Teorie matroidů

2. ledna 2013

Obsah

Pojmy

Matroid je uspořádaná dvojice $\mathcal{M} = (E, \mathcal{I})$, kde E je neprázdná nosná množina matroidu a $I \subseteq 2^E$ je množina nezávislých množin splňující:

- $\emptyset \in \mathcal{I}$
- $(I \in \mathcal{I} \wedge I' \subseteq I) \Rightarrow I' \in \mathcal{I}$
- $(I_1, I_2 \in \mathcal{I} \wedge |I_1| < |I_2|) \Rightarrow (\exists e \in I_2 \backslash I_1)\,(I_1 \cup \{e\} \in \mathcal{I})$

Isomorfismus na matroidech funguje obvykle (je to zobrazení, které převádí nezávislé na nezávislé).

Minimální závislé množiny (co do inkluze) jsou ***kružnice***.

Lemma 1 *Máme matroid $\mathcal{M} = (E, \mathcal{I})$ a $\mathcal{C}$ je množina kružnic v $\mathcal{M}$. Potom platí:*

- $\emptyset \notin \mathcal{C}$
- $(C_1, C_2 \in \mathcal{C} \wedge C_1 \subseteq C_2) \Rightarrow (C_1 = C_2)$
- $(C_1, C_2 \in \mathcal{C}, C_1 \neq C_2, e \in C_1 \cap C_2) \Rightarrow (\exists C_3 \in \mathcal{C}; C_3 \subseteq (C_1 \cup C_2) - e$

Důkaz:
První a druhé je jednoduché, přímo z axiomů.

To třetí dokazujeme sporem. Nechť máme tedy C_1, C_2. Ty jsou různé, proto existuje f, které je v C_2 a není v C_1. Když ho z C_2 odeberu, dostanu něco nezávislého. Zkusím přidávat tak, abych dostal maximální nezávislou I. Tam určitě není f. Celé C_1 tam také není, proto tam chybí ještě nějaké $g \in C_1 \backslash I$. A je vidět, že $f \neq g$, tedy v I chybí minimálně 2 prvky oproti sjednocení $C_1 \cup C_2$. Ale sjednocení bez e je jen o 1 menší. Na I tedy aplikuji třetí axiom, přidám prvek, ale to je spor s maximalitou I, proto toto nastat nemůže.

☻

Jednoprvkové kružnice se nazývají ***smyčky***.

Věta 1 *Nechť $\mathcal{C} \subseteq 2^E$ o kterém platí podmínky z Lemmatu 1. Potom $\mathcal{I} := \{I|\,(I \subseteq E) \wedge (\forall C \in \mathcal{C}(C \nsubseteq I)\}$ tvoří matroid $\mathcal{M} = (E, I)$ a $\mathcal{C}$ jsou kružnice $\mathcal{M}$.*

Důkaz:
Protože prázdná nesmí být kružnice, prázdná je v $\mathcal{I}$. Pokud něco neobsahuje kružnici, pak ani nic menšího, druhá podmínka také platí.

Třetí dokazujeme sporem, máme dva prvky, $I_1, I_2, |I_1| < |I_2|$ a kdykoliv cokoliv k I_1 přidáme z I_2, tak dostaneme kružnici/závislou množinu. Zvolme nezávislou množinu I_3 takovou, že $|I_3| > |I_1|$ a $|I_1 \backslash I_3|$ je minimální (přidáváme, dokud to jde). Tento rozdíl je neprázdný. Fixujme $e \in I_1 \backslash I_3$. Definujme $T_f := (I_3 - f + e)$, pro každé $f \in I_3 \backslash I_1$, kde to jde.

Pokud T_f je nezávislá, pak zmenším rozdíl, tedy spor s minimalitou $|I_1 \backslash I_3|$. Tedy je závislá, je tam kružnice C_f. $e \in C_f, f \notin C_f$. Pokud $C_f \cap (I_3 \backslash I_1) = \emptyset \Rightarrow C_f \subseteq (I_3 \cap I_1 + e - f)$. To je spor.

Existuje tedy $\exists g \in C_f \cap (I_3 \backslash I_1)$. Aplikujeme třetí podmínku Lemmatu 1. $e \in C_f \cap C_g; g \in C_f; g \notin C_g$, tedy $C_g \neq C_f$, tedy $\exists C \subseteq (C_f \cup C_g) - e \subseteq I_3, C \in \mathcal{C}$, což je spor. Proto původní předpoklad je chybný.

☻

Co do inkluze maximální nezávislé množiny jsou ***báze***, značíme $\mathcal{B}$ nebo $\mathcal{B}(\mathcal{M})$.

Lemma 2 *Nechť $B_1, B_2 \in \mathcal{B}$. Potom $|B_1| = |B_2|$*

Důkaz:
Triviálně plyne z výměnného axiomu (třetího).

☻

Lemma 3 (Vlastnosti báze) *Jednak, existuje alespoň jedna báze. A když mám dvě báze, z jedné něco odeberu a přidám něco z druhé, mám opět bázi.*

Důkaz:
Triviálně plyne z prvního a z třetího.

☻

Lemma 4 *Nechť $\mathcal{B}$ splňuje podmínky v Lemmatu 3. Potom libovolné dvě báze jsou stejně velké.*

Důkaz:
Sporem. Máme $|B_1| > |B_2|$. Vezmu prvek $e \in B_1 \backslash B_2$, aplikuji druhou podmínku, získám opět bázi, stejně velkou, pokračuju, dokud mi nedojdou prvky e – ale potom mám něco většího, než B_2.

☻

Věta 2 *Vlastnosti báze jsou dostatečné zadání matroidu (když vezmu všechny podmnožiny bazí, mám $\mathcal{I}$).*

Důkaz:
První triviální, druhé také.

Pro spor předpokládejme, že třetí neplatí. Máme dvě nezávislé $I_1, I_2, |I_1| < |I_2|$ a vezmu libovolný prvek z I_2 e, který není v I_1. Když ho přidám, dostanu závislou.

Pro ně existují nějaké báze, tam lze něco přestrkovat.

☻

Lemma 5 *Třetí podmínka kružnic jde zesílit – můžu si vybrat i jeden prvek z $C_1 \backslash C_2$, který tam musí skončit.*

Lemma 6 *U bází to jde i naopak – ne, že řeknu „tenhle vyhoď" a v závislosti na tom si nějaký vyberu, ale řeknu „tenhle přidej" a v závislosti na tom jeden vynechám.*

0.1 Ranková funkce

Ranková funkce je funkce $r : 2^E \to \mathbb{Z}_0^+$. Na matroidech funguje tak, že přiřazuje velikost maximální nezávislé podmnožiny.

$r(\mathcal{M})$ je rank celého matroidu a je to zřejmé, co je.

Lemma 7 (Vlastnosti rankové funkce)

- $0 \leq r(X) \leq |X|$
- $X \subseteq Y \Rightarrow r(X) \leq r(Y)$
- $X, Y \subseteq E; r(X \cup Y) + r(X \cap Y) = r(X) + r(Y)$

Důkaz:
První a druhé je vidět.

Třetí je potřeba utlouct, vezmeme si ty nejlepší nezávislou v průniku a v sjednocení. Poté se začne počítat s těma „ušima" a utluče se to.

☻

Lemma 8 *Nechť $\mathcal{M}(E, \mathcal{I})$ je matroid a $r : 2^E \to \mathbb{Z}_0^+$ splňuje vlastnosti z Lemma 7. Potom $X, Y \subseteq E$ takevé, že $\forall y \in Y \backslash X; r(X + y) = r(X)$. Poto $r(X \cup Y) = r(X)$*

Důkaz:
Indukcí podle velikosti rozdílu. Pokud je jen 1, tak pohoda.

Jinak štípnu ty rozdílné na dvě části (Y_1, Y_2), když přidám ty, tak dle indukčního předpokladu to platí. Na ty dvě části platí pustíme submodularitu.

$$
\begin{aligned}
r(X \cup Y_1) &= r(X) \\
r(X \cup Y_2) &= r(X) \\
r(X \cup Y) + r(X) &\leq r(X) + r(X) \\
r(X) \leq r(X \cup Y) &\leq r(X)
\end{aligned}
$$

☻

Věta 3 *Nechť E je konečná množina, r je funkce splňující věci z Lemma 7. Potom $\mathcal{M}(E, \mathcal{I} = \{I \subseteq E; r(I) = |I|\})$ je matroid a r je jeho ranková funkce.*

Důkaz:
První je, že prázdná je nezávislá, což zjevně je.

Dvojku dokážeme pomocí submodularity, vyjde nám, že velikosti stále sedí.

Trojku dokážeme sporem. Vezmeme I_1, I_2 nezávislé, $I_1 < I_2$, ale žádné z rozdílu nejde přidat. To znamená, že ten prvek přebývá v mohutnosti oproti ranku $(r(I_1) \leq r(I_1 + e) < |I_1| + 1$, tedy se přidáním nezmění. Podle lemmatu 8 ale to musí být totéž jako $r(I_1 \cup I_2)$. $|I_2| = r(I_2) \leq r(I_1 \cup I_2) = r(I_1) = |I_1|$, což je ale ve sporu s velikostmi v předpokladu.

To, že je to ranková funkce, je vidět z definice.

☻

$H \subseteq E$ je ***nadrovina***, pokud H je maximální podmnožina s vlastností, že $r(H) < r(\mathcal{M})$.

Lemma 9 (Sčítání matroidů) *Nechť $\mathcal{M}_1 = (E_1, \mathcal{I}_1)$, $\mathcal{M}\left(E_2, \mathcal{I}_2\right)$, $\mathcal{M}_1 \cap \mathcal{M}_2 = \emptyset$. Potom $\mathcal{M}\left(E := E_1 \cup E_2, \{I \subseteq E; I \cap E_1 \in \mathcal{I}_1 \wedge I \cap E_2 \in \mathcal{I}_2\}\right)$ je také matroid.*

Když máme matici A a její nezávislé sloupce, máme matroid.

Matroid je nad nějakým tělesem ***representovatelný***, pokud existuje matice nad tím tělesem, která tvoří tento matroid. Obecně (bez tělesa) je reprezentovatelný, pokud existuje alespoň jedno těleso, nad kterým to jde.

Lze převést na jednotkovou matici nějakého řádu a pak nějaký zbytek (ten řád bude rank matroidu). Báze bude ty jednotkové sloupce.

0.2 Dualita

Máme $\mathcal{B}$ množinu bazí matroidu $\mathcal{M} = (E, \mathcal{I})$. Definujme $\mathcal{B}^* = \{E \backslash B; B \in \mathcal{B}\}$. Toto splňuje podmínky bazí, tedy je to matroid. Takovému říkáme že je ***duální***.

Tvrzení 1 *$\mathcal{B}^*$ je množina bazí.*

Důkaz:
Je to neprázdné (to je vidět).

Když vyměňuji prvky, tak budu jen vyměňovat naopak.

☻

Důsledek 1 $(\mathcal{M}^*)^* = \mathcal{M}$

$$r(E) + r^*(E) = |E|$$

Tvrzení 2
$$\forall X \subseteq E; r^*(X) = |X| - r(E) + r(E \backslash X)$$

Důkaz:
Jen upočítat, nějakým doplňováním na bázi.

☻

Lemma 10 *$C*$ je co-kružnice, právě když její komplement je nadrovina.*

Důkaz:
To je upočítatelné z předchozího tvrzení a z toho, že kružnice je minimální, co má rank o jedna menší, než počet prvků, nadrovina zase max co je o 1 menší, než matroid.

☻

Důsledek 2 *Nadroviny v grafech jsou minimální hranové řezy G.*

Tvrzení 3 *C je kružnice, C^* je duální kružnice. Potom $|C \cap C^*| \neq 1$.*

Důkaz:
Sporem. Vezmeme nadrovinu H, která je doplňkem C^*. e (který je v C i v C^* tam neleží. Tak ho tam zkusíme přidat. Vezmu $r(C) + r(E) = r(C - e) + r(H + e)$ (do nadroviny můžu přidat, to se zvětší, ale u kružnice se rank nezmění). To je totéž jako $r(C \cap H) + r(C \cup H) \leq r(C) + r(H)$. Tedy, $r(E) \leq r(H)$, což nejde.

☻

Tvrzení 4 *$\mathcal{M}_1, \mathcal{M}_2$ jsou matroidy na disjunktních množinách. $\mathcal{M}_1^* \oplus \mathcal{M}_2^* = (\mathcal{M}_1 \oplus \mathcal{M}_2)^*$.*

Důkaz:
Z definice přes baze. Prostě v každém žije kus báze.

☻

0.3 Minory

Chceme vynechávat a kontrahovat.

Když vynechám hrany, tak mám $\mathcal{M} \backslash T = (E \backslash T, \mathcal{I}' = \{I; I \subseteq E \backslash T \wedge I \in \mathcal{I}\})$. Toto je matroid, to je vidět.

Pokud kontrahuji, tak dostanu $\mathcal{M}/T = (\mathcal{M}^* \backslash T)^*$. Používám jen matroidové operace, takže dostanu matroid.

Tvrzení 5 *Nechť mám $\mathcal{M}$, $T \subseteq E$, $X \subseteq E \backslash T$. Po vynechání rank X zůstane. U kontrakce $r_{\mathcal{M}/T}(X) = r_{\mathcal{M}}(X \cup T) - r_{\mathcal{M}}(T)$.*

Důkaz:
Přes vzoreček pro duality, jen upočítání.

☻

$C' \subseteq E\backslash T$ je kružnice v $\mathcal{M}/T$ právě když C' je minimální neprázndá z $\{C\backslash T; C \in \mathcal{C}(\mathcal{M})\}$.

Pořadí vynechávání a kontrahování lze libovolně prohazovat.

$\mathcal{N}$ je minor $\mathcal{M} \Leftrightarrow \mathcal{N}^*$ je minor $\mathcal{M}^*$.

Duál k K_5 a k $K_{3,3}$ není grafový (matroid dle definice existuje, ale nejde nakreslit jako graf).

1 Souvislost

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

V matroidu můžeme mít totéž, jen říkáme s hranami, ne s vrcholy, ale vychází stejná vlastnost.

Vlastnost, že jsou spolu v kružnici je symetrická, reflexivní a tranzitivní (to poslední se dokáže sporem).

Množina X je ***separátor***, pokud X je sjednocení komponent souvislosti.

Každá kružnice leží v právě jedné komponentě.

Tvrzení 6 *X je separátor $\Leftrightarrow r(X) + r(E\backslash X) = r(\mathcal{M})$.*

Důkaz:
Jedním směrem ze submodularity. Dokážeme, že báze jsou jen v jedné nebo druhé části.

☻

Lemma 11 *X je separátor. Potom je $r(F) = r(F \cap X) + r(F\backslash X)$.*

Lemma 12 *$\mathcal{M}/X = \mathcal{M}\backslash X \Leftrightarrow X$ je separátor.*

Důkaz:
Přes báze a definice.

☻

Lemma 13 *X je separátor $\Leftrightarrow r(X) + r^*(X) = |X|$.*

Důkaz:
Plyne z $r^*(X) = |X| - r(\mathcal{M}) + r(E\backslash X)$.

☻

Důsledek 3 *X je separátor v $\mathcal{M}$ $\Leftrightarrow$ X je separátor $\mathcal{M}^*$.*

Věta 4 *Matroid je direktním součtem svých komponent souvislosti.*

Lemma 14 *$\mathcal{M}$ je souvislý $\Leftrightarrow$ pro každé dva prvky existuje nadrovina, která jimi neprochází.*

2 Matroid intersection theorem

Máme dva matroidy $\mathcal{M}_1, \mathcal{M}_2$ na stejné množině E. Snažíme se najít co největší nezávislou množinu v obou (třeba i váženě).

Věta 5

$$\max_{X \subseteq E; r_1(X) = r_2(X) = |X|} |X| = \min_{E_1 \dot{\cup} E_2 = E} r_1(E_1) + r_2(E_2)$$

Důkaz:
Napřed $\leq$. Pokud X je nezávislá v $\mathcal{M}_1$ i $\mathcal{M}_2$ a $E_1 \dot{\cup} E_2 = E$, potom:

$$|X \cap E_i| \leq r_i(E_i)$$

V druhé části ukážeme algoritmus, máme orákulum, to říká, jestli je podmnožina nezávislá.

Iterativně v krocích, v každém kroku buď najdeme rozklad nebo X o kousek zvětšíme. Začneme s prázdnou množinou.

Sestrojíme pomocný graf. Bude bipartitní, na jedné straně X, na druhé $E \backslash X$. Hranu z $y \in E \backslash X$ do $x \in X$ dám, pokud nahrazení x prvkem y bude nezávislou v $\mathcal{M}_2$. Opačnou dám, pokud je nezávislá v $\mathcal{M}_1$.

Množina Y_1 jsou ty prvky y takové, že je můžu přidat a bude nezávislá v $\mathcal{M}_1$ a Y_2 obdobně.

První příklad je, když existuje orientovaná cesta z Y_1 do Y_2 a druhý případ je, když není.

Vezmeme napřed případ druhý.

$E_2 := \{z;$ existuje orientovaná cesta do z z $Y_1\}$. $E_1 := E \backslash E_2$. Celé $Y_1 \subseteq E_1, Y_2 \subseteq E_2$, všechny případné hrany vedou z E_2 do E_1.

$r_2(E_2) = |X \cap E_2|$. Určitě je to $\geq$, protože E_2 je nezávislá v $\mathcal{M}_2$. Kdyby neplatilo opačně, tak $|Z| > |X \cap E_2|$, Z je nezávislá v $\mathcal{M}_2$. BÚNO $X \cap E_2 \subseteq$

Z. Tedy $\exists z \in Z \backslash X \cup E_2$. $X \cup \{z\}$ je závislá $\mathcal{M}_2$, protože jinak $z \in Y_2$. $r_2(X \cup \{z\}) = |X|$. $(X \cap E_2) \cup \{z\}$ je nezávislá v $\mathcal{M}_2$, $(X \cap E_2) \cup \{z\} \subseteq Z' \subseteq X \cup \{\}\,; r_2(Z') = |Z'| = |X|$. Tedy $Z' = (X \backslash \{x\}) \cup \{z\}$. Našel jsem tedy šipku z E_2 do E_1, tedy spor.

Protože jsme použili jen směr šipek, ne dostupnost, lze totéž udělat i pro E_1.

Nyní případ, kdy orientovaná cesta z nějakého vrcholu v Y_1 do nějakého v Y_2 vede.

Vezmu tu nejkratší cestu. Označím ji jako $y_0, x_1, y_1, x_2, \ldots, y_k$, $y_0 \in Y_1, y_k \in Y_2$. Vezmu množinu $X' := X\,\{x_1, \ldots, x_k\} \cup \{y_0, \ldots, y_k\}$. Pokud se Y_1, Y_2 protínají, je něco, co je nezávislé v obou, lze to prostě přidat ($y_0 = y_k$).

Tato množina je větší, chceme dokázat, že je nezávislá v obou matroidech.

Dokážeme v $\mathcal{M}_1$, druhý směr je stejný, jen se prohodí ${}_{1,2}$ a směr šipek.

Vezmeme indukcí. X je nezávislá, po první výměně (jdeme od posledního prvku na cestě) je to ještě definice hrany.

Jsme tedy ve stavu, kdy jsme dokázali, že $X \backslash \{x_{i+1}, \ldots, x_k\} \cup \{y_{i+1}, \ldots y_k\}$ je závislá a pro spor předpokládejme, že $X \backslash \{x_i, \ldots, x_k\} \cup \{y_i, \ldots, y_k\}$ je závislá. V té staré je tedy prvek, který zvedne té nové rank, musí být mezi těmi, které vyhazuju.

Také $X \backslash \{x_i\} \cup \{y_i\}$ je nezávislá (existence šipky). Tedy existuje x_j, které tam můžu přidat (y_i to není, to by nebyla závislá). Tedy, mám nezávislou množinu velikosti $|X|$. Z této množiny můžu přidat něco do $X \backslash \{x_i\}$, je to některé y_l, ale pro $l \geq i$. Potom tam je ale šipka a je to zkratka, nebyla to nejkratší cesta. Takže máme jinou množinu stejné velikosti.

Dále, dle Y_1, $X \cup \{y_i\}$ je nezávislá. Takže tam můžeme přidat jeden prvek tak, aby byla nezávislá. Pokud je to y_0, pak hurá, nechť tedy je to některé x_i. To, co vznikne, je větší, než X a lze tedy tam lze něco přidat, je to některé y_i. No ale potom $y_i \in Y_1$ a nemám nejkratší cestu.

☻

3 Souvislost

Tvrzení 7 *G je souvislý graf, X, Y rokzlad E a G_X, G_Y indukované X, Y. Potom $r(X) + r(Y) - r(E) \leq |V(G_x) \cap V(G_y) - 1|$. Navíc je to rovnost pouze pro G_X, G_Y souvislé.*

Důkaz:
Budeme počítat počty hran podle počtu vrcholů v lesech.

☻

Nechť $\mathcal{M} = (E, I)$, (X, Y) rozklad E je k***-separace*** pokud z $r(X) + r(Y) - r(E) \leq k - 1$. k-separace je ***Tutteovská***, pokud $\min \{|X|, |Y|\} \geq k$. Je ***cyklická***, pokud $r(x) < |X|$ a $r(Y) \leq |Y|$ (každá obsahuje kružnici). Esenciální (vertikální) je $\min \{r(X), r(Y)\} \geq k$.

Esenciální separace je i tutteovská.

Souvislost (tutteovská) matroidu $\mathcal{M}$ je $\lambda(\mathcal{M}) = \min\{\infty, k; \mathcal{M}$ má tutteovskou separaci $\}$.

Je (tutteovsky) k-souvislý, pokud jeho souvislost je alespoň k. Matroid je souvislý, právě když je $\lambda(\mathcal{M}) \geq 2$.

Cyklická je $\gamma(\mathcal{M})$ a esenciální $\kappa(\mathcal{M})$.

Tvrzení 8 $\lambda(\mathcal{M}) = \lambda(\mathcal{M}^*)$

Důkaz:
$r(Y) = r(E) - r(X) = r(X) + r^*(X) - |X| = r^*(X) + r^*(E \backslash X) - r^*(E)$

☻

Tvrzení 9 $\kappa(\mathcal{M}) = \gamma(\mathcal{M}^*)$

Důkaz:
Něco žije v nadrovině, doplněk je kružnice v duálu.

☻

Tvrzení 10 *Mějme matroid $\mathcal{M}$ s $\lambda(\mathcal{M}) < \infty$. Potom $\mathcal{M}$ je tutteovsky k-souvislý $\Leftrightarrow$ cyklicky k-souvislý a essinciálně k-souvislý.*

Důkaz:
Esenciálí k-separace je také tutteovská.

Opačně sporem přes nejmenší protipříklad.

☻

Věta 6 *$k \geq 2$ a G souvislý graf s alespoň $k + 1$ vrcholy. G je vrcholově k-souvislý, pokud $\mathcal{M}(G)$ je esenciálně k-souvislý.*

Důkaz:
Vezmeme minimální řez. Máme tedy části A, B, grafy G_A, G_B jsou ta komponenta i s řezem, hrany E_A jsou grafu G_A, tak aby E_A, E_B byl rozklad. $R(e_a) \geq |S|$. Je to tedy esenciální $|S|$-separace.

Druhé sporem. G je k-souvislý. Vezmu G_1, G_2, což je všechny vrcholy jen s jednou množinou hran.

Najdeme dva vrcholy, co jsou v různých komponentách v obou grafech. Dokáže se, že taková dvojice neexistuje. Tedy, alespoň jeden z nich je souvislý. Takže $r(E_1) = r(E)$.

☻

V grafu ***cyklický*** k-řez je takový, že obě části jsou cyklické. Pozor, řez je průnik, ne odebrání.

Věta 7 *k je alespoň 2, G je cyklicky k-souvislý $\Leftrightarrow$ $\mathcal{M}(G)$ je cyklicky k-souvislý.*

Důkaz:
Sporem. Máme v grafu malý řez. Z definice.

Opačně, malý řez v $\mathcal{M}(G)$, minimalizujeme i počet komponent. Chvíli předpokládáme, že G_1 i G_2 je souvislý. Vytáhneme spor, můžeme nerovnost použít s rovností.

Máme tedy v každém kružnici, každá taková žije v jedné komponentě. Nechť tedy G_2 je ten nesouvislý. Vezmeme komponentu, která neobsahuje alespoň jednu kružnici. Přestrčím tuto komponentu z E_2 do E_1. Rank se na jedné straně zmenší přesně o rank té komponenty, na druhé straně vzroste nejvýše o to. Stále máme k'-separátor. Musí mít ale méně komponent, proto spor.

☻

E_1, E_2 rozklad hran, $|V(G[E_1]) \cap V(G(E_2)| = k$, $|E_1|, |E_2| \geq k$.

Tutteovský řez je buď vrcholový nebo cyklický.

Věta 8 *G je souvislý. Je tutteovsky k-souvislý když $\mathcal{M}(G)$ je tutteovsky k-souvislý.*

Důkaz:
Zase dvěma spory.

☻

Věta 9 *$\mathcal{M}, \lambda(\mathcal{M}) < \infty$. Potom $\lambda(\mathcal{M}) = \min \kappa(\mathcal{M}), g(\mathcal{M}$, kde g je obvod – délka minimální kružnice.*

Důkaz:
$\lambda(\mathcal{M}) \leq \kappa(\mathcal{M})$. Dále, $\lambda(\mathcal{M}) \leq \gamma(\mathcal{M})$. Pokud zbytek grafu obsahuje nějakou kružnici, pak také $\leq g(\mathcal{M})$.

☻

Důsledek 4 *G souvislý, $|V| \geq 3$, není to trojúhelník. Potom $\lambda(\mathcal{M}(G)) = \{\kappa(G), g(G)\}$.*

Chceme minimalizovat počet nezávislých množin na pokrytí. To je $\forall E' \subseteq E; |E'| \leq k \cdot r(E)$.

Maximální průměrný stupeň $mad(G) = \max_{G' \subseteq G} \frac{2 \cdot |E(G')|}{|V(G)|}$.

Když ho chceme najít, tak ho hledáme mezi hodnotami $\frac{2k}{l}$. Chceme nejmeníš, co je alespoň tak velký jako mad.

$mad(G) \leq 2k \Leftrightarrow$ lze najít k nezávislými z $\mathcal{M}^{+}(G)$. Představme si, že máme matroid $\mathcal{M}$ a jeho standardní reprezentaci. ***Pivotace*** je výběr prvkku matice a zeliminování podle něho. Toto zachovává matroid, jen vyměňuje prvek v bázi. Lze jen s těmi, které jsou na fundamentální kružnici.

Věta 10 *Matroid $\mathcal{M}$ je binární $\Leftrightarrow$ nemá minor $U_{2,4}$.*

Důkaz:
$U_{2,4}$ není binární, proto nic, co ho má jako minor.

Opačně, nechť $\mathcal{M}$ je minorově minimální nebinární matroid a BÚNO $2r(\mathcal{M}) \leq |E|$ (jinak můžu udělat duál). Neobsahuje smyčky a paralelní hrany (stejně nedělají problém). B je máze, D je matice incidence fundamentálních kružnic vzhledem k B. Toto by byla reprezentace, pokud by byl binární. Existuje B' taková, že fundamentální kružnice vzhledem k B' nejsou korektně reprezentovány. Má tedy dva sloupce, tedy má nejvýše 4 elementy (jinak by byla moc malá báze, kvůli předpokladu na rank). Ale má alespoň jeden element.

☻

Lemma 15 *$\mathcal{M}$ je binární matroid, $C \in \mathcal{C}; C^* \in \mathcal{C}^*; \Rightarrow |C \cap C^*|$ je sudý.*

Důkaz:
Pokud je to nula, tak OK.

Jinak, máme x z průniku. Bude se koukat, jeden prvek s jedničkou v bázi, musí se posčítávat na 0 v řádku i ve sloupečku.

☻

Lemma 16 *Symetrický rozdíl kružnic je disjunktní sjednocení kružnic.*

Důkaz:
Vidět ze součtů sloupečků, ty musejí vyjít 0.

☻

Věta 11 *Pro matroid $\mathcal{M}$ je ekvivalentní:*

- $\mathcal{M}$ *je binární.*
- $\forall C \in \mathcal{C}; \forall C^* \in \mathcal{C}^*; |C \cap C^*|$ *sudý.*
- *Symetrický rozdíl* 2 *kružnic obsahuje kružnici.*
- *Symetrický rozdíl* 2 *kružnic je disjunktní sjednocení kružnic.*
- *Totéž pro libovolné systémy kružnic.*
- *Pro každou bázi a* $\forall C \in \mathcal{C}$ *je* C *symetrický rozdíl fundamentálních kružnic vzhledem k* B *přes všechny prvky* $C \backslash B$.
- *Existuje báze taková, že platí předchozí.*

Tvrzení 11 F_7 *a jeho duál jsou zakázané minory pro všechna tělesa kromě těles charakteristiky* 2.

Věta 12 *U* GF_3 *jjsou zakázané minory* $F_7, F_7^*, U_{2,5}, U_{3,5}$.

Věta 13 q *je mocnina prvočísla,* $\mathcal{M}$ *je mtroid ranku* r *nereprezentovatelný nad* GF_q *bez smyček a paralelních prvků. Potom je omezený počet prvků.*

4 Ternární matroidy

4.1 Totálně unimodulární matice

A je ***totálně unimodulání*** matice (bude nad $\mathbb{R}$), pokud pro každou její čtvercovou podmatici platí, že její determinant je buď 0, ± 1. Tedy, i prvky jsou $0, \pm 1$.

$\mathcal{M}$ je unimodulární, pokud je reprezentovatelný nad $\mathbb{R}$ pomocí totálně unimodulární matice.

Lemma 17 *A je totálně unimodulární matice. Potom pivotací získáme opět totálně unimodulární matici.*

Důkaz:
Jediné, co se může změnit na determinantu, je jeho znaménko, pomocí násobení. Je potřeba rozmyslet, co se bude dít, když pivot je mimo. Ale pak je tam můžu přidat a tvářit se na to.

☻

Lemma 18 *Duál unimodulárního matroidu je opět unimodulární.*

Důkaz:
Transpozice bude zachovávat determinanty podmatic.

☻

Lemma 19 *Minory zachovávají unimodularitu.*

Důkaz:
Vynechání jen omezí množinu podmatic. A kontrakce je vynechání v duálu.

☻

Lemma 20 *$\mathcal{M}$ je binární a $[I_r|D_1]$ je jeho reprezentace nad M s prvky $0, 1, -1$ a $[I_r|D_2]$ vznikne pivotací z $[I_r|D_1]$. Potom jsou prvky jen $0, \pm 1$.*

Důkaz:
Rozbor případů.

☻

Věta 14 *Následující charakteristiky $\mathcal{M}$ jsou ekvivalentní:*

- *$\mathcal{M}$ je unimodulární.*
- *$\mathcal{M}$ je regulární (reprezentovateléné $\forall \mathbb{F}$ tělesa).*
- *$\mathcal{M}$ binární a $\mathbb{F}$-reprezentovatelné pro nějaké těleso $\mathbb{F}$ charakteristiky $\neq 2$.*

Důsledek 5 *$\mathcal{M}$ je regulární $\Leftrightarrow$ je binární a ternární.*

Věta 15 *Minory zakázané pro regulární matroidy jsou $U_{2,4}, F_7, F_7^*$*

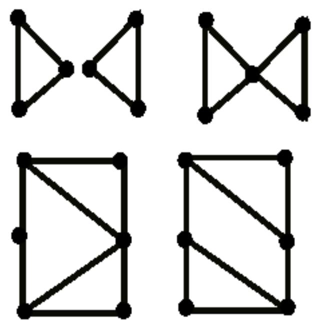
Plyne ze zakázaných pro binární a ternární, jen vyházu to, co už není potřeba.

5 Grafové minory

$G(V, E), X \subseteq E; r(X) = |V| - C(V, X)$

Budeme brát jen grafy bez smyček a izolovaných vrcholů.

Zatímco graf určuje matroid jednoznačně, opačně to neplatí. Např. můžu mít dva grafy se stejným matroidem, viz:



Tedy, můžu identifikovat vrchol různých komponent (opačně, rozdělit artikulaci) a protočit v 2-řezu.

Lemma 21 *G je 3-souvislý graf, H je bez izolovaných vrcholů a $\mathcal{M}(G) = \mathcal{M}(H)$. Potom $G \cong H$.*

Důkaz:
Minimální hranový řez G je kokružnice v $\mathcal{M}(G)$. Doplněk je nadrovina v $\mathcal{M}(G)$. Potom $H \subseteq E$ je souvislá nadrovina $\mathcal{M}(G)$. $E \backslash H$ je incidentní s jedním vrcholem. Tedy G indukuje izomorfní graf s H.

☻

Věta 16 (Whitney) *Nechť G, H jsou grafy, $\varphi(E(G)) \to \varphi(E(H))$ isomorfizmus $\mathcal{M}(G)$ a $\mathcal{M}(H)$. Tak lze G použitím operací na začátku kapitoly převést na H. Navíc, jsou-li G, H 2-souvislé, používáme pouze přetáčení.*

Věta 17 *Máme G graf a $\mathcal{M}$ matroid. $\mathcal{M} \cong \mathcal{M} * G \Leftrightarrow r(\mathcal{M}) = r(\mathcal{M}(G)) \wedge$ každý elementární řez je sjednocení kokružnic $\mathcal{M}$.*

Důkaz:
Jedním směrem triviální.

Opačně indukcí podle počtu prvků. Nosná množina je $|E|$. Búno G je souvislý. Předpokládejme, že nejsou stejné, ale tamto platí.

☻

5.1 Testování binarity

Vezmeme $k \in \mathbb{N}, k \geq 3$ a množinu $E\{x_1, \ldots, x_k, y_1, \ldots y_k\}$ a $\mathcal{C}_\infty \{\{x_i, x_j, y_i, y_j\}; i \neq j\}, \mathcal{C}_\in = \{\{z_1, \ldots, z_k\}; z_i \in \{x_i, y_j\}; \{z_1, \ldots, z_k\} \cap \{y_1, \ldots, y_k\}$ je sudé $\}$.

Toto je binární matroid.

6 Grafové šířky

Viz např. minory.

Nyní u brandwidth budeme definovat:

šířka hrany $e = r(E_1) + r(E_2) - r(E) + 1$ (hrana rozkladu) – při rozkladu na (E_1, E_2) po odebrání e z rozkladu. Nyní se to ale liší od grafové šířky, liší se, pokud má graf most, pokud nemá, potom se rovnají.

Branchwidth matroidu a jeho duálu jsou stejné.

Nechť $k \geq 1$. k-rozklad matroidu bude strom, kde všechny vnitřní kromě kořene mají stupeň 3, kořen má stupeň 2 (binární zakořeněný strom). Uděláme bijekci mezi prvky matroidu a listy, označím si smyčky. Pro vnitřní máme funkci φ_v, která dvojici čísel $(0 \ldots k)^2 \to 0 \ldots k$ a $\varphi_v^r : (0 \ldots k)^2 \to \mathbb{N}_0$.

Když chci spočítat rank, tak obarvím prvky množiny 1, jinak 0. Listy obarvené 1, které nejsou smyčky označím značkou 1. Všechny ostatní dostanou značku 0.

Barva vnitřního γ bude $\varphi_v(\gamma_1, \gamma_2)$ a značka $\lambda := \lambda_1 + \lambda_2 - \varphi_v^r(\gamma_1, \gamma_2)$. Pokud vždy v kořeni najdeme rank, tak to je dekompozice. Dekompoziční šířka je nejmenší k, pro které existuje funkční dekompoziční strom.

To jde někdy, protože můžu vždycky mít exponenciálně mnoho barev, tak do toho můžu zakódovávat celé množiny.

Věta 18 *$\mathcal{M}$ reprezentovatelný nad konečným tělesem $\mathbb{F}, |\mathbb{F}| = q$. $mbw(\mathcal{M}) \geq 1$, potom existuje k-dekompozice $\mathcal{M}$, kde $k = \frac{q^{k+1} - q(k+1) + k}{(q-1)^2}$. Je-li dán rozklad, najdu k-dekompozici v čase $O(n^{1+\alpha}$, kde α je exponent u násobení matic.*

Důkaz:
Kořen vrazím do libovolné hrany. W_v je lineární obal listů podstromu zakořeněného ve v. W_v' je lineární obal ostatních listů. $D_v = W_v \cap W_v'$. Dimenze tohoto je nejvýše k. Mám nejvýše $\sum_{i=1}^{k} \frac{q^i - 1}{q-1} + 1$ různých podprostorů.

☻