Matroid Intersection a Matroid Partition Problem

Jan Volec

V tomto textu ukážeme vzájemnou ekvivalenci dvou velmi známých problémů z teorie matroidů a poté šikovným algoritmem dokážeme jeden z nich. Předpokládáme základní znalosti o matroidech, které čtenář může v případě zájmu najít např. v [1], [2], či [3].

Věta 1 (Matroid Intersection Problem)**.** *Pro libovolné matroidy $\mathcal{M}_1 = (E, \mathcal{I}_1)$ s řádovou funkcí r_1 a $\mathcal{M}_2 = (E, \mathcal{I}_2)$ s řádovou funkcí r_2 nad množinou E platí*

$$\max_{E' \in \mathcal{I}_1 \cap \mathcal{I}_2} |E'| = \min_{E_1 \cup E_2 = E} r_1(E_1) + r_2(E_2).$$

Slovy řečeno, velikost největší nezávislé množiny E' v matroidech $\mathcal{M}_1$ a $\mathcal{M}_2$ je stejná, jako velikost nejmenšího rozkladu nosné množiny E na dvě části E_1 a E_2, přičemž velikostí rozkladu rozumíme součet velikosti největší nezávislé množiny $I_1 \subseteq E_1$ v matroidu $\mathcal{M}_1$ s velikostí největší nezávislé množiny $I_2 \subseteq E_2$ v matroidu $\mathcal{M}_2$. V podstatě jde o zobecnění maximálního párování v bipartitních grafech a Königovy věty.

Všimněme si, že bez újmy na obecnosti můžeme předpokládat, že množiny E_1 a E_2 jsou disjunktní. Dále si všimněme, že nerovnost „$\leq$“ se dokáže jednoduše:

Pozorování 2. *Pro každou nezávislou množinu $E' \in \mathcal{I}_1 \cap \mathcal{I}_2$ a libovolný rozklad $E_1 \cup E_2 = E$ platí $r_1(E_1) + r_2(E_2) \geq |E'|$.*

Důkaz. Z monotónie řádové funkce vyplývá, že $r_1(E_1) \geq r_1(E_1 \cap E')$ a analogicky $r_2(E_2) \geq r_2(E_2 \cap E')$. Dále víme, že E' je nezávislou množinou $\mathcal{M}_1$ resp. $\mathcal{M}_2$, proto i $E_1 \cap E'$ resp. $E_2 \cap E'$ je nezávislou množinou $\mathcal{M}_1$ resp. $\mathcal{M}_2$. Platí tedy, že $r_1(E_1)+r_2(E_2) \geq r_1(E_1 \cap E')+r_2(E_2 \cap E') = |E_1 \cap E'|+|E_2 \cap E'|$. Nyní z toho, že E_1 a E_2 tvoří rozklad nosné množiny E, musí pro jakoukoli množinu $E' \subseteq E$ platit, že každý její prvek je v součtu $|E_1 \cap E'| + |E_2 \cap E'|$ započten alespoň jednou. Tím získáváme $|E_1 \cap E'| + |E_2 \cap E'| \geq |E'|$ a spojením všech nerovností dohromady pak $r_1(E_1) + r_2(E_2) \geq |E'|$. $\square$

Důkaz nerovnosti „$\geq$“ prozatím odložme a podívejme se na druhý problém. Než jej vyslovíme, budeme však potřebovat následující definici.

Definice 1 (Rozložitelná množina)**.** *Mějme matroidy $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ definované nad množinou E a se systémy nezávislých množin $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_k$. Řekneme, že množina $J \subseteq E$ je rozložitelná (vzhledem k matroidům $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$), pokud lze J zapsat jako sjednocení k částí $J_1, J_2, \ldots, J_k$, kde J_i je nezávislá množina v matroidu $\mathcal{M}_i$ pro všechna $i \in \{1, 2, \ldots, n\}$.*

Opět bez újmy na obecnosti můžeme předpokládat, že části J_i jsou po dvou disjunktní.

Věta 3 (Matroid Partition Problem)**.** *Buď $J \subseteq E$ největší rozložitelná množina vzhledem k matroidům $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ nad E s řádovými funkcemi $r_1, r_2, \ldots, r_k$. Poté platí, že*

$$|J| = \min_{A \subseteq E} |E \setminus A| + \sum_{i=1}^{k} r_i(A).$$

I v tomto případě platí, že důkaz nerovnosti není „$\leq$“ těžký:

Pozorování 4. *Pro každou rozložitelnou množinu $J \subseteq E$ vzhledem k matroidům $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ nad E a každou množinu $A \subseteq E$ platí*

$$|J| \leq |E \setminus A| + \sum_{i=1}^{k} r_i(A)$$

.

Důkaz. Nejprve prvky J rozdělíme do dvou skupin dle toho, zda jsou v A, či nikoli, tj. $|J| = |J \setminus A| + |J \cap A|$. Dále víme, že množinu J lze vyjádřit jako sjednocení systému množin J_i po řadě nezávislých v $\mathcal{M}_i$. Z toho vyplývá, že $|J \cap A| \leq \sum_i |J_i \cap A| = \sum_i r_i(J_i \cap A) \leq \sum_i r_i(A)$. Protože $|J \setminus A| \leq |E \setminus A|$, dostáváme spojením všech nerovností dohromady $|J| \leq |E \setminus A| + \sum_{i=1}^{k} r_i(A)$. $\square$

Nyní se zaměříme na vzájemné převody problémů mezi sebou. Tvrdíme, že z platnosti Věty 1 (Matroid Intersection Problem) vyplývá platnost Věty 3 (Matroid Partition Problem). K tomu si nejprve uvědomíme, že následující množinový systém tvoří matroid.

Definice 2 (Rozkladový matroid)**.** *Mějme nosnou množinu E a její libovolný rozklad na disjunktní množiny $E_1, E_2, \ldots, E_k$. Řekneme, že $I \subseteq E$ je prvkem systému množin $\mathcal{I}$, jestliže $|I \cap E_i| \leq 1$ pro všechna $i \in \{1, 2, \ldots, k\}$. Je snadné nahlédnout, že $\mathcal{P} = (E, \mathcal{I})$ je matroid, a je-li matroid $\mathcal{M}$ izomorfní s nějakým takto vytvořeným matroidem $\mathcal{P}$, říkáme pak, že $\mathcal{M}$ je rozkladový matroid. Pro úplnost ještě dodejme, že rozkladové matroidy jsou speciální případ tzv. transverzálních matroidů.*

Teď už máme připraveno vše pro slibované tvrzení.

Tvrzení 5. *Platí-li věta Matroid Intersection, potom platí i věta Matroid Partition.*

Důkaz. V podstatě převyprávíme redukci popsanou v [2]. Mějme posloupnost matroidů $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ nad E. Nejprve místo množiny E uvažme množinu F vzniklou jako sjednocení k disjunktních kopií E. Tyto kopie označme E_i a matroidy $\mathcal{M}_i$ nyní uvažujme nad množinami E_i místo nad E. Sestrojme matroid $\mathcal{U}$ jako direktní součet matroidů $\mathcal{M}_i$ a matroid $\mathcal{P}$ jako rozkladový matroid množin $\{F_e; e \in E\}$, kde F_e označuje množinu všech kopií prvku $e \in E$ v F.

Je zřejmé, že každá nezávislá množina I pro matroidy $\mathcal{U}$ a $\mathcal{P}$ „kóduje“ rozložitelnou množinu v $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$. Představíme-li si každý prvek F jako dvojici (e, i), kde $e \in E$ a $i \in \{1, 2, \ldots, k\}$, pak nezávislost v $\mathcal{U}$ říka, že množina prvků I s druhou souřadnicí i je nezávislá v $\mathcal{M}_i$, tj. půjde opravdu o rozklad. Nezávislost v $\mathcal{P}$ naopak říká, že I obsahuje nejvýše jednu kopii každé $e \in E$, tj. zakódovaný rozklad bude disjunktní. Buď J největší nezávislá množina v matroidech $\mathcal{U}$ a $\mathcal{P}$. Z věty Matroid Intersection víme, že pak existuje rozklad množiny F na disjuknktní části $F_{\mathcal{U}}$ a $F_{\mathcal{P}}$ takové, že $|J| = r_{\mathcal{U}}(F_{\mathcal{U}}) + r_{\mathcal{P}}(F_{\mathcal{P}})$. O J ukážeme, že je i největší rozložitelnou množinou v $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ ve smyslu formule z Věty 3.

Teď přijde klíčová část důkazu – obsahuje-li část $F_{\mathcal{P}}$ alespoň jednu kopii nějakého prvku $e \in E$, můžeme bez újmy na obecnosti předpokládat, že obsahuje všech k kopií e. A důvod je prostý, obsahuje-li $F_{\mathcal{P}}$ alespoň jednu kopii e, přesuňme z $F_{\mathcal{U}}$ do $F_{\mathcal{P}}$ i všechny případné další kopie e, které v $F_{\mathcal{P}}$ nejsou. Takto upravený rozklad si označme $\widetilde{F}_{\mathcal{U}}, \widetilde{F}_{\mathcal{P}}$. Z definice $\mathcal{P}$ resp. z monotónie řádové funkce vidíme, že $r_{\mathcal{P}}\left(\widetilde{F}_{\mathcal{P}}\right) = r_{\mathcal{P}}(F_{\mathcal{P}})$ resp. $r_{\mathcal{U}}\left(\widetilde{F}_{\mathcal{U}}\right) \leq r_{\mathcal{U}}(F_{\mathcal{U}})$. Ale výraz $r_{\mathcal{U}}(F_{\mathcal{U}}) + r_{\mathcal{P}}(F_{\mathcal{P}})$ měl nejmenší hodnotu přes všechny rozklady F, proto $r_{\mathcal{U}}\left(\widetilde{F}_{\mathcal{U}}\right) \geq r_{\mathcal{U}}(F_{\mathcal{U}})$ a tím i $|J| = r_{\mathcal{U}}\left(F_{\mathcal{U}}\right) + r_{\mathcal{P}}\left(F_{\mathcal{P}}\right) = r_{\mathcal{U}}\left(\widetilde{F}_{\mathcal{U}}\right) + r_{\mathcal{P}}\left(\widetilde{F}_{\mathcal{P}}\right)$.

Položme $A = \left\{e \in E : \widetilde{F}_{\mathcal{U}} \text{ obsahuje kopii } e\right\}$. Z definice matroidu $\mathcal{U}$ plyne rovnost $\sum_{i=1}^{k} r_i(A) = r_{\mathcal{U}}\left(\widetilde{F}_{\mathcal{U}}\right)$. Naopak z definice matroidu $\mathcal{P}$ víme, že $|E \setminus A| = r_{\mathcal{P}}\left(\widetilde{F}_{\mathcal{P}}\right)$. Již víme, že J je rozložitelná, a ve spojení s Pozorováním 4 musí být i největší rozložitelná množina vzhledem k $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$, čímž je důkaz hotov. □

Ukážeme teď i opačnou redukci, jinými slovy z platnosti Věty 3 vyplývá platnost Věty 1, díky čemuž jsou problémy Matroid Intersection a Matroid Partition ekvivalentní. I teď budeme na začatku potřebovat připomenout si nějaké základní pojmy o matroidech, tak směle do toho.

Mějme matroid $\mathcal{M}$ nad E a označme jeho systém bazí $\mathcal{B} = \{B : B \text{ báze } \mathcal{M}\}$. Pro úplnost poznamenejme, že báze B je do inkluze maximální nezávislá množina $\mathcal{M}$. Je snadné si rozmyslet, že všechny báze mají stejnou velikost, jež je rovna $r(E)$. Tato hondota se běžně označuje jako řád matroidu a značí se $r(\mathcal{M})$.

Nad matroidy můžeme také vybudovat dualitu, která je v podstatě zobecněním duality v rovinných grafech. Stejně jako samotné matroidy můžeme zavést více způsoby, i dualitu lze definovat různě. My se budeme držet definice z [1] či [3].

Definice 3. *Mějme matroid $\mathcal{M}$ nad E se systémem bazí $\mathcal{B}$ a definujme systém $\mathcal{B}^* = \{E \setminus B : B \in \mathcal{B}\}$. Potom platí, že $\mathcal{B}^*$ je opět systém bazí nějakého matroidu, tento matroid se nazývá duálním matroidem k $\mathcal{M}$ a označuje se $\mathcal{M}^*$.*

O dualních matroidech lze dokázat řada zajímavých vlastností, např. duální matroid k duálnímu matroidu $\mathcal{M}$ je opět $\mathcal{M}$, neboli $(\mathcal{M}^*)^* = \mathcal{M}$. My si však z duality, vyjma konceptu samotného, vypůjčíme jen následující vlastnost řádové funkce duálu r^*, která se běžně označuje jako co-řádová funkce.

Fakt 6. *Pro co-řádovou funkci r^* k matroidu $\mathcal{M}$ nad E platí následující formule:*

$$r^*(X) = |X| - r(\mathcal{M}) + r(E \setminus X).$$

S pomocí tohoto faktu již dokážeme redukci snadno.

Tvrzení 7. *Platí-li věta Matroid Partition, potom platí i věta Matroid Intersection.*

Důkaz. Důkaz je opět volně inspirován [2], kde je uveden jako cvičení s návodem. Hlavním trikem je použit dualitu. Mějme $\mathcal{M}_1$ a $\mathcal{M}_2$ matroidy nad E a hledejme jejich společnou největší nezávislou množinu. Označme J největší rozložitelnou množinu v $\mathcal{M}_1$ a $\mathcal{M}_2^*$ s rozkladem na části J_1 a J_2^*.

Podle věty Matroid Partition existuje $A \subseteq E$, pro kterou platí, že velikost J je rovna $|E \setminus A| + r_1(A) + r_2^*(A)$. Rozšiřme teď J_2^* na bázi B_2^* matroidu $\mathcal{M}_2^*$ a uvažme množinu $E' = J \setminus B_2^*$. Jednak platí, že $E' \subseteq J_1$, a proto E' je nezávislá v $\mathcal{M}_1$, na druhou stranu ale $E' \subseteq (E \setminus B_2^*)$, tudíž je E' nezávislá i v M_2.

Zbývá nám ukázat, že E' je největší nezávislou množinou v $\mathcal{M}_1$ a $\mathcal{M}_2$, k čemuž stačí najít vhodný rozklad E. Malé překvapení je, že tento rozklad už máme, což si uvědomíme použitím Faktu 6 o co-řádové funkci na $E \setminus A$ v $\mathcal{M}_2^*$. Počítejme tedy: $r_1(A) + r_2(E \setminus A) = r_1(A) + |E \setminus A| + r_2^*(A) - |B_2^*| = |J| - |B_2^*|$. Tím jsme však hotovi, neboť $|E'| = |J \setminus B_2^*| \geq |J| - |B_2^*| = r_1(A) + r_2(E \setminus A)$, což dohromady s Pozorováním 2 říká, že E' je opravdu největší nezávislá množina pro $\mathcal{M}_1$ a $\mathcal{M}_2$ ve smyslu formule z Věty 1. ☐

Na samotný závěr dokážeme nerovnost „$\geq$“ z Věty 1, kterou jsme na začátku odložili. Tím završíme důkaz Věty 1 a zároveň, jak už nyní víme, i Věty 3. Důkaz pochází z [3], podobný argument však můžeme najít i v [2]. Důkaz je algoritmický a jeho popis nám přímo dává polynomiální algoritmus pro řešení problému Matroid Intersection.

Abychom nemuseli některé množinové operace psát dlouhými formulemi, zavedeme si následující vcelku intuitivní značení.

Definice 4. *Pro množinu M a prvek p budeme výrazem $M + p$ označovat $M \cup \{p\}$. Analogicky pak $M - p$ definujeme jako $M \setminus \{p\}$.*

Věta 8. *Mějme matroidy $\mathcal{M}_1 = (E, \mathcal{I}_1)$ s řádovou funkcí r_1 a $\mathcal{M}_2 = (E, \mathcal{I}_2)$ s řádovou funkcí r_2 nad množinou E. Potom v polynomiálním čase pro každou jejich společnou nezávislou množinu E' můžeme buď najít „vhodný“ rozklad, který dokazuje její největší velikost, nebo ostře větší množinu E'', jež je opět nezávislou množinou v $\mathcal{M}_1$ a $\mathcal{M}_2$.*

Důkaz. Na základě E' si nejprve zkonstruujme pomocný orientovaný bipartitní graf H s partitami E' a $X = E \setminus E'$. Z prvku $e \in E'$ vede (orientovaná) hrana do $x \in X$ právě když množina $(E' - e) + x$ je nezávislá v $\mathcal{M}_1$. Naopak z $x \in X$ vede hrana do $e \in E'$ právě když množina $(E' - e) + x$ je nezávislá v $\mathcal{M}_2$. Uvažme ještě množiny $X_1 = \{x \in X : (E' + x) \in \mathcal{I}_1\}$ resp. $X_2 = \{x \in X : (E' + x) \in \mathcal{I}_2\}$ a podívejme se, zda v H existuje orientovaná cesta z X_1 do X_2.

Nejprve rozebereme jednodušší případ, kdy žádná taková cesta neexistuje. Tvrdíme, že v tomto případě najdeme „vhodné“ rozdělení E. Buďte $E_1 \supseteq X_2$ a $E_2 \supseteq X_1$ rozdělení takové, že v H nevede žádná orientovaná cesta z E_2 do E_1. Není těžké si uvědomit, že za našich předpokladů je toto vždy možné.

Ukážeme, že $|E' \cap E_1| = r_1(E' \cap E_1) = r_1(E_1)$. Nechť pro spor $r_1(E' \cap E_1) < r_1(E_1)$. Nejprve si všimněme, že potom nemůže platit $E' \subseteq E_1$. Každý prvek $x \in E_1$, který rozšiřuje E', je z definice prvkem X_1. Avšak X_1 a E_1 jsou dle svých definic disjunktní, takže je-li $E' \subseteq E_1$, tak E' tvoří bázi v $\mathcal{M}_1$ zúženém na E_1, a nutně tedy $r_1(E_1) = r_1(E') = r_1(E' \cap E_1)$. Můžeme tedy předpokládat, že $r_1(E' \cap E_1) = |E' \cap E_1| < |E'|$ a že existuje $e \in (E' \setminus E_1)$. Rozšiřme nejprve $E' \cap E_1$ o prvek $z \in (E_1 \setminus E')$ na nezávislou množinu $Z = (E' \cap E_1) + z$. Poté postupně rozšiřujme Z o prvky E', dokud můžeme použít rozšiřující axiom na tyto množiny v $\mathcal{M}_1$. Skončíme tedy s nezávislou množinou $Z' \supseteq Z$, jejíž velikost je přesně $|E'|$. Není těžké si rozmyslet, že potom Z' musí být rovna množině $(E' - e) + z$ pro nějaký prvek $e \in (E' \setminus E_1) = (E' \cap E_2)$. Ovšem Z' je nezávislá v $\mathcal{M}_1$, proto v H vede hrana z e do z. Jenže $e \in E_2$ a $z \in E_1$, což je spor s tím, že nevede žádná cesta z E_2 do E_1.

Obdobně nahlédneme, že $|E' \cap E_2| = r_2(E' \cap E_2) = r_2(E_2)$. Analogickou argumentací bychom jinak našli množinu $(E' - f) + y$ pro nějaká $y \in E_2$ a $f \in E_1$. To by v tomto případě říkálo, že v H vede hrana z y do f, čímž opět dostáváme spor s neexistencí cesty z E_2 do E_1. Pokud tedy v H neexistuje cesta z X_1 do X_2, pak je $|E'| = |E' \cap E_1| + |E' \cap E_2| = r_1(E_1) + r_2(E_2)$, a $E_1 \cup E_2 = E$ je dobrým rozkladem vzhledem k E'.

Nechť tedy nastane druhá možnost a v H existuje cesta z X_1 do X_2, vezměme si **nejkratší** takovou cestu P. Neformálně řečeno, budeme chtít E' zvětšit „podél“ cesty P analogicky k zvětšení podél volné střídavé cestě při hledání max. párování. Buď $P = x_0 e_1 x_1 e_2 \dots e_l x_l$, kde $x_0 \in X_1$ a $x_l \in X_2$. Všimněme si na okraj, že pokud by $l = 0$, je $x_0 \in X_1 \cap X_2$ a tím je přímo z definice množina $E'' = (E' + x_0)$ nezávislá v $\mathcal{M}_1$ i v $\mathcal{M}_2$. Tvrdíme, že množina

$$E'' = (E' \setminus \{e_1, \dots, e_l\}) \cup \{x_0, x_1, \dots, x_l\}$$

je nezávislá v $\mathcal{M}_1$ a $\mathcal{M}_2$. Protože bude následující argumentace opět symetrická (buď bychom hrany v následujícím procházeli v opačném pořadí, nebo bychom prohodili role $\mathcal{M}_1$ a $\mathcal{M}_2$ při konstrukci H), dokážeme pouze, že E'' je nezávislá v $\mathcal{M}_1$. Nejprve vyslovíme následující mírně technické lemma.

Lemma 9. *Množiny $E'_k = (E' \setminus \{e_k, \dots, e_l\}) \cup \{x_k, \dots, x_l\}$ jsou nezávislé množiny matroidu $\mathcal{M}_1$ pro $k \in \{1, 2, \dots, l\}$.*

Důkaz. Indukcí dle k, (netradičně) jdoucí dolů od l k 1. Pro $k = l$ je tvrzení samozřejmé, neboť z e_l do x_l vede hrana právě proto, že E'_l je nezávislá v $\mathcal{M}_1$.

Předpokládejme nyní, že množiny $E'_{k+1}, \dots, E'_l$ jsou nezávislé. Potom $(E'_k - x_k) \subseteq E'_{k+1}$, čímžto $E'_k - x_k$ je nezávislá množina velikosti $|E'| - 1$. Protože v H vede hrana z e_k do x_k, je i $(E' - e_k) + x_k$ nezávislá množina, tentokrát velikosti $|E'|$. Použijme tedy na tuto dvojici množin rozšiřující axiom v $\mathcal{M}_1$, díky čemuž získáváme nezávislou množinu $(E'_k - x_k) + z$ pro nějaké $z \in \{x_k, e_{k+1}, \dots, e_l\}$. Kdyby $z = x_k$, jsme hotovi. Pro spor tedy předpokládejme, že $z = e_{>k}$. Rozšiřme množinu $E' - e_k$ o prvek y z množiny $(E'_k - x_k) + e_{>k}$. Je zřejmé, že musí $y \in \{x_{k+1}, \dots, x_l\}$, a proto $(E' - e_k) + x_{>k}$ je nezávislou množinou v $\mathcal{M}_1$. To však znamená, že v H vede hrana z e_k do $x_{>k}$, což je spor s tím, že P byla nejkratší cesta. □

Dokončit celý důkaz je nyní už jen cvičení na řádovou funkci. Z předcházejícího lemmatu víme, že $E'_1 = (E' \setminus \{e_1, \dots, e_l\}) \cup \{x_1, \dots, x_l\}$ je nezávislá množina velikosti $|E'|$. Dále víme, že $E' + x_0$ je nezávislá množina velikosti $|E'| + 1$, protože $x_0 \in X_1$. Naopak si všimněme, že množina $E' + x_{\geq 1}$ v $\mathcal{M}_1$ nemůže být nezávislá, protože pak by P nebyla nejkratší. Proto $r_1(E' + x_{\geq 1}) = |E'|$ a díky tomu i $r_1(E' \cup \{x_1, \dots, x_l\}) = |E'|$ (kdyby měla obsahovat nezávislou množinu velikosti větší než $|E'|$, tak o nějaký její prvek rozšíříme E', čímž bychom získali nezávislou množinu tvaru $E' + x_{\geq 1}$). Množinu $E' \cup \{x_1, \dots, x_l\}$ si označme D. Když nyní rozšíříme E'_1 o prvek x množiny $E' + x_0$, kde $x \in \{x_0, e_1, \dots, e_l\}$, víme, že $x \neq e_i$. Kdyby $x = e_i$, měli bychom nezávislou množinu velikosti $|E'| + 1$, která je podmnožinou D, ačkoli $r_1(D)$ je pouze $|E'|$. To však nejde, proto $x = x_0$, E'' je nezávislá v $\mathcal{M}_1$, a celá věta tímto dokázána. □

Reference

[1] J. G. Oxley: Matroid Theory, Oxford Graduate Texts in Mathematics 3, Oxford University Press, 1992.

[2] W. J. Cook, W. H. Cunningham, W. R. Pulleyblank, A. Schrijver: Combinatorial Optimization, John Wiley and Sons, New York, 1998

[3] D. Král', O. Pangrác: Introduction to Matroid Theory (lecture notes), ITI Series 2009-430, Matematicko-Fyzikální Fakulta UK Praha, 2009.