Osnovno o Matroidih

Davorin Učakar

25. maja 2007

1 Postulati

Matroide si lako predstavljamo na več različnih načinov, saj v raznih vejah matematike najdemo strukture, ki tvorijo matroide. Najenostavnejša primera matroida sta končna množica vektorjev skupaj z družino svojih linearno neodvisnoh podmnožic in končen graf skupaj z družino vseh svojih podgrafov, ki so brez ciklov.

Ker se matroidi pojavljajo na tako različnih področjih, se izkaže, da je tudi načinov, kako definirati matroid, kar precej. Nekaj si jih bomo ogledali v nadaljevanju.

Matroid $M = (S, \mathcal{I})$ definiramo kot končno množico S skupaj z družino $\mathcal{I} \subseteq 2^S$, za katero velja:

1. $\emptyset \in \mathcal{I}$.
2. Če je $X \in \mathcal{I}$ in $Y \subseteq X$, potem je tudi $Y \in \mathcal{I}$.
3. Če sta $X, Y \in \mathcal{I}$ in velja $|X| = |Y| - 1$, potem obstaja tak $y \in Y \backslash X$, da je $X \cup \{y\} \in \mathcal{I}$.

Množicam iz $\mathcal{I}$ pravimo *neodvisne množice* matroida M.

Množica $B \in \mathcal{B}$ je *baza* matroida M, če je neodvisna in ni prava podmnožica nobene neodvisne množice. Družino vseh baz matroida M označimo z $\mathcal{B}$.

Za vsako podmnožico $X \subseteq S$ definiramo *rang* množice X kot

$$\rho(X) = \max\{|Y|; Y \in \mathcal{I}, Y \subseteq X\} \ .$$

Rang matroida M je $\rho(S)$.

Izrek 1.1 (Dopolnitveni izrek) *Če sta X in Y neodvisni množici matroida M in $|X| < |Y|$, potem obstaja množica $Z \subseteq Y \backslash X$, da je $|X \cup Z| = |Y|$ in $X \cup Z$ neodvisna množica.*

Dokaz: Naj bo Z_1 po moči maksimalna med takšnimi množicami Z, za katere velja $Z \subseteq Y \backslash X$ in $X \cup Z \in \mathcal{I}$. Takšna množica očitno obstaja, saj že prazna množica zadostuje temu pogoju.

Recimo, da je $|X \cup Z_1| < |Y|$. Naj bo $Y_1 \subseteq Y$ takšna, da je $|X \cup Z_1| + 1 = |Y_1|$. Po točki (2) iz definicije matroida je $Y_1 \in \mathcal{I}$ in po (3) obstaja nek $y \in Y_1 \backslash (X \cup Z_1)$, da je

$(X \cup Z_1) \cup \{y\} \in I$. Nova množica $Z_1 \cup \{y\}$ tudi zadostuje zgornjim zahtevam za Z in, ker je $|Z_1| < |Z_1 \cup \{y\}|$, Z_1 ni maksimalna in imamo protislovje.

Torej je $|X \cup Z_1| \geq |Y|$. Ker je $|X| < |Y|$, mora obstajati $Z_2 \subseteq Z_1$, da je $|X \cup Z_2| = |Y|$. Po (2) iz definicije matroida je očitno $X \cup Z_2 \in \mathcal{I}$, torej je to naša iskana množica Z. ∎

Iz tega izreka očitno sledi naslednja posledica:

Posledica 1.2 *Vse baze matroida M imajo enako moč in ta je enaka rangu matroida M.*

Če bi namreč imeli dve bazi različnih moči, bi lahko eno povečali po dopolnitvenem izreku in zato ne bi bila baza, saj bi bila prava podmnožica neke neodvisne množice. Zato so baze po moči največje neodvisne množice v matroidu in je torej njihova moč enaka rangu tega matroida.

Iz tega izreka pa tudi vidimo, da lahko katerokoli neodvisno množico dopolnimo z elementi iz neke baze in tako dobimo novo množico, ki je spet baza. Torej je vsaka neodvisna množica podmnožica neke baze.

Izrek 1.3 (Izmenjalni aksiom) *Če sta $B_1, B_2 \in \mathcal{B}$ in $x \in B_1 \backslash B_2$, potem obstaja nek $y \in B_2 \backslash B_1$, da je $B_1 \backslash \{x\} \cup \{y\} \in \mathcal{B}$.*

Izmenjalni aksiom sledi iz prej definiranih aksiomov za matroid, če za neodvisni množici $B_1 \backslash \{x\}$ in B_2 uporabimo točko (3).

Neodvisne množice matroida določajo družino baz. Velja tudi obratno; če družino baz definiramo z izmenjalnim aksiomom, ta določa družino neodvisnih množic

$$\mathcal{I} = \{X; \exists B \in \mathcal{B} : X \subseteq B\}.$$

Da bo definicija dobra, mora ta družina zadoščati aksiomom za matroid.

Izrek 1.4 *Naj bo $\mathcal{B}$ neprazna družina podmnožic končne množice S, ki zadostuje izmenjalnemu aksiomu. Tedaj je $\mathcal{B}$ družina baz matroida M nad S, katerega družina neodvisnih množic je določena z*

$$\mathcal{I} = \{X; \exists B \in \mathcal{B} : X \subseteq B\}.$$

Dokaz: Najprej pokažimo, da imajo vse baze enako moč. Predpostavimo, da je nimajo. Izberimo $B_1, B_2 \in \mathcal{B}$ tako, da bo $|B_1| > |B_2|$ in bo imel $B_1 \backslash B_2$ najmanjšo moč. Naj bo $x \in B_1 \backslash B_2$. Zaradi 1.3 obstaja $y \in B_2 \backslash B_1$, da je $B_3 := (B_1 \backslash \{x\}) \cup \{y\} \in \mathcal{B}$. To pa je protislovje, saj ima $B_3 \backslash B_2$ manj elementov kot $B_1 \backslash B_2 = B_3 \backslash B_2 \oplus \{x\}$, kjer $\oplus$ označuje disjunktno unijo. Torej so vse množice v $\mathcal{B}$ enake moči.

Naj bo $\mathcal{I}$ določen kot v izreku. Preveriti moramo če se sklada z definicijo matroida. Točki (1) in (2) sta očitni. Naj bosta sedaj $I_1, I_2 \in \mathcal{I}$ in $|I_1| = |I_2| - 1$. Torej je $I_1 \subseteq B_1$ in $I_2 \subseteq B_2$, za neka $B_1, B_2 \in \mathcal{B}$. Radi bi našli $y \in I_2 \backslash I_1$, da bo $I_1 \cup \{y\} \subseteq B_3$ za nek $B_3 \in \mathcal{B}$. Najprej dopolnimo I_1 do B_1 in I_2 do B_2:

$$B_1 = I_1 \oplus \{l_1, l_2, \ldots, l_s\}, \quad B_2 = I_2 \oplus \{k_1, k_2, \ldots, k_t\}.$$

Ker imajo vse baze enako moč, je $s = t + 1$. Če je $I_2 \cap \{l_1, l_2, \ldots, l_s\}$ neprazen, je iskani y poljuben element tega preseka, saj je $I_1 \cup \{y\} \subseteq B_1$.

V nasprotnem primeru pa obstaja $l_i \in B_1 \backslash B_2$ za nek i. Po izmenjalnem aksiomu obstaja $y \in B_2 \backslash B_1$, da velja $B_3 := (B \backslash \{l_i\}) \cup \{y\} \in \mathcal{B}$. Baza B_3 ima z B_2 več skupnih elementov kot B_1, zato se ta postopek enkrat konča. Takrat je $I_2 \cap \{l_1, l_2, \ldots, l_s\}$ neprazen, zato se prevede na prejšnji primer. ∎

Matroid pa lahko definiramo tudi na podlagi funkcije ranga. Ker pa tega ne bomo potrebovali v nadaljevanju, je dokaz izpuščen. Tako bomo le dokazali, da za funkcijo ranga veljajo naslednji izreki, ne pa tudi, da so funkcije, ki zadoščajo naslednjim izrekom funkcije ranga nekega matroida.

Izrek 1.5 *Naj bo ρ funkcija ranga matroida M. Tedaj za vsak $X \subseteq S$ in za poljubna elementa $y, z \in S$ velja:*

1. $\rho(\emptyset) = 0$.
2. $\rho(X) \leq \rho(X \cup \{y\}) \leq \rho(X) + 1$.
3. *Če je $\rho(X \cup \{y\}) = \rho(X \cup \{z\}) = \rho(X)$, potem je $\rho(X \cup \{y\} \cup \{z\}) = \rho(X)$.*

Dokaz: Lastnosti (1) in (2) sledita direktno iz definicije ranga. Pokažimo sedaj lastnost (3). Recimo, da je $\rho(X \cup \{y\} \cup \{z\}) > \rho(X)$. Tedaj iz točke (2) sledi $\rho(X \cup \{y\} \cup \{z\}) = \rho(X \cup \{y\}) + 1 = \rho(X) + 1$. Ker se množici razlikujeta le za element $\{z\}$, mora biti ta vsebovan v vsaki maksimalni neodvisni podmnožici $X \cup \{y\} \cup \{z\}$. Naj bo X_1 maksimalna neodvisna množica v X in X_2 maksimalna neodvisna množica v $X \cup \{y\} \cup \{z\}$. Tedaj lahko po definiciji matroida najdemo nek $w \in (X \cup \{y\} \cup \{z\}) \backslash X = \{y, z\}$, da je $|X_1 \cup \{w\}| = |X_2| = \rho(X \cup \{y\} \cup \{z\})$. Brez škode splošnosti recimo, da je $z = y$. To pa je protislovje, saj vemo, da je $X_1 \cup \{y\} \subseteq X \cup \{y\}$ in zato $|X_1 \cup \{y\}| = \rho(X \cup \{y\}) = \rho(X) = \rho(X \cup \{y\} \cup \{z\}) - 1$. ∎

Za naslednji izrek se izkaže, da je ekvivalenten zgornjemu, zato bi lahko tudi na podlagi tega definirali matroid. Dokaz ekvivalence izpuščamo.

Izrek 1.6 *Naj bo ρ funkcija ranga matroida M. Tedaj za vsak $X \subseteq S$ in za poljubna elementa $y, z \in S$ velja:*

1. $0 \leq \rho(X) \leq |X|$.
2. *Če je $X \subseteq Y$, je $\rho(X) \leq \rho(Y)$.*
3. $\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$.

Lastnost (2) iz zgornjega izreka imenujemo *monotonost*, lastnost (3) pa *submodularnost* funkcije ρ.

Dokaz: Lastnosti (1) in (2) očitno sledita iz definicije ranga. Naj bo $I \subseteq X \cap Y$ neodvisna množica, za katero velja $|I| = \rho(I) = \rho(X \cap Y)$. Po dopolnitvenem izreku lahko I dopolnimo do neke maksimalne neodvisne podmnožice $J \subseteq X \cup Y$. Sedaj lahko zapišemo

$J = I \oplus A \oplus B$, kjer sta $A = J \cap (X \backslash Y)$ in $B = J \cap (Y \backslash X)$ neodvisni množici. Ker sta $I \oplus A$ in $I \oplus B$ neodvisni, velja:

$$\begin{aligned} \rho(X) + \rho(Y) &\geq |I \oplus A| + |I \oplus B| \\ &= 2|I| + |A| + |B| \\ &= |I| + |I \oplus A \oplus B| \\ &= \rho(X \cap Y) + \rho(X \cup Y). \end{aligned}$$

■

2 Operator zaprtja

Naj bo S končna množica. Tedaj je *operator zaprtja* predpis $\sigma : 2^S \to 2^S$, ki ima naslednje lastnost:

1. $X \subseteq S \Rightarrow X \subseteq \sigma(X)$;
2. $X \subseteq Y \subseteq S \Rightarrow \sigma(X) \subseteq \sigma(Y)$;
3. $X \subseteq S \Rightarrow \sigma(X) = \sigma(\sigma(X))$.

Za operator zaprtja na matroidih običajno uporabimo naslednji predpis:

$$\sigma(X) = \{x \in S; \rho(X \cup \{x\}) = \rho(X)\}.$$

Pokažimo, da ta predpis zadošča zgornjim lastnostim za zaprtje. Lastnost (1) je očitna. Lastnosti (2) tudi ni težko pokazati: videti moramo, da iz $X \subseteq Y$ in $\rho(X \cup \{x\}) = \rho(X)$ sledi $\rho(Y \cup \{x\}) = \rho(Y)$ za vsak $x \in \sigma(X)$. Če je $x \in Y$ je to očitno, sicer pa uporabimo submodularnost funkcije ranga 1.6(3) na množicah $X \cup \{x\}$ in Y:

$$\begin{aligned} \rho(Y \cup \{x\}) + \rho(X) &= \rho((X \cup \{x\}) \cup Y) + \rho((X \cup \{x\} \cap Y) \\ &\leq \rho(X \cup \{x\}) + \rho(Y) \\ &= \rho(X) + \rho(Y). \end{aligned}$$

Zaradi monotonosti ranga je torej enakost: $\rho(Y \cup \{x\}) = \rho(Y)$. Pri dokazu lastnosti (3) si bomo pomagali z naslednjo lemo:

Lema 2.1 *Če imamo operator zaprtja σ definiran z zgornjim predpisom, je za vsak $X \subseteq S$:*

$$\rho(X) = \rho(\sigma(X)).$$

Dokaz: Naj bo I maksimalna neodvisna množica v X in J maksimalna neodvisna množica v $\sigma(X)$. Recimo, da zgornja enakost ne velja, torej je $|I| < |J|$. Po definiciji obstaja $x \in J \backslash I$, da je $I \cup \{x\}$ neodvisna. To je očitno maksimalna neodvisna množica v $X \cup \{x\}$, zato velja:

$$\rho(X \cup \{x\}) = |I \cup \{x\}| = |I| + 1 = \rho(X) + 1,$$

vendar je $x \in \sigma(X)$, zato po definiciji σ velja $\rho(X) = \rho(X \cup \{x\})$. To pa je protislovje. ∎

Vsebovanost $\sigma(X) \subseteq \sigma(\sigma(X))$ sledi iz definicije zaprtja. Recimo, da je $\sigma(X) \subset \sigma(\sigma(X))$. Potem obstaja $z \in \sigma(\sigma(X)) \backslash \sigma(X)$. Ker $z \notin \sigma(X)$, z uporabo 1.5(2) dobimo $\rho(X \cup \{z\}) = \rho(X) + 1$. Po drugi strani je $\rho(\sigma(X) \cup \{z\}) = \rho(\sigma(X))$, saj je $z \in \sigma(\sigma(X))$. Torej velja:

$$\rho(X) + 1 = \rho(X \cup \{z\}) \leq \rho(\sigma(X) \cup \{z\}) = \rho(\sigma(X))$$

To pa je v protislovju s prejšnjo lemo.

3 Primeri matroidov

Vektorski matroidi. Naj so S končna množica vektorjev iz danega vektorskega prostora V. Če za $\mathcal{I}$ vzamemo linearno neodvisne podmnožice S, dobimo matroid. Vsak matroid, ki je izomorfen tako dobljenemu matroidu, imenujemo *vektorski matroid*.

Enakomerni matroidi Naj bosta k in n naravni števili in $0 \leq k \leq n$. Naj bo $|S| = n$ in $\mathcal{I}$ družina vseh njenih podmnožic s kvečjemu k elementi. $U_{n,k} = (S, \mathcal{I})$ je tedaj matroid. Baze so ravno vse množice moči k, rang $A \in \mathcal{I}$ pa je $\rho(A) = |A|$, če je $|A| \leq k$ oziroma $\rho(A) = k$, če je $|A| > k$. Matroidu $U_{n,k}$ pravimo *enakomerni matroid* ranga k.

Algebrajski matroidi. Recimo, da je $\mathbb{F}$ polje in K njegova razširitev. Potem so elementi $x_1, x_2, \ldots, x_k \in K$ *algebrajsko neodvisni*, če obstaja tak neničelni polinom $p \in \mathbb{F}[y_1, y_2, \ldots, y_k]$, da je $p(x_1, x_2, \ldots, x_k) = 0$.

Naj bo sedaj $S \subseteq K$ neka končna množica in $\mathcal{I}$ družina vseh njenih algebrajsko neodvisnih podmnožic. Izkaže se, da je dobljena struktura matroid.

Geometrijski matroidi. Geometrijske matroide konstruiramo podobno kot vektorske, le da namesto linearne neodvisnosti uporabimo afino; množica vektorjev $\{x_1, \ldots, x_k\} \subseteq \mathbb{R}^d$ je *afino neodvisna*, če za vsa števila $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$, ki zadostijo pogojema

$$\sum_{i=1}^{k} \lambda_i x_i = 0$$

in

$$\sum_{i=1}^{k} \lambda_i = 0,$$

sledi $\lambda_1 = \cdots = \lambda_k = 0$.

Naj bo S končna podmnožica $\mathbb{R}^d$ in $\mathcal{I}$ družina vseh afino neodvisne podmnožice iz S. Tedaj je $(S, \mathcal{I})$ matroid.

Grafovski matroidi. Naj bo G graf, ki ni nujno enostaven; dopuščamo tudi zanke. Naj bo $S = E(G)$. Družina $\mathcal{I} \subseteq 2^S$ vsebuje natanko tiste množice povezav, ki ne tvorijo nobenega cikla v grafu G. Dobljeni matroid $M(G) = (S, \mathcal{I})$ imenujemo *matroid ciklov* grafa G. Vsak matroid, ki je izomorfen matroidu ciklov kakega grafa, imenujemo *grafovski matroid*.

Baze v matroidu ciklov grafa G ustrezajo vpetim drevesom, če je G povezan, oziroma vpetim gozdovom, če graf G ni povezan. Naj bosta T in T' vpeti drevesi grafa G in $e = xy \in E(T)\backslash E(T')$. Če odstranimo povezavo e iz T, potem T razpade na drevesi T_1 in T_2. Pot v T' od x do y vsebuje neko povezavo $e' \neq e$, ki ima eno krajišče v T_1 in drugo v T_2. Torej je $(E(T)\backslash e) \cup e')$ spet vpeto drevo. Ker to velja za vsako komponento grafa G, velja tudi za vpete gozdove. Torej za vpete gozdove velja izmenjalni aksiom 1.3. Ker vsak graf vsebuje vpet gozd, po izreku 1.4 dobimo matroid. Podmnožice vpetih gozdov tako tvorijo $\mathcal{I}$. Rang podgrafa F definiramo kot $|E(H)|$, če je H največje vpeto drevo v F.

4 Požrešna metoda

Posplošimo Krusalkov algoritem za iskanje najcenejšega vpetega drevesa v grafu. Vpeta drevesa namreč ravno ustrezajo bazam matroida ciklov.

Naj bo $M = (S, \mathcal{I})$ matroid nad množico S. Recimo, da ima vsak element $x \in S$ *ceno* $w(x) \in \mathbb{R}$. Tedaj za poljubno množico $X \subseteq S$ definiramo *ceno* $w(X)$ kot

$$w(X) = \sum_{x \in X} w(x).$$

Problem iskanja najcenejšega vpetega drevesa se tako prevede na *problem najcenejše baze*. Za ta problem sestavimo naslednji postopek:

Naj bo B neodvisna množica, v katero bomo dodajali elemente in bo na koncu tvorila bazo, Y pa množica kandidatov za vstop v bazo, torej množica tistih elementov y, za katere je $B \cup \{y\} \in \mathcal{I}$. Na začetku je $B = \emptyset$ in $Y = S$. Dokler ni $Y = \emptyset$ ponavljamo naslednji postopek: iz Y izvzamemo vse tiste elemente y, za katere $B \cup \{y\} \notin \mathcal{I}$. Potem izberemo najcenejši $y \in Y$ in ga dodamo v B.

Zgornji postopek lahko še izboljšamo, tako da imamo elemente iz Y sortirane po ceni, da nam ni potrebno vsakokrat iskati najcenejšega elementa. Nadalje lahko za začetni Y vzamemo $S\backslash\sigma(\emptyset)$; če bi bila namreč za nek $y \in \sigma(\emptyset)$ množica $B \cup \{y\}$ neodvisna, bi bila tudi $\{y\}$ neodvisna, torej $\rho(\{y\}) = 1$. Ker pa je $y \in \sigma(\emptyset)$, bi veljalo $\sigma(\emptyset) \geq \rho(\{y\}) = 1$, kar pa je v nasprotju z lemo 2.1.

Izrek 4.1 *Požrešna metoda za iskanje najcenejše baze pri poljubnem matroidu M nad množico S in dani funkciji cene $w : S \to \mathbb{R}$ kot rezultat vrne najcenejšo bazo matroida M.*

Dokaz: Iz konstrukcije množice B je očitno, da je ta na koncu postopka neodvisna. Preprosto je videti tudi, da je B baza matroida M. Recimo, da B ni baza. Ker se da vsako neodvisno množico dopolniti do baze, velja $B \subset B'$ za neko bazo B'. Poljuben

$x \in B' \setminus B$ z B in vsako njeno podmnožico tvori neodvisno množico, torej ni mogel izpasti iz Y. Zato je $Y \neq \emptyset$ in postopek še ni zaključen.

Pokazati moramo še, da je B najcenejša baza. Recimo, da ni najcenejša baza. Tedaj obstaja baza B', za katero velja $w(B') < w(B)$. Med vsemi najcenejšimi bazami za B' izberemo tisto, ki ima največji presek z B. Recimo, da je postopek v B po vrsti dodajal elemente $x_1, \ldots, x_{|B|}$. Naj bo t najmanjši indeks, za katerega $x_t \notin B'$. Množica $B' \cup \{x_t\}$ očitno vsebuje natanko en cikel C. Ker je B brez ciklov, obstaja $y \in C \setminus B$. Sedaj lahko tvorimo novo bazo $B'' = (B' \cup \{x_t\}) \setminus \{y\}$. To je res baza, saj je enake moči kot B' in ne vsebuje cikla, ker smo izvzeli s povezavo y, ki leži na ciklu C. Ker je B' najcenejša baza, mora biti $w(B'') \geq w(B')$ in torej $w(x_t) \geq w(y)$. Opazimo, da je $\{x_1, \ldots, x_{t-1}, y\}$ neodvisna množica. Ker požrešna metoda na t-tem kotaku ni izbrala y, sledi $w(x_t) \leq w(y)$, torej velja enakost. Zato je tudi B'' najcenejša baza. Vendar B'' ima več skupnih elementov z B, kar je v nasprotju z našo izbiro baze B'. ∎

5 Literatura

- Bojan Mohar: *Teorija matroidov*, DMFA, Ljubljana, 1996.