1, X_2 .

Věta (sjednocení matroidů je matroid) sjednocení matroidů je matroid s řádovou funkcí

$$r(U) = \min_{T \subseteq U} \{|U - T| + r_1(T \cap X_1) + \dots + r_k(T \cap X_k)\}$$

Důkaz (náznak) matroidy zdisjunktníme ($X'_i = X_i \times \{i\}$), sečteme a pak zobrazíme.

[3] Mazání hran v grafu.

Mazání – pro matroid $\mathcal{M} = (X, \mathcal{S})$ a $Y \subseteq X$:

[3]

$$\mathcal{M} - Y = (X - Y, \{A - Y \mid A \in \mathcal{S}\})$$

je opět matroid.

Kontrakce – nechť $\mathcal{M} = (X, \mathcal{S})$ je matroid, $A \subseteq X$ a $J \in \mathcal{S}$ je max. nezávislá množina v A . Pak

[4]

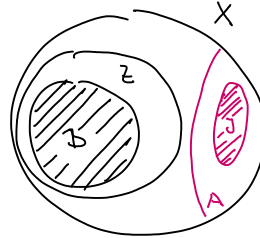
$$\mathcal{M} \setminus A = (X - A, \{Z \subseteq X \mid Z \cup J \in \mathcal{S}\})$$

Věta (kontrakce matroidu je matroid) nechť $\mathcal{M} = (X, \mathcal{S})$ je matroid a $A \subseteq X$. Pak $\mathcal{M} \setminus A$ je matroid s řádovou funkcí

$$r'(Z) = r(Z \cup A) - r(A)$$

Důkaz: nechť J je max. nz. mn v A (viz definice kontrakce); ověříme axiomy

1. $\emptyset \in \mathcal{S} \iff \emptyset \cup J = J \in \mathcal{S}$, platí
2. mějme $Y \in \mathcal{S}'$ a $Y' \subseteq Y$. Z definice víme $Y \in \mathcal{S}' \implies Y \cup J \in \mathcal{S}$. Díky tomu, že $Y' \cup J \subseteq Y \cup J \in \mathcal{S}$, tak rovněž $Y' \cup J \in \mathcal{S}$ (definice matroidu) a tedy $Y' \in \mathcal{S}'$
3. nechť $Z \subseteq X \setminus A$, $B \subseteq Z$ je max. nez. mn. v $\mathcal{M} \setminus A$ a J max. nez. mn. v A



$B \cup J$ je max. nezávislá podmnožina $Z \cup A$ v $\mathcal{M}$ a tedy

$$\begin{aligned} |B| + |J| &= r(Z \cup A) \\ |B| &= r(Z \cup A) - |J| \\ r'(Z) &= \underbrace{r(Z \cup A) - r(A)}_{\text{určený jednoznačně}} \end{aligned}$$

Partition matroid – nechť $X_1, \dots, X_n$ jsou disjunktní množiny a $\mathcal{S}_i = \{A \subseteq X_i \mid |A| \leq 1\}$. Pak $\sum_i (X_i, \mathcal{S}_i)$ je partiční matroid.

Věta (Edmondsova MiniMaxová o průniku matroidů) nechť $\mathcal{M}_1 = (X, \mathcal{S}_1)$ a $\mathcal{M}_2 = (X, \mathcal{S}_2)$ jsou matroidy. Pak

$$\max \{|Y| \mid Y \in \mathcal{S}_1 \cap \mathcal{S}_2\} = \min_{A \subseteq X} r_1(A) + r_2(X \setminus A)$$

Důkaz ($\leq$) Nechť $J \in \mathcal{S}_1 \cap \mathcal{S}_2$. Pak $\forall A \subseteq X$

$$\begin{aligned} J \cap A \in \mathcal{S}_1 &\implies |J \cap A| \leq r_1(A) \\ J \cap (X \setminus A) \in \mathcal{S}_2 &\implies |J \cap (X \setminus A)| \leq r_2(X \setminus A) \end{aligned}$$

A tedy

$$|J| = |J \cap A| + |J \cap (X \setminus A)| \leq r_1(A) + r_2(X \setminus A)$$

Důkaz ($\geq$) TODO, tenhle důkaz je naprosto brutální

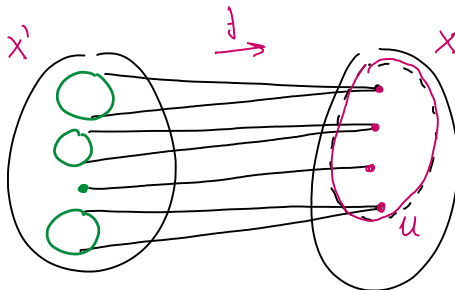
Důsledek (obraz matroidu je matroid) mějme matroid $\mathcal{M}' = (X', \mathcal{S}')$ a funkci $f : X' \implies X$. Definujme

$$\mathcal{S} = \{f[I] \mid I \in \mathcal{S}'\}$$

[4] Podobné jako mazání, ale chová se dost jinak (viz kontrakce/mazání hran v grafu). Např. na mostech grafu se ale chová stejně.

Potom $(X, \mathcal{S})$ je také matroid a navíc pro $U \subseteq T$ platí

$$r(U) = \min_{T \subseteq U} \{|U - T| + r'(f^{-1}(T))\}$$



Poznámka: tvrzení by platilo triviálně, pokud by se jednalo o prostou funkci (tedy pouze přejmenování prvků matroidu). Zajímavé je to, že některé prvky se mohou zobrazit na jiné a nezávislé množiny se tak zmenší, ale matroidnost se zachová.

Dualita matroidu

Definice (duální matroid) necht $\mathcal{M} = (X, \mathcal{S})$ je matroid. Definujeme duální matroid jako $\mathcal{M}^* = (X, \mathcal{S}^*)$ t.ž. B^* je báze $\mathcal{M}^* \iff (X - B^*)$ je báze $\mathcal{M}$ (s tím, že $\mathcal{S}^*$ jsou všechny podmnožiny bází). [5]

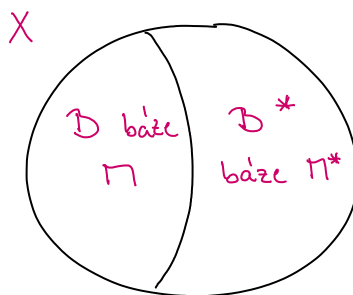
(☺☺): necht $\mathcal{M}$ je matroid, $\mathcal{M}^*$ jeho duál a $A \subseteq X$. Pak

$$r(X) = r(X \setminus A) \iff A \in \mathcal{S}^*$$

Důkaz: A můžeme rozšířit na bázi B^* duálu, přičemž bude stále platit $r(X - B^*) = r(X)$, protože $X - B^*$ je báze $\mathcal{M}$. Tohle můžeme dělat i když jsme další větu ještě nedokázali, jelikož pro $\mathcal{M}^*$ platí axiomy 1 a 2 matroidu, jelikož jsme ho definovali jako báze.

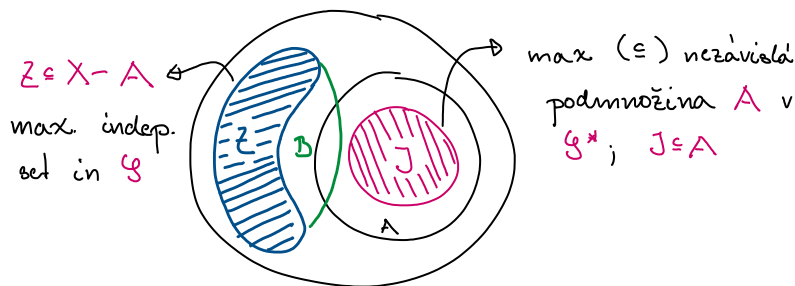
Věta (duální matroid je matroid) necht $\mathcal{M}$ je matroid. Pak $\mathcal{M}^*$ je také matroid a navíc platí

$$r^*(A) = |A| - r(X) + r(X - A)$$



Důkaz: stačí dokázat 3' (pro dané A mají všechny nezávislé množiny stejnou velikost), jelikož 1 a 2 platí triviálně z toho, že jsme definovali pouze báze. Uvažme libovolné A a následující obrázek

[5] Duální matroid grafového matroidu je matroid množin hran, které když odebereme tak graf zůstane spojitý.



Nechť B je báze $\mathcal{M}$ t.ž. $Z \subseteq B$ a $B \subseteq X - J$ (existuje, protože $r(X) = r(X - J)$)

Jestli existuje $x \in (A - J) - B$, pak $r(X - (J \cup \{x\})) = r(X)$ a $J \cup \{x\} \in \mathcal{S}^*$ a J není maximální, díky čemuž $J = A - B$. Rovněž platí $Z = B - A$ (jinak můžeme rozšířit, což je spor) a tedy

$$\begin{aligned} r^*(A) &= |J| = |A - B| \\ &= |A| - |B \cap A| \\ &= |A| - |B \cap (B - Z)| \\ &= |A| - |B| + |Z| \\ &= |A| - r(X) + r(X - A) \end{aligned}$$

Poznámka: Matroid může být **duální sám sobě** (v tom smyslu, že $\mathcal{M}_1$ a $\mathcal{M}_2$ jsou izomorfní).

Definice (Cobáze, conezávislost) nechť $\mathcal{M}$ je matroid a $\mathcal{M}^*$ jeho duální matroid. Pak $Y \subseteq X$ je

- **cobáze**, pokud je báze v $\mathcal{M}^*$
- **conezávislá**, pokud je nezávislá v $\mathcal{M}^*$

Definice (kružnice) nechť $\mathcal{M}$ je matroid. Pak $Y \subseteq X$ je kružnice, je-li minimální ($\subseteq$) **závislá** množina.

Věta: $Y \subseteq X$ je cokružnice (kružnice v duálu) $\iff Y$ je min ($\subseteq$) protínající **každou bázi**. [6]

Důkaz ($\Rightarrow$) sporem nechť $Y \subseteq X$ je cokružnice ale $\exists B$ báze $\mathcal{M}$ t.ž. $Y \cap B = \emptyset$. Pak $Y \subseteq X - B$ ale z definice je $X - B$ báze $\mathcal{M}^*$, což je spor se závislostí Y v $\mathcal{M}^*$. Navíc kružnice je do inkluze minimální, takže minimalitu splňujeme taky.

Důkaz ($\Leftarrow$) opět sporem nechť Y je minimální množina (do inkluze) protínající každou bázi, ale není cokružnice. Rozebereme případy toho, co může být (chceme, aby byla minimálně nezávislá):

- Y je nezávislá v $\mathcal{M}^*$ (a tedy $r(X) = r(X - Y)$)
 - pak existuje báze $B \subseteq X - Y$ v $\mathcal{M}$, což je spor s tím, že protíná každou bázi
- Y není minimálně nezávislá (tedy $\exists y \in Y$ t.ž. $Y \setminus \{y\}$ je závislá v $\mathcal{M}^*$):
 - $(Y \setminus \{y\}) \notin \mathcal{S}^*$
 - $r(X) > r(X - (Y \setminus \{y\}))$
 - $Y \setminus \{y\}$ protíná každou bázi, což je spor s minimalitou

Důsledek: nechť G graf souvislý. Pak cokružnice $\mathcal{M}_G$ jsou přesně **minimální hranové řezy**.

Perfektní párování

Poznámka: o tomto tématu jsem vytvořil [YouTube video](#), které algoritmus shrnuje.

Definice (párování) nechť $G = (V, E)$ graf. Pak $M \subseteq E$ je párování $\iff \forall e \neq e' \in M$ platí $e \cap e' = \emptyset$.

Definice (největší párování) pokud $|M|$ je maximální.

(☹☹): je rozdíl mezi **maximálním** párováním (počítá se do **inkluze**) a **největším** (počítá se do **velikosti**), jelikož si hrany můžeme hladově vybrat špatně (viz lichá cesta).

Definice (perfektní párování) pokud $|M| = |V|/2$

[6]_V grafu jsou to kružnice.

Definice (pokrytí) vrchol je M -pokrytý, pokud je v nějaké hraně z párování.

Definice (defekt) $\text{def}(M)$ je počet M -nepokrytých vrcholů

Definice (alternující cesta) podgraf, který je cesta

- je **zlepšující**, pokud má krajní vrcholy M -nepokryté

Věta: graf $G = (V, E)$, M párování. Pak M je největší $\iff G$ nemá zlepšující cestu.

Důkaz:

- $\Leftarrow$ pokud má zlepšující cestu, tak párování můžeme zlepšit a není tedy maximální
- $\Rightarrow$ pokud G není maximální tak existuje párování M' t. ž. $M' > |M|$
 - uvažme graf $M \Delta M'$ – stupně mají vrcholy nejvýše dva, komponenty jsou tedy buď alternující cykly nebo cesty – díky tomu, že nám jedna hrana přebývá, tak alespoň jedna komponenta je cesta

($\odot\odot$): $G = (V, E)$, $A \subseteq V$. Pak v libovolném párování M musí být liché komponenty $G - A$ pokryté pouze z A (i v nejlepším zpárování v nich zbyde alespoň jeden volný vrchol) a tedy

$$\text{def}(M) \geq \text{lc}(G - A) - |A|$$

Kde lc značí počet lichých komponent grafu.

($\odot\odot$): $G = (V, E)$. Pak

$$\max_{\text{párování } M} |M| = \min_{\text{párování } M} \frac{1}{2} (|V| - \text{def}(M)) \leq \min_{A \subseteq V} \frac{1}{2} (|V| - \text{lc}(G - A) + |A|)$$

kde první nerovnost plyne z úvahy, že největší párování minimalizuje defekt a druhá z dosazení pozorování výše.

Věta (Tutte-Berge) Pro výše uvedené pozorování platí rovnost.

Důkaz: stačí najít párování M t.ž. platí rovnost.

Najdeme algoritmem (Edmonds), který najde maximální párování

- postupně zvětšujeme párování M :
- 1. M perfektní $\implies$ je maximální a věta platí ($A = \emptyset$)
- 2. M má M -nepokrytý vrchol r : budujeme alternující strom T tím, že sřídavě přidáváme hrany:
 - B -vrcholy: vrcholy v sudé vzdálenosti od r
 - A -vrcholy: vrcholy v liché vzdálenosti od r
 - zastavíme se, když:
 - existuje $w \notin T$, $\{v, w\} \in E$ a w je nepokrytý – pak jsme našli alternující cestu
 - neexistuje w
 - * pokud je graf bipartitní, tak nemáme žádné $B - B$ hrany a všechny zbývající hrany z B -vrcholů vedou do A -vrcholů – poté když uvážíme $G - A$, tak liché komponenty vedou pouze do A vrcholů ale B je o jedna více (máme r), tedy $|B| = |A| + 1$ a G nemá perfektní párování a **našli jsme defektní vrchol**

Pro **bipartitní grafy** můžeme algoritmus výše opakovat (opakovaně stavíme stromy z vrcholů, které nejsou v párování), najít všechny defektní vrcholy a věta výše platí (máme množinu defektních vrcholů a párování splňující rovnost).

Pro **nebipartitní grafy** může existovat hrana mezi $B - B$ vrcholy (lichá kružnice).

($\odot\odot$): nechť C lichá kružnice v G , G' vznikne kontrakcí C do jednoho (pseudo)vrcholu a M' je párování v G' . Potom existuje párování M v G , že počet M' -nepokrytých vrcholů je stejný jako počet M -nepokrytých.

Podgrafy G reprezentované pseudovrcholy mají lichý počet vrcholů (chceme opět dostat M a A , abychom větu dokázali). To platí, protože pseudovrcholy vznikly kontrakcí liché kružnice na vrchol a tedy přišly o sudý počet vrcholů.

Postup pro $B - B$ hrany je tedy ten, že zkontrahujeme C , vyřešíme párování a odkontrahujeme.

[7] A může být i prázdné (eliminuje grafy s lichým počtem vrcholů).

Důsledek (Tutte) G má perfektní párování právě tehdy, když

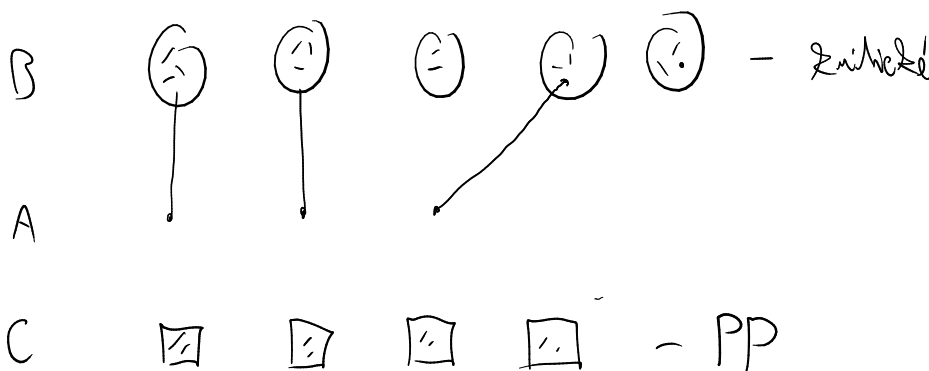
[7]

$$\forall A \subseteq V : \text{lc}(G - A) \leq |A|$$

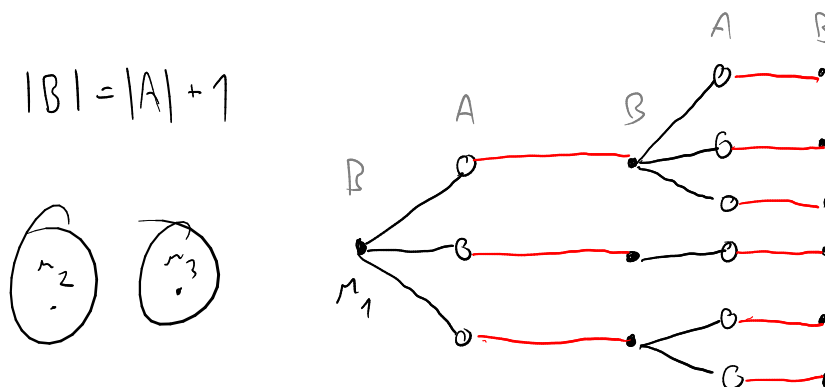
Důkaz: vychází přímo z Tutte-Berge dosazením $|M| = |V|/2$ (jedná se o perfektní párování).

Věta (Edmonds-Gallai dekompozice) G graf, $G = (V, E)$, $B \subseteq V$ vrcholů nepokrytých nějakým maximálním párováním. Nechť $A \subseteq V - B$ sousedé vrcholů z B , $C = V - (B \cup A)$. Pak

- každá komponenta $G - (A \cup C)$ je kritická ($\forall v \in K : K - \{v\}$ má perfektní párování)
 - G kritický $\iff G$ lze zkonstruovat z liché kružnice lepením lichých uší
- každé maximální párování M splňuje:
 - $e \in M, e \cap A \neq \emptyset \implies |e \cap A| = 1$ a e vede do B
 - tohle nezamezuje, že by dvě hrany z A nevedly do jedné z B
 - do každé komponenty B vede ≤ 1 hrana M



Důkaz: Uvažme poslední alternující les v Edmondsově algoritmu.



Každá hrana s koncem v A vede do B (s tím, že vrcholy v B jsou (pseudo)vrcholy vzniklé operací kontrakce. Defekt $\text{def}(M)$ je počet komponent v tomto lese.

Nepokryté vrcholy žádným maximálním párováním:

- ne v A , jelikož všechny musí být pokryté každým maximálním párováním
- ne mimo $A \cup B$, protože tam je perfektní párování

Takové vrcholy tedy mohou být pouze v B , čímž jsme dokázali (1).

Část (2) rovněž plyne z Edmondsova algoritmu.

Generující funkce magic

Nechť $G = (V, E)$ rovinný, $w : E \mapsto \mathbb{Q}$ váhová funkce

1. **maximální perfektní párování** – najdi M perfektní párování t.ž. $w(E)$ je maximální
 - polynomiální (pro všechny grafy)
2. **maximální hranový řez** – najdi E' hranový řez t.ž. $w(E')$ je maximální
 - obecně je NP-těžný, pro grafy na 2D plochách polynomiální

Definice (determinant) nechť A je reálná matice. Pak determinant je

$$\text{Det}(A) = \sum_{\pi} (-1)^{\text{sign}(\pi)} \overbrace{\prod_{i=1}^n A_{i,\pi(i)}}^{\text{transverzála}}$$

- polynomiální, jde řešit přes Gaussovu eliminaci

Definice (permanent) nechť A je reálná matice. Pak permanent je

$$\text{Per}(A) = \sum_{\pi} \prod_{i=1}^n A_{i,\pi(i)}$$

- $\#P$ -complete (alespoň tak těžký jako NP -úplný), neumíme nic lepšího

Příklad: $G = (V_1, V_2, E)$ bipartitní graf, $A^{|V_1| \times |V_2|}$ 0/1 matice podle toho, jaké obsahuje hrany. Pak $\text{Per}(A)$ je počet perfektních párování G .

$$\mathcal{P}(G, x, w) = \sum_{P \text{ perf. pár.}} x^{w(P)}$$

$$\mathcal{E}(G, x, w) = \sum_{E' \text{ sudá}} x^{w(E')}$$

$$\varphi(G, x, w) = \sum_{C \text{ hranový řez}} x^{w(C)}$$

Věta: G rovinový. Pak

$$\varphi(G) \equiv \mathcal{E}(G^*) \equiv \mathcal{P}(G_{\Delta}^*)$$

kde symbolem $\equiv$ rozumíme vzhledem k vypočitatelnosti a G_{Δ} následující operaci:



Rovněž předpokládáme $w(e) \in \mathbb{Z}$, $|w(e)| \leq |V(G)|^c$ pro c konstantu.

Věta (Kasteleyn) Když G rovinový, pak $\mathcal{P}(G, x, w)$ lze spočítat v polynomiálním čase.

Důsledek:

- umíme spočítat jak maximální párování, tak jejich počet (a počet všech ostatních párování s danými vahami)
- max. řez, max. perf. párování jsou pro rovinné grafy polynomiální

Důkaz (naznačení) pro D orientaci G , M_0 fixní perfektní párování definujeme „determinantní verzi“ $\mathcal{P}$ následně:

$$\mathcal{P}(G, D, \mathcal{M}, \S, \sqsupseteq) = \sum_{P \text{ perf. pár.}} \text{sign}(D, M_0, P) x^{w(P)}$$

kde

$$\text{sign}(D, M_0, P) = (-1)^{\# \text{ } D\text{-sudých cyklů } M_0 \Delta P}$$

- D -sudý je, když v D má sudý počet hran orientovaných jedním směrem; nezáleží na tom, jakou stranou jdeme, jelikož symetrická difference perfektních párování tvoří jen sudé cykly

Postup důkazu:

- $\mathcal{P}(G, D, M_0, x, w)$ lze pro obecné grafy spočítat variantou Gaussovske eliminace (Pfaffaon)
- Existuje orientace D^K , že všechna znaménka $\text{sign}(D^K, M_0, P)$ jsou stejná, tedy

$$\mathcal{P}(G, D^K, M_0, *, w) = \pm \mathcal{P}(G, x, w)$$

- Tuhle D^K lze zkonstruovat v polynomiálním čase.

Připomenutí: pro další plochy je to trochu komplikovanější, ale jde to dělat podobně.

Pošťáci a cestující

Definice: $G = (V, E)$ graf silniční sítě, $l : E \mapsto \mathbb{Q}^+$ váhová funkce:

- problém **čínského pošťáka**: najdi trasu minimální délky, která projde všechny *hrany* a vrátí se do výchozího vrcholu (eulerovský tah)
 - polynomiální
- problém **obchodního cestujícího**: najdi trasu minimální délky, která projde všechny *vrcholy* a vrátí se do výchozího vrcholu (hamiltonovskou kružnici)
 - NP-úplný

Problém (čínského pošťáka)

1. $G = (V, E)$ má **všechny stupně sudé** $\implies$ řešení je uzavřený eulerovský tah
 - (☹☹): když $H = (W, F)$ má všechny stupně sudé a $F \neq \emptyset$ je neprázdná, pak F má cyklus; odstraněním cyklu má opět všechny stupně sudé; opakováním dostaneme disjunktní sjednocení cyklů, což jde do eulerovského tahu udělat trivialně
2. nechť $T = \{v \mid \deg_G(v) \text{ lichý}\}$

(☹☹): $|T|$ je sudé (součet stupňů je sudý)

Definice (T-join) $E' \subseteq E$ je T -join (pro množinu vrcholů T), pokud $G_T = (V, E')$ platí

$$(\forall v \in V) (\deg_{G_T}(v) \text{ lichý} \iff v \in T) \quad [8]$$

Věta: nechť $E' \subseteq E$ je množina hran min. trasy čínského pošťáka, které se projdou více než jednou. Pak se projdou **právě 2-krát** a E' je **min. T-join** (kde T je výše definovaná množina).

Důkaz: (☹☹): nechť G' vznikne z G dodáním násobných hran, násobnost je podle počtu procházení minimální trasou P . Potom G' má všechny stupně sudé.

- $F = E(G') - E(G)$ jsou dodané hrany
- F nemá násobné hrany, protože pak bychom je mohli (po dvou) vynechat

Z pozorování plyne (1), jelikož F spolu s původními hranami dává 2 průchody.

Navíc jelikož $E(G') = E(G) \cup F$ je T -join, jelikož přesně splňuje definici (stupně budou liché v G' , protože musí být sudé po přidání do G). Navíc $E(G) \cup \overline{F}$ rozhodně nebude lepší než minimální cesta čínského pošťáka a tedy naše F .

Algoritmus (čínský pošťák)

1. najdi minimální T -join
 - použij konstrukci (modifikovanou) Fischera z minulé přednášky ($G \mapsto G_\Delta$), o čemž víme, že je polynomiální
 - (alternativně) uvažme pomocný graf $H = \left(T, \binom{T}{2}\right)$ a váha $w : \binom{T}{2} \mapsto \mathbb{Q}^+$, kde $w(\{u, v\}) =$ délka nejkratší cesty mezi u, v v G
 - nechť M je min. perfektní párování v H

[8] Je to taková množina vrcholů a hran, na kterou když se omezíme, tak všechny stupně vrcholů v T jsou liché a ostatní jsou sudé.

- necht $F = \bigcup_{e \in M} P_e$, kde P_e je nejkratší cesta v G spojující vrcholy e
- 2. přidej zbylé hrany
- 3. profit?

Problém (obchodního cestujícího) předpokládáme

- $G = K_n$ (pro neexistující hrany nastavíme váhu na nekonečno)
- nezáporné délky
- trojúhelníková nerovnost $(\forall u, v, w \in V) l(u, v) + l(v, w) \geq l(u, w)$

Algoritmus (Christofidesova heuristika) viz moje [poznámky z aproximačních algoritmů](#)

Spojitá optimalizace

Má [pěkná skripta](#).

Zkouška

Na obou částech jsem si vytáhl okruh, o kterém jsem napsal co vím a pak jsem to se zkoušejícím probíral.

Diskrétní část

Zkušební okruhy:

1. Matroidy: základní definice, příklady.
2. Řádová funkce a submodularita.
3. Kontrakce, dualita.
4. Hladový algoritmus.
5. Průnik matroidů, obraz, sjednocení.
6. Edmondsův algoritmus na maximální párování, Tuttova věta.
7. Problém Obchodního cestujícího a Čínského poštáka.

Spojitá část

- z webových stránek přednášky: „Na zkoušce se probírá jen teorie.“

Odkazy

- Web diskrétní části: <https://kam.mff.cuni.cz/~loebldsopt22.html>
- Web spojitě části: <https://kam.mff.cuni.cz/~hladikDSO/>

Poděkování

- Davidu Kubkovi za zápisky, ze kterých jsem první polovinu poznámek vytvářel (včetně obrázků).