NOPT048: Optimalizační metody - LS 2012 Jiří Sgall

Matroidy

18. 5. 2012, 13. přednáška *Zapsal: Pavel Taufer, Jakub Hajič*
Poslední změna: 16. června 2012

1 Úvodní definice

Definice 1. Dvojice (X, $\mathcal{S}$), X je množina, $\mathcal{S} \subseteq 2^X = \mathcal{P}(X)$, je **matroid**, právě tehdy když platí:

- I1: $\emptyset \in \mathcal{S}$
- I2: $A \in S, A' \subseteq A \Rightarrow A' \in \mathcal{S}$
- I3: $U, V \in \mathcal{S}, |U| > |V| \Rightarrow \exists x \in U - V : V \cup x \in \mathcal{S}$ (Výměnný axiom)

Definice 2. Matroidy $M = (X, \mathcal{S}), M' = (X', \mathcal{S}')$ jsou **izomorfní**, pokud $\exists h$ bijekce $X \rightarrowtail\!\!\!\rightarrow X'$: $y \in \mathcal{S} \Leftrightarrow h(y) \in \mathcal{S}'$

Definice 3. M je matroid **reprezentovatelný** nad tělesem $\mathbb{F}$, existuje-li izomorfní vektorový matroid nad $\mathbb{F}$.

Pozn.: Prvky $\mathcal{S}$ se nazývají nezávislé množiny, maximální nezávislé množiny se nazývají báze matroidu.

2 Příklady

2.1 Matroid nad vektorovým prostorem

Buď A matice nad tělesem $\mathbb{F}$, X množina sloupců matice A, $\mathcal{S} = \{Y \subseteq X \mid Y \text{ je lineárně nezávislá}\}$ pak (X, S) je vektorový matroid (I1, I2 triviálně splněno, I3: Výměnný axiom odpovídá Steinitzově větě o výměně).

2.2 Grafové matroidy

Buď $G = (V, E)$ graf, $X = E$, $\mathcal{S} = \{E' \subseteq E \mid E' \text{ acyklická}\}$

I1, I2 triviálně splněno, I3: Buďte E_1, $E_2 \in \mathcal{S}$, $|E_1| < |E_2|$, pak (V, E_1) má nějaké $(2...n)$ komponenty souvislosti, E_2 má alespoň jednu hranu mimo tyto komponenty (z $|E_2| > |E_1|$, pokud E_1 je kostra G, pak takové E_2 neexistuje), tedy tuto hranu z E_2 lze přidat do E_1. QED

2.3 Fanův matroid

F_7 vektorový matroid nad $\mathbb{F}_2 = (0, 1, \bullet_2, +_2)$

matice $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$

F_7 odpovídá Fanově projektivní rovině (sloupce matice jsou jednotlivé body a na přímkách platí, že součet dvou bodů je roven třetímu modulo 2).

3 Další definice

Definice 4. Buď $(X, \mathcal{S})$ matroid, $A \subseteq X$, pak **řád množiny** A je maximální nezávislá podmnožina Z množiny A. $(= max|Z|, Z \subseteq A, Z \in S)$

Pozn.: Buď A matice, $(X, \mathcal{S})$ vektorový matroid nad A, pak $r(X) = \text{rank}(A)$.

Pozn.: Buď $G = (V, E)$ souvislý graf, $(X, \mathcal{S})$ grafový matroid nad G, pak $r(X) = |V| - 1$ (maximální acyklická množina, tj. kostra, má vždy o jednu hranu méně, než je počet vrcholů).

Pozorování 5. *Matroidy jsou přesně dědičné systémy, kde lze definovat řád podmnožin pomocí maximality vzhledem k inkluzi takto: Buď X množina, $\mathcal{A} \subseteq 2^X$ množinový systém, pak buď řád množiny $Y \subseteq X$ definován jako $\max |Z|$, $Z \subseteq Y$, $Z \in \mathcal{A}$, kde max je maximalita vzhledem k uspořádání inkluzí. Tohle nemusí být korektní definice, pokud jsou (vzhlede. k inkluzi) maximální množiny různě velké, na matroidech však platí:*

Pozorování 6. *$(X, \mathcal{S})$ je matroid právě když platí podmínky I1, I2, I3', kde podmínka I3' je: Buď $A \subseteq X$, dále buďte Y_1, $Y_2 \subseteq A$, Y_1, Y_2 maximální vzhledem k inkluzi, potom $|Y_1| = |Y_2|$.*

Důkaz. "I3 $\Rightarrow$ I3$'$": sporem: BÚNO $|Y_1| > |Y_2| \Rightarrow$ dle I3 $\exists x \in Y_1 - Y_2$, $Y_2 \cup x \in S \Rightarrow$ SPOR s maximalitou Y_2

"I3$'$ $\Rightarrow$ I3": obměna I3 říká, že je-li BÚNO $|Y_1| > |Y_2|$, pak $|Y_2|$ není maximální, tedy $\exists x \in A - Y_2, Y_2 \cup \{x\} \in \mathcal{S}$, speciálně pro $A = Y_1 \cup Y_2$ je pak $x \in Y_1$, tedy i pro obecné A obsahující Y_1, Y_2 je možné přidat x z Y_1, což vyžaduje I3. QED. $\square$

Pozorování 7. *Buď X množina, pak $r\colon \mathcal{P}(X) \to \mathbb{N}_0$ je řádová funkce matroidu $\Leftrightarrow$ r splňuje podmínky R1, R2, R3*

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

Důkaz. "$\Rightarrow$": (Matroidy splňují R1, R2, R3)

R1 triviálně

R2: $Z : max|Z|, Z \subseteq \mathcal{S}, Z \subseteq Y$, pak přidání prvku do Y nemůže Z jakožto $\subseteq Y$ zvětšit o víc než o 1

R3: sporem: Buďte Z' max nezávislá $\subseteq Y \cup \{y, z\}$, Z max. nezávislá $\subseteq Y$ (též max nezávislá $\subseteq Y \cup \{y\}$ a max. nezávislá $\subseteq Y \cup \{y\}$). Dále pro spor nechť $|Z'| > |Z|$. Pak podle I3 $\exists x \in (Z' - Z), Z \cup \{x\} \in \mathcal{S}$. Ovšem zároveň platí jedna ze tří možností:

- $x \in Y \Rightarrow$ spor s maximalitou $|Z|$ v Y
- $x = y \Rightarrow$ spor s maximalitou $|Z|$ v $\subseteq Y \cup \{y\}$
- $x = z \Rightarrow$ spor s maximalitou $|Z|$ v $\subseteq Y \cup \{z\}$

"$\Leftarrow$": definujme matroid tak, že r je jeho řádová funkce, $A \subseteq X$ je nezávislá ($A \in \mathcal{S}$) jestliže $r(A) = |A|$. Takto definovaný systém splňuje I1 (triviálně). I2: Buď $A' = A$ po odebrání libovolného prvku x, pak zjevně $r(A') \leq |A| - 1 = r(A) - 1$ (z R2 indukcí plyne $r(C) \leq |C|$). Ale z R2 také plyne, že při vrácení x do A' r stoupne maximálně o 1, tedy $r(A') \geq r(A) - 1$, tedy celkem $r(A') = r(A) - 1 = |A| - 1 = |A - \{x\}| = |A'|$.

I3: Buďte $U, V \in \mathcal{S}$, $r(U) = |U|$, $r(V) = |V|$, $|U| > |V|$. Pak pro libovolné $y \in U - V$ platí jedna ze dvou možností:

- a) $r(V \cup \{y\}) > r(V)$.
- b) $r(V \cup \{y\}) = r(V)$.

Situace b) ale nemůže nastat $\forall y \in U - V$, neboť pak podle R3 $r(V) = r(V \cup U - V) = r(U)$. Tedy $\exists y$, takové, že platí a) , pak podle R2 $r(V \cup \{y\}) = r(V)+1 = |V \cup \{y\}|$, tedy $V \cup \{y\} \in S$, což jsme chtěli dokázat. QED.

$\square$

Pozorování 8. *Buď X množina, $r\colon \mathcal{P}(X) \to \mathbb{N}_0$ je řádová funkce matroidu $\Leftrightarrow$ platí podmínky R1', R2', R3':*

- *R1':* $0 \leq r(Y) \leq |Y|$
- *R2':* $Z \subseteq Y \Rightarrow r(Z) \leq r(Y)$
- *R3': submodularita* $: Y, Z \subseteq X \Rightarrow r(Y) + r(Z) \geq r(Y \cup Z) + r(Y \cap Z)$

Důkaz. R1$'$, R2$'$ plyne z R1, R2 triviálně.

"R3 $\Rightarrow$ R3$'$": Buďte Y, $Z \in \mathcal{P}(X)$ Dále buďte B max. nez. $\subseteq Y \cap Z$, $B_Y \supset B$, B_Y max. nez. $\subseteq Y$, $B_Z \supset Z$, B_Z max. nez. $\subseteq Z$. Pak $r(Y)+r(Z) \geq |B_Y|+|B_Z| = |B_Y \cap B_Z|+|B_Y \cup B_Z| = |B| + |B_Y \cup B_Z| = r(Y \cap Z) + |B_Y \cup B_Z|$. Zbývá ukázat, že $|B_Y \cup B_Z| \geq r(Y \cup Z)$, ukažme sporem:

Nechť $\exists Q$, Q max. nez. $\subseteq Y \cup Z$, $|Q| > |B_Y \cup B_Z|$. Pak podle I3 $\exists x$, $x \in Q$, $B_Y \cup B_Z \cup x \in S$. Tedy $x \in Z$ nebo $x \in Y$, dále $Q \cap Z$ je nezávislá a $Q \cap Y$ je nezávislá Tedy buď $x \in (Q \cap Z) - B_Z$ nebo $x \in (Q \cap Y) - B_Y$, ale to je spor s maximalitou B_Y v Y nebo B_Z v Z.

Opačná implikace: R1 z R1$'$, R2 z R2$'$ (první $\leq$) a R3$'$ (druhá $\leq$). R3 jako DÚ. $\square$

4 Úloha diskrétní optimalizace

Definice 9. Úloha diskrétní optimalizace: $(X, \mathcal{A}), \mathcal{A} \subset 2^X, w : X \to \mathbb{Q}, A \subseteq X \Rightarrow w(A) = \sum_{x \in A} w(x)$. Cílem je nalézt $Y \subset \mathcal{A}$ takovou, že $w(Y)$ je maximální.

Definice 10. Hladový algoritmus:

(i) Seřaď $X = x_1, x_2, ..., x_n$ tak, že $w(x_1) \geq w(x_2) \geq \; \geq w(x_n)$

(ii) $J := 0$

(iii) for $i = 1..n$ do:

  if $J \cup \{x_i\} \in S \wedge w(x_i) \geq 0 : J := J \cup \{x_i\}$

 endfor.

Věta 11. *Nechť $(X, \mathcal{S})$ je dědičný množinový systém, $S \neq \emptyset$. Potom pro každé $w\colon X \to Q$ najde hladový algoritmus optimální řešení $\Leftrightarrow$ $(X, \mathcal{S})$ je matroid.*

Důkaz. "$\Leftarrow$" obměnou: I1, I2 platí z podmínek věty $\Rightarrow$ ($(X, \mathcal{S})$ není matroid $\Rightarrow$ $I3'$ neplatí). Tedy $\exists A, B$ různé maximální nezávislé podmnožiny vhledem k inkluzi, BÚNO $|A| > |B|$. Mějme w definované následovně:

- $w(x) < 0$ pro $X \notin A \cup B$

- $w(x) = b > 0$ pro $X \in B$
- $w(x) = a > 0$ pro $X \in A - B, a < b$.

Tedy hladový algoritmus najde nejprve postupně všechna $x \in B$, pak už se mu B nepodaří rozšířit tedy vrátí B, neboli hodnotu $w(B) = b * |B|$. Ale $w(A) = a * |A - B| + b * |B \cap A|$, volme tedy a, b tak, aby $a * |A - B| > b * |B - A|$, tedy $a > b * \frac{|B-A|}{|A-B|}$, ale protože $|A| > |B|$, tak to lze i při dodržení podmínky $a < b$.

"$\Rightarrow$": ponecháno na příští přednášku... $\square$