Diskrétní matematika

Roman Čada
Tomáš Kaiser
Zdeněk Ryjáček

Katedra matematiky FAV
Západočeská univerzita v Plzni
2004

Úvodem

Máte před sebou text k přednášce Diskrétní matematika pro první ročník na Západočeské univerzitě v Plzni. Cílem přednášky, a tím i této publikace, je nejen předat základní znalosti o diskrétní matematice, ale také přispět k tomu, aby se posluchači a čtenáři zdokonalili ve schopnosti přesného myšlení a formulování, a získali cit pro vnitřní krásu matematického argumentu.

Diskrétní matematika je moderní a dynamickou disciplínou, která úzce souvisí jak s ostatními matematickými obory (např. s lineární algebrou nebo analýzou), tak s teoretickou informatikou. Za řadu impulsů vděčí prudkému rozvoji počítačů a komunikace ve druhé polovině minulého století.

Skripta vznikla volně na základě staršího textu [1]. Předpokladem při jejich četbě je znalost lineární algebry v rozsahu úvodního kursu. Lze je zhruba rozdělit na dvě části: první čtyři kapitoly jsou věnovány matematickým strukturám, u ostatních osmi jsou tématem základy teorie grafů.

Doporučujeme vypracovat co nejvíce cvičení — stejně jako v jiných oborech i v diskrétní matematice čtenář nejvíce získá, když látku samostatně promýšlí. Cvičení jsou označena symbolem ▶, u obtížnějších problémů jsou tyto symboly dva. Výsledky vybraných cvičení jsou uvedeny na konci skript. Jedná se především o ta cvičení, ve kterých je cílem zodpovědět nějakou otázku (a nikoli dokázat nějakou větu).

Jsou na světě matematické knihy, jejichž četba je zábavou a občas i "dobrodružstvím poznání". Snažili jsme se, aby k nim patřila i tato skripta; zda se to podařilo, posoudí nejlépe čtenář.

Své podněty, postřehy a upozornění na chyby posílejte prosím na adresu `kaisert@kma.zcu.cz`. Opravy a doplňky budou k dispozici na internetové stránce `http://home.zcu.cz/~kaisert/dma/errata`.

Děkujeme autorům softwaru použitého při přípravě této publikace. Jedná se především o tyto programy a soubory maker: TEX, LATEX, MetaPost, dvipdfm, subfigure, hyperref, emp a dvichop. V textu jsou použita cvičení z knih [3], [4], [5] a [6]. Dále děkujeme kolegovi J. Brouskovi za cenné připomínky k pracovním verzím tohoto textu.

Plzeň, únor 2004 Autoři

Obsah

Kapitola 1

Relace

Úvodní kapitola je věnována důležitému a velmi obecnému pojmu relace, který zastřešuje řadu na pohled různorodých pojmů jako zobrazení, ekvivalence nebo uspořádání. Protože relace popisují vztahy mezi prvky množin a navíc jsou samy množinami, bude vhodné množiny nejprve krátce připomenout.

1.1 Stručně o množinách

Množiny patří k základním matematickým objektům. V jistém smyslu je celá matematika, jak ji dnes známe, vystavěna na pojmu množiny. Všechny ostatní matematické objekty, ať jde o přirozená čísla nebo spojité funkce, lze totiž modelovat pomocí množin.

Komplikované vlastnosti množinového světa jsou předmětem samostatného oboru, tzv. *teorie množin*. Nás ale v této přednášce nebudou jemnosti této teorie příliš zajímat a postačí nám následující intuitivní pohled na věc.

Množina je pro nás soubor navzájem různých objektů[1], které označujeme jako její *prvky*. Je-li a prvkem množiny X, píšeme $a \in X$, jinak $a \notin X$. Množina je buď *konečná* (má-li konečný počet prvků) nebo *nekonečná*. Počet prvků konečné množiny X označujeme symbolem $|X|$. Sestává-li množina X z prvků $x_1, \ldots, x_k$, píšeme $X = \{x_1, \ldots, x_k\}$. Podobně například zápis $X = \{m \in \mathbf{N} : m \text{ je sudé číslo}\}$ znamená, že množina X je složena ze všech sudých přirozených čísel (symbol $\mathbf{N}$ bude i nadále označovat množinu všech přirozených čísel).

Podmnožina množiny X je množina Y, jejíž každý prvek je také prvkem množiny X. Je-li Y podmnožinou množiny X, píšeme $Y \subset X$ (případně $Y \subseteq X$, chceme-li zdůraznit, že množiny X, Y mohou být shodné). Pro pocvičení ve formálním zápisu můžeme definici vyjádřit takto:

$$Y \subset X \quad \text{právě když} \quad \forall y : y \in Y \Rightarrow y \in X.$$

[1] Neříkáme už ale, co to je objekt. V tom právě spočívá intuitivnost našeho přístupu.

Množina $Y \subset X$ je *vlastní* podmnožinou množiny X (psáno $Y \subsetneq X$), pokud platí $Y \neq X$. Všimněme si, že *prázdná množina* $\emptyset$ (tj. množina, která nemá žádné prvky) je podle definice podmnožinou každé množiny.

Mezi pojmy prvek a podmnožina je zásadní a někdy přehlížený rozdíl. Je-li $X = \{1, 2, 3\}$, pak platí $1 \in X$, ale zápis $1 \subset X$ nemá smysl, protože přirozené číslo 1 (alespoň zatím) nepovažujeme za množinu. Podobně platí $\{1\} \subset X$, ale neplatí $\{1\} \in X$. Další podmnožiny množiny X jsou například $\emptyset$, $\{2, 3\}$ nebo X.

Jiný příklad: platí $\emptyset \subset \emptyset$, ale $\emptyset \notin \emptyset$, protože množina $\emptyset$ žádné prvky neobsahuje.

S množinami lze provádět následující základní operace. *Průnik* $X \cap Y$ sestává ze všech společných prvků množin X a Y, *sjednocení* $X \cup Y$ ze všech prvků alespoň jedné z množin X a Y, *rozdíl* $X - Y$ (psáno také $X \setminus Y$) je složen ze všech prvků množiny X, které nejsou obsaženy v množině Y. *Kartézský součin* $X \times Y$ množin X a Y je množina všech uspořádaných dvojic (x, y), kde $x \in X$ a $y \in Y$.

Cvičení

▶ **1.1** Napište formální definici sjednocení, průniku a rozdílu množin.

▶ **1.2** Dvě množiny A, B jsou si *rovny*[2], pokud mají přesně tytéž prvky, tedy pokud platí $A \subset B$ a $B \subset A$. Dokažte přímo z definic, že pro množiny A, B, X platí de Morganovy[3] zákony:

$$X - (A \cup B) = (X - A) \cap (X - B),$$
$$X - (A \cap B) = (X - A) \cup (X - B).$$

▶ **1.3** Nechť A je n-prvková množina. Kolik má podmnožin? Kolik z těchto podmnožin má sudý počet prvků?

▶ **1.4** Počet k-prvkových podmnožin n-prvkové množiny označujeme symbolem $\binom{n}{k}$ (čteno 'n nad k'). Číslům $\binom{n}{k}$ se říká *kombinační čísla*.

(a) Vyjádřete $\binom{n}{k}$ jako výraz v proměnných n, k. Určete kombinační čísla $\binom{6}{3}$, $\binom{10}{6}$, $\binom{10}{0}$ a $\binom{0}{0}$.

(b) Dokažte, že platí

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

[2]Tento 'očividný fakt' je vlastně definicí rovnosti množin. V teorii množin jde o jeden ze základních axiomů.

[3]Augustus de Morgan (1806–1871).

(c) Dokažte

$$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}.$$

▶ **1.5** Spočítejte:

(a)

$$\sum_{k=0}^{n} \binom{n}{k},$$

(b)

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

▶ **1.6** *Symetrický rozdíl* množin A, B definujeme předpisem

$$A \triangle B = (A - B) \cup (B - A).$$

Dokažte podrobně:

(a) $A \triangle (A \cap B) = A - (A \cap B)$,

(b) $A \triangle (A \cup B) = (A \cup B) - A$.

▶ **1.7** Dokažte:

$$X \subset A \cup B \iff (X - A) \subset B \iff (X - A) \cap (X - B) = \emptyset.$$

▶ **1.8** Platí pro libovolnou čtveřici množin rovnost $A \times B = C \times D$ právě tehdy, když $A = C$ a $B = D$? Jak se situace změní, nahradíme-li všechny symboly rovnosti '=' symbolem '$\subset$'?

1.2 Relace

Mějme dvě množiny X,Y a představme si, že každý prvek $x \in X$ může (a nemusí) být ve 'vztahu' R s libovolným počtem prvků $y \in Y$. Na tento vztah nejsou kladeny žádné další podmínky.

Přirozeným způsobem, jak takový vztah popsat, je vyjmenovat všechny dvojice (x, y) prvků $x \in X$ a $y \in Y$, které spolu jsou ve vztahu R. Připomeneme-li si, že kartézský součin $X \times Y$ je v oddílu 1.1 definován jako množina všech uspořádaných dvojic s prvním prvkem z množiny X a druhým prvkem z množiny Y, dostáváme se k následující definici pojmu relace:

Definice 1.1 *Relace z množiny X do množiny Y* je libovolná podmnožina R kartézského součinu $X \times Y$.

Takové relaci se říká *binární*, protože určuje vztah mezi dvojicemi objektů. Definici lze snadno zobecnit na *n-ární relace* (vztahy mezi n-ticemi prvků), ale nás zajímá především binární případ.

Je-li dána relace R z množiny X do množiny Y, pak pro každou dvojici $(x, y) \in R$ také píšeme $x\,R\,y$ (a čteme 'prvek x je v relaci R s prvkem y'). Daný prvek $x \in X$ ovšem nemusí být v relaci R s žádným prvkem množiny Y (v extrémním případě může být relace R třeba prázdná). Proto definujeme *levý obor* relace R jako

$$L(R) = \{x \in X : \text{existuje nějaké } y \in Y \text{ tak, že } x\,R\,y\}$$

a podobně *pravý obor*

$$P(R) = \{y \in Y : \text{existuje nějaké } x \in X \text{ tak, že } x\,R\,y\}$$

Příklad 1.2 Vezměme si například množiny $X = \{2, 3, 5\}$ a $Y = \{1, 4, 7, 10\}$. Jedna z relací z množiny X do množiny Y pak vypadá třeba takto:

$$R = \{(2, 4), (2, 10), (5, 10)\}.$$

Relace R má shodou okolností dosti přirozený popis; platí totiž, že x je v relaci s y, právě když x dělí y. To ale vůbec není podmínkou: stejně tak je relací z X do Y třeba množina $\{(2, 4), (3, 7), (5, 1)\}$, u které žádný takový popis asi nenajdeme.

Cvičení

► **1.9** Mějme množiny přirozených čísel $A = \{1, 2, 3, 4\}$ a $B = \{3, 4, 5, 6\}$. Určete levý a pravý obor relace

$$R = \{(a, b) : a \geq b, a \in A, b \in B\}$$

z množiny A do množiny B.

► **1.10** Nechť $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$ jsou dvě množiny. Uvažme následující relace z A do B:

$$R = \{(1, a), (1, c), (2, b), (3, a), (3, b), (4, b), (4, c), (4, d)\}$$
$$T = \{(1, b), (1, c), (3, a), (4, a)\}.$$

Určete množiny $R \cup T$, $R \cap T$, $R - T$ a symetrický rozdíl $R \triangle T$. Jedná se ve všech případech o relace?

► **1.11** Mějme m-prvkovou množinu X a n-prvkovou množinu Y. Kolik je všech binárních relací z X do Y? (Hádáte-li $m \cdot n$, přečtěte si ještě jednou definici.)

► **1.12** Nechť R a S jsou relace z množiny X do množiny Y. Řekneme, že relace R *implikuje* relaci S, platí-li

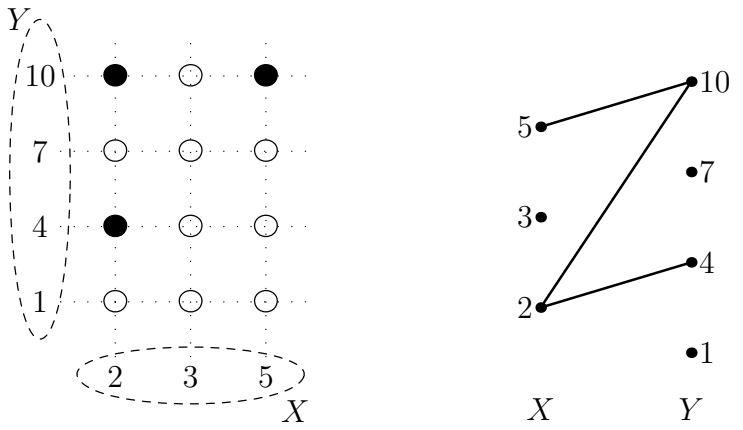
$$x\,R\,y \Rightarrow x\,S\,y$$

pro každé $x \in X$ a $y \in Y$. Co to znamená o relacích R a S jakožto o množinách uspořádaných dvojic?

1.3 Znázornění relací

Relaci R z minulého příkladu můžeme znázornit několika užitečnými způsoby. Na obr. 1.1a je znázorněn kartézský součin $X \times Y$, v němž jsou plnými kroužky zvýrazněny prvky relace R. Na obr. 1.1b pak jednotlivým prvkům množin X a Y odpovídají body, přičemž množina X je zobrazena vlevo a množina Y vpravo. Dva body jsou spojeny čarou, pokud jsou odpovídající prvky v relaci R. Relace R je tak znázorněna v podobě *grafu*, což je pojem, kterým se budeme zabývat v pozdějších přednáškách.

Těmto dvěma typům znázornění relace R budeme říkat *kartézské* a *grafové* znázornění.



Obrázek 1.1: Dva způsoby zobrazení relace: (a) jako podmnožina kartézského součinu, (b) jako graf.

Cvičení

► **1.13** Jak z obr. 1.1a a 1.1b poznáme levý a pravý obor relace R?

► **1.14** Znázorněte oběma způsoby relaci R ze cvičení 1.9.

1.4 Skládání relací

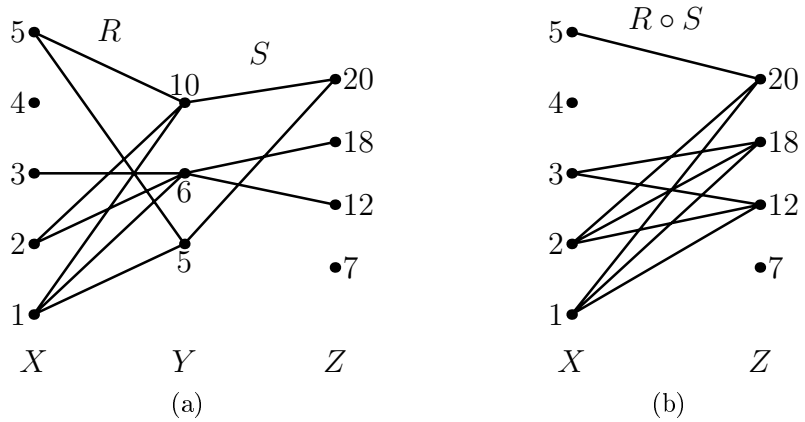
Za chvíli uvidíme, že zobrazení (funkce), jak je známe z analýzy, jsou speciálním případem relací. Následující definice skládání relací je zobecněním představy skládání funkcí.

Definice 1.3 Nechť R je relace z množiny X do množiny Y a S je relace z množiny Y do množiny Z. Pak *složení relací* R *a* S je relace $R \circ S \subset X \times Z$ z množiny X do množiny Z, definovaná takto:

$$(x, z) \in R \circ S, \text{ právě když existuje } y \in Y \text{ tak, že } x\, R\, y \text{ a } y\, S\, z,$$

kde $x \in X$ a $z \in Z$. Všimněme si, že složení relací R,S je definováno jen v případě, že relace R 'končí' v množině, kde S 'začíná'.

Podívejme se na konkrétní příklad. Nechť $X = \{1, 2, 3, 4, 5\}$, $Y = \{5, 6, 10\}$ a $Z = \{7, 12, 18, 20\}$, a definujme relace $R \subset X \times Y$ a $S \subset Y \times Z$ opět pomocí dělitelnosti (tedy například pro $x \in X$ a $y \in Y$ bude $(x, y) \in R$, pokud x dělí y). V grafovém znázornění relací R a S dostaneme situaci na obr. 1.2a.



Obrázek 1.2: (a) Relace R a S, (b) jejich složení.

Z definice skládání plyne, že prvky $x \in X$ a $z \in Z$ budou v relaci $R \circ S$, pokud se z x do z dá přejít 'po spojnicích' přes nějaký prvek $y \in Y$. Ověřte, že $R \circ S$ vypadá jako na obr. 1.2b.

V tomto znázornění relace je průhledný i další pojem: inverzní relace.

Definice 1.4 *Relace inverzní* k relaci $R \subset X \times Y$ je relace $R^{-1} \subset Y \times X$, definovaná vztahem

$$y\, R^{-1}\, x \text{ právě když } x\, R\, y$$

pro $x \in X, y \in Y$.

V grafovém znázornění se přechod k inverzní relaci projeví zrcadlovým otočením obrázku podle svislé osy. Jak tomu bude v kartézském znázornění? (Cvičení 1.18.)

Vezměme například relaci S z obr. 1.2a. Relace inverzní k S bude

$$S^{-1} = \{(20, 5), (12, 6), (18, 6), (20, 10)\}$$

a jedná se o relaci z množiny Z do množiny Y.

Nechť je dána množina X. Místo o 'relaci z X do X' mluvíme prostě o *relaci na množině* X. Všimněme si, že pro každé dvě relace na X je definováno jejich složení. Význačným příkladem relace na množině X je *identická relace*

$$E_X = \{(x, x) : x \in X\}.$$

Co se stane, složíme-li relaci $R \subset X \times Y$ s relací k ní inverzní? Zjevně $R \circ R^{-1}$ je relace na množině X a lákavá hypotéza je, že je rovna identické relaci E_X. To ale není pravda, jak ukazuje třeba prázdná relace $R = \emptyset$, pro kterou je $R \circ R^{-1}$ rovněž prázdná. Obecně neplatí ani jedna z inkluzí mezi E_X a $R \circ R^{-1}$. (Viz cvičení 1.19.) Podobně je tomu u opačného pořadí skládání, totiž pro relace $R^{-1} \circ R$ a E_Y.

Záleží u skládání operací na pořadí? Obecně samozřejmě ano — pokud R je relace z X do Y, a S je relace z Y do Z, pak $R \circ S$ je dobře definovaná relace, zatímco $S \circ R$ definována není. Jsou-li ovšem R,S relace na množině X, pak tento problém nemůže nastat. Ani tam ale nemusí být $R \circ S = S \circ R$. Příkladem je tato situace: množina X je dvouprvková, $X = \{a, b\}$. Relace $R \subset X \times X$ sestává z jediné dvojice (a, a), zatímco $S = \{(a, b)\}$. Pak platí

$$R \circ S = \{(a, b)\} \quad \text{a} \quad S \circ R = \emptyset.$$

(Této otázky se týká také cvičení 1.17.)

Třebaže u skládání relací záleží na jejich pořadí (není to tedy *komutativní* operace), jednou pěknou vlastností nás skládání překvapí. Je totiž *asociativní*, což znamená, že nezáleží na způsobu, jakým relace uzávorkujeme. Přesněji to vyjadřuje následující věta. Její důkaz může být při prvním čtení poněkud obtížný, vyplatí se ale jej důkladně prostudovat.

Věta 1.5 (O asociativitě skládání relací) *Nechť $R \subset X \times Y$, $S \subset Y \times Z$ a $T \subset Z \times W$ jsou relace. Potom*

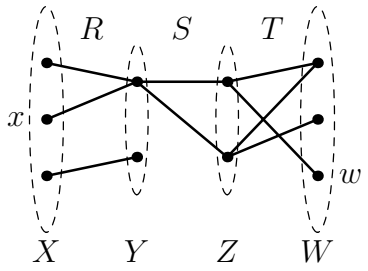
$$R \circ (S \circ T) = (R \circ S) \circ T.$$

Důkaz. K lepšímu pochopení důkazu může pomoci, budeme-li si relace R, S, T představovat v grafovém znázornění jako na obr. 1.3.

Dejme tomu, že $x \in X$ a $w \in W$ jsou spolu v relaci $R \circ (S \circ T)$. Podle definice složení relací R a $S \circ T$ to znamená, že existuje $y \in Y$ tak, že $x\,R\,y$ a $y\,(S \circ T)\,w$. Opět z definice složení relací S a T existuje $z \in Z$ tak, že $y\,S\,z$ a $z\,T\,w$.

Jinak řečeno, pokud $x\,(R \circ (S \circ T))\,w$, pak existují $y \in Y$ a $z \in Z$ tak, že $x\,R\,y\,S\,z\,T\,w$ (tj. v našem obrázku lze z x do w přejít 'po spojnicích' zleva doprava). A tato implikace platí i obráceně, což plyne přímo z definice skládání.

Stejně se dokáže, že $x\,((R \circ S) \circ T)\,w$, právě když existují $y \in Y$ a $z \in Z$ tak, že $x\,R\,y\,S\,z\,T\,w$. To ovšem znamená, že platí $x\,(R \circ (S \circ T))\,w$, právě když platí $x\,((R \circ S) \circ T)\,w$, protože obě tato tvrzení jsou ekvivalentní téže podmínce. Z toho už vyplývá dokazovaná věta. □



Obrázek 1.3: Ilustrace k důkazu věty 1.5.

Cvičení

▶ **1.15** Jak vypadá relace E_X ve znázorněních z obr. 1.1?

▶ **1.16** Je-li R relace na X, jak vypadá složení $R \circ E_X$ a $E_X \circ R$?

▶ **1.17** Najděte příklad relace R na nějaké množině X, pro kterou platí

(a) $R \circ R^{-1} \neq R^{-1} \circ R$,

(b) $R \circ R^{-1} = R^{-1} \circ R$.

▶ **1.18** Jak se liší kartézské znázornění relace R a inverzní relace R^{-1}?

▶ **1.19** Najděte množinu X a relaci R na X s vlastností:

(a) $R \circ R^{-1} \subsetneqq E_X$,

(b) $E_X \subsetneqq R \circ R^{-1}$,

▶ **1.20** Mějme dvě relace R a S na množině X s vlastností $L(R) = P(S)$ a $L(S) = P(R)$. Jsou pak R a S *záměnné*, tj. platí pak $R \circ S = S \circ R$?

▶ **1.21** Nechť R, S, T jsou binární relace na množině X. Dokažte podrobně:

(a) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$,

(b) $(R \cup S) \circ T = (R \circ T) \cup (S \circ T)$.

Zůstane vztah (b) v platnosti, nahradíme-li v něm všechny symboly sjednocení za průnik?

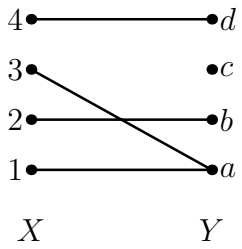
1.5 Zobrazení

Zobrazení je speciálním případem relace.

Definice 1.6 *Zobrazení* (nebo také *funkce*) množiny X do množiny Y je relace $f \subset X \times Y$, pro kterou platí, že pro každý prvek $x \in X$ existuje *právě jeden* prvek $y \in Y$ tak, že $(x, y) \in f$. Skutečnost, že f je zobrazením X do Y, zapisujeme jako $f : X \to Y$.

Pro $x \in X$ nazýváme ono jediné y *hodnotou* zobrazení f v bodě x a píšeme $f(x) = y$. Říkáme také, že prvek x je *vzorem* prvku y při zobrazení f. Nepřehlédněme, že libovolný prvek může mít více vzorů.

Například relace f z množiny $X = \{1, 2, 3, 4\}$ do množiny $Y = \{a, b, c, d\}$ na obr. 1.4 je zobrazením. Platí třeba $f(3) = a$ atd.



Obrázek 1.4: Zobrazení $f : X \to Y$.

Zobrazení mohou mít několik důležitých vlastností.

Definice 1.7 Zobrazení $f : X \to Y$ je

- *prosté*, pokud každé $y \in Y$ má nejvýše jeden vzor při zobrazení f,
- *na*, pokud každé $y \in Y$ má alespoň jeden vzor při zobrazení f,
- *vzájemně jednoznačné* (jinak též *bijekce*), pokud je prosté a na.

Zobrazení f z obr. 1.4 není ani prosté, ani na, neboť prvek c nemá vzor, zatímco a má hned dva.

Co se stane, utvoříme-li inverzní relaci k nějakému zobrazení $f : X \to Y$? Tato inverzní relace f^{-1} je vždy definována (je dokonce definována pro libovolnou relaci), ale nemusí to být zobrazení (viz cvičení 1.22). Příkladem je třeba právě zobrazení f z obr. 1.4.

Složíme-li dvě zobrazení $f : X \to Y$ a $g : Y \to Z$, výsledná relace $f \circ g$ je zobrazení X do Z, pro jehož hodnoty platí

$$(f \circ g)(x) = g(f(x)).$$

(Často je možné se setkat i se zápisem v obráceném pořadí, ve kterém se stejné zobrazení označuje jako $g \circ f$. V tomto textu se držíme výše uvedeného značení.)

Cvičení

▶ **1.22** Ukažte, že inverzní relace f^{-1} k zobrazení $f : X \to Y$ je sama zobrazením, právě když f je bijekce.

▶ **1.23** Nechť $f\colon X \to Y$ a $g\colon Y \to Z$ jsou dvě zobrazení. Dokažte, že $f \circ g$ je zobrazení.

▶ **1.24** Nechť N je n-prvková množina a M je m-prvková množina. Určete počet:

(a) zobrazení množiny N do množiny M,

(b) prostých zobrazení N do M,

(c) bijekcí mezi N a M.

▶ **1.25** Najděte příklad zobrazení $f : \mathbf{N} \to \mathbf{N}$, které

(a) je prosté, ale není na,

(b) je na, ale není prosté.

▶ **1.26** (a) Je-li $f \circ g$ zobrazení na, musí f být na? Musí g být na?

(b) Je-li $f \circ g$ prosté zobrazení, musí f být prosté? Musí g být prosté?

▶ **1.27** Nechť $p : Y \to Z$ je prosté zobrazení. Ukažte, že pro zobrazení $f, g : X \to Y$ platí, že pokud $p \circ f = p \circ g$, potom $f = g$. Najděte analogický fakt pro zobrazení p, které je na.

▶ **1.28** Mějme zobrazení $f\colon S \to T$, $g\colon T \to S$. Řekneme, že g je *pravé*, resp. *levé inverzní zobrazení* k f, platí-li $f \circ g = E_S$, resp. $g \circ f = E_T$. Dokažte, že zobrazení f je:

(a) prosté, právě když f má pravé inverzní zobrazení,

(b) na, právě když f má levé inverzní zobrazení,

(c) bijekce, právě když má pravé i levé inverzní zobrazení a tato zobrazení jsou shodná.

▶ **1.29** Relace $R \subset A \times B$ je:

(a) zobrazení, právě když R^{-1} je zobrazení,

(b) bijekce, právě když R^{-1} je bijekce,

Dokažte.

▶ **1.30** Dokažte, že pro bijekce $f\colon X \to Y$ a $g\colon Y \to Z$ platí:

(a) $E_X = f \circ f^{-1}$,

(b) $E_Y = f^{-1} \circ f$,

(c) $f \circ g$ je bijekce.

▶ **1.31** Najděte bijekci:

(a) množiny sudých celých čísel $2\mathbf{Z}$ na množinu celých čísel $\mathbf{Z}$,

(b) množiny celých čísel $\mathbf{Z}$ na množinu kladných celých čísel $\mathbf{N}^+$,

▶ **1.32** Dokažte, že zobrazení $f\colon \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ definované předpisem $f(m,n) = 3^n \cdot 2^m$ je bijekce.

1.6 Znázornění relací na množině X

Pro tuto chvíli opustíme relace z množiny X do množiny Y a budeme se věnovat výhradně relacím na jediné množině X. Pro takové relace máme k dispozici ještě několik typů znázornění. Vezměme si jako příklad relaci R na množině $X = \{a,b,c,d,e,f\}$ definovanou vztahem

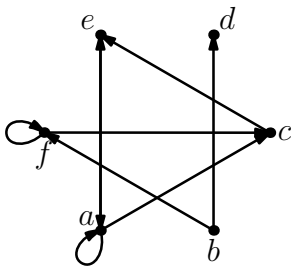
$$R = \{(a,a),(f,f),(a,c),(a,e),(b,d),(b,f),(f,c),(e,a),(c,e)\}.$$

U *maticového* znázornění relace R sestrojíme matici, řekněme $M(R)$, jejíž řádky (a právě tak sloupce) jednoznačně odpovídají prvkům množiny X. V matici $M(R)$ bude na řádku odpovídajícím prvku x a ve sloupci odpovídajícím prvku y jednička, pokud $x\,R\,y$, a v opačném případě tam bude nula. Pro výše uvedenou relaci R dostaneme matici

$$M(R) = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

v níž řádky odpovídají shora dolů (a sloupce zleva doprava) prvkům $a,\ldots,f$.

Další variantou je znázornění v podobě *orientovaného grafu*. Idea je podobná jako u grafového znázornění, ovšem s tím, že nyní můžeme ušetřit jednu množinu bodů. Každý prvek množiny x bude nyní zastoupen jen jedním bodem (a ne dvěma, jako by tomu bylo na obr. 1.1b). Vztah $x\,R\,y$ znázorníme šipkou z bodu x do bodu y. Výsledek pro výše uvedenou relaci R je na obr. 1.5.



Obrázek 1.5: Relace R jako orientovaný graf.

1.7 Vlastnosti relací

Vzhledem k obecnosti pojmu relace je přirozené, že se relace dále dělí podle toho, zda mají nebo nemají určité základní vlastnosti.

Definice 1.8 Relace R na množině X je

- *reflexívní*, pokud pro každé $x \in X$ platí $x\,R\,x$,
- *symetrická*, pokud pro každé $x, y \in X$,

$$x\,R\,y \Rightarrow y\,R\,x,$$

- *slabě antisymetrická*, pokud pro každé $x, y \in X$,

$$x\,R\,y \quad \text{a} \quad y\,R\,x \Rightarrow x = y,$$

- *tranzitivní*, pokud pro každé $x, y, z \in X$,

$$x\,R\,y \quad \text{a} \quad y\,R\,z \Rightarrow x\,R\,z.$$

Tyto vlastnosti většinou mají srozumitelnou interpretaci v jednotlivých znázorněních relace R. Uvažme třeba znázornění pomocí orientovaného grafu. Reflexívní relaci poznáme podle toho, že v tomto orientovaném grafu je u každého z bodů 'smyčka', u symetrické relace má každá z čar svou dvojnici v opačném směru, atd. (Dále viz cvičení 1.38.)

Příklad 1.9 Uvažme relaci S, definovanou na množině kladných reálných čísel $\mathbf{R}^+$ předpisem

$$x\,S\,y \quad \text{právě když} \quad 2x < y.$$

Tato relace není reflexívní, protože dokonce pro žádné $x \in \mathbf{R}^+$ není $2x < x$. Není ani symetrická (stačí uvážit $x = 1, y = 3$), a to do té míry, že je dokonce slabě[4] antisymetrická. Kdyby totiž $2x < y$ a $2y < x$, pak bychom dostali $4x < x$, což je na $\mathbf{R}^+$ nemožné. Žádná dvojice tedy nesplňuje předpoklad implikace v definici antisymetričnosti. Relace S je také tranzitivní: pokud $2x < y$ a $2y < z$, pak $2x < z/2$ a tedy $2x < z$.

Situace se dramaticky změní, pokud uvažujeme relaci S' zadanou stejným předpisem, ale na množině záporných reálných čísel $\mathbf{R}^-$. Relace S' totiž *je* reflexívní a *není* slabě antisymetrická (dokažte!). Není ani tranzitivní, jak ukazuje trojice $x = -2, y = -3, z = -4$, pro kterou máme $2x < y$ a $2y < z$, ale neplatí $2x < z$.

Cvičení

▶ **1.33** Dokažte, že zobrazení $f : X \to X$ je jakožto relace na množině X:

(a) reflexívní, právě když f je identické zobrazení,

(b) symetrické, právě když f je bijekce a $f = f^{-1}$,

(c) tranzitivní, právě když pro všechna $y \in f(X)$ platí $y \in f^{-1}(y)$, kde $f^{-1}(y) = \{x \in X : f(x) = y\}$.

Jak je možné charakterizovat slabě antisymetrická zobrazení?

▶ **1.34** Nechť $X \subset \mathbf{Z}$ je nějaká množina celých čísel. *Relace dělitelnosti* na X je množina všech dvojic $(x, y) \in X^2$ takových, že x dělí y (tj. existuje $k \in \mathbf{Z}$ s vlastností $kx = y$). Dokažte, že relace dělitelnosti je slabě antisymetrická na množině přirozených čísel $\mathbf{N}$, ale ne na množině nenulových celých čísel $\mathbf{Z} - \{0\}$.

▶ **1.35** Rozhodněte, zda relace S v tabulce 1.1 jsou na příslušných množinách X (1) reflexívní, (2) symetrické, (3) slabě antisymetrické, (4) tranzitivní. Kladné odpovědi dokažte, záporné doložte protipříkladem.

▶ **1.36** Je libovolná tranzitivní a symetrická relace na nějaké množině nutně reflexívní?

▶ **1.37** Dokažte, že je-li relace na množině symetrická i antisymetrická, je nutně tranzitivní. Charakterizujte tyto relace.

▶ **1.38** Jak poznáme z maticového znázornění, zda je relace reflexívní a symetrická?

▶ **1.39** Dokažte, že relace R na množině X je tranzitivní, právě když $R \circ R \subset R$.

[4] I silně, ale tento pojem jsme zatím nedefinovali.

	množina X	$x\,S\,y$, pokud ...
(a)	$\mathbf{R}$	$x \leq y$
(b)	$\mathbf{R}$	$x < y$
(c)	rovina $\mathbf{R}^2$	vzdálenost bodů x a y je ≤ 1
(d)	přímky v $\mathbf{R}^2$	x je rovnoběžná s y
(e)	$\{1,2,3,4\}$	$(x,y) \in \{(1,1),(2,3),(3,2),(3,4),(4,3)\}$
(f)	přirozená čísla $\mathbf{N}$	x dělí y
(g)	nenulová celá čísla $\mathbf{Z} - \{0\}$	x dělí y
(h)	uzavřený interval $[0,1]$	$x + y \leq xy$
(i)	$\mathbf{N}$	$x^2 \leq y$
(j)	$[0,1)$	$x^2 \leq y$
(k)	$\mathbf{R}$	$x < 2y$
(l)	$\mathbf{R}$	$x - y \in \mathbf{Z}$.

Tabulka 1.1: Relace v cvičení 1.35.

▶ **1.40** Nechť R je relace na množině X. *Tranzitivní uzávěr* relace R je relace R^+ (rovněž na X) sestávající ze všech dvojic (x,y), pro které lze najít konečný počet prvků $z_1, \ldots, z_k$ s vlastností

$$x\,R\,z_1\,R\,z_2\,R\,\ldots\,R\,z_k\,R\,y.$$

(Tento zkrácený zápis samozřejmě znamená $x\,R\,z_1$, $z_1\,R\,z_2$ atd.) Dokažte, že

(a) R^+ je tranzitivní relace,

(b) je to dokonce nejmenší tranzitivní relace na X obsahující R. (Přesněji: pokud T je tranzitivní relace na X, která obsahuje relaci R, pak také $R^+ \subset T$.)

▶ **1.41** Nechť relace R na množině X je reflexívní (symetrická, antisymetrická, tranzitivní). Je pak R^{-1} také reflexívní (symetrická, antisymetrická, tranzitivní)?

1.8 Ekvivalence a rozklady

Význačné místo mezi relacemi mají ekvivalence.

Definice 1.10 *Ekvivalence na množině X* je relace R na množině X, která je reflexívní, symetrická a tranzitivní.

Příklad 1.11 Dobrý příklad ekvivalence se objevil ve cvičení 1.35. Nechť X je množina všech přímek v rovině. Definujme na X relaci R předpisem

$$(p,q) \in R \quad \text{právě když} \quad p \text{ a } q \text{ jsou rovnoběžné přímky.}$$

Pečlivý čtenář již určitě nahlédl, že relace má všechny tři vlastnosti z definice ekvivalence.

Příklad 1.12 Důležitým příkladem ekvivalence, který se nám bude hodit v příští kapitole, je *kongruence modulo p*. Jde o relaci na množině celých čísel $\mathbf{Z}$. Zvolme pevně celé číslo p a definujme relaci $\equiv$ na $\mathbf{Z}$ předpisem

$$x \equiv y \quad \text{právě když} \quad p \text{ dělí } x - y.$$

(Připomeňme, že p *dělí* $x - y$, pokud $x - y = pk$ pro nějaké $k \in \mathbf{Z}$.)

Relace $\equiv$ je reflexívní, protože p jistě pro každé x dělí číslo $x - x = 0$. Je také symetrická, neboť pokud $x - y = kp$, pak $y - x = (-k) \cdot p$.

Dokažme, že $\equiv$ je tranzitivní. Mějme x, y, z s vlastností $x \equiv y$ a $y \equiv z$. Je tedy $x - y = kp$ a $y - z = \ell p$ pro nějaké k, ℓ. Pak ovšem

$$x - z = (x - y) + (y - z) = kp + \ell p = p(k + \ell)$$

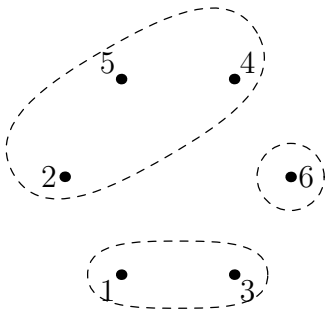
a $x \equiv z$. Tím je tranzitivita dokázána. Relace $\equiv$ tedy skutečně je ekvivalence.

Relacím, které jsou pouze reflexívní a symetrické (a nemusí být tranzitivní) se někdy říká *tolerance*.

Příklad 1.13 Nechť X je množina všech k-tic nul a jedniček, kde $k \geq 2$. Dvě k-tice jsou v relaci R, pokud se liší nejvýše v jednom symbolu. Taková relace R je tolerancí, nikoli však ekvivalencí (ověřte!). Jak je tomu pro $k = 1$?

Ekvivalence úzce souvisí s pojmem rozkladu množiny.

Definice 1.14 Nechť X je množina. (Neuspořádaný) soubor podmnožin $\{X_i\}_{i \in I}$ množiny X je *rozklad* množiny X, pokud množiny X_i jsou neprázdné, navzájem disjunktní a jejich sjednocením je celá množina X. Množiny X_i nazýváme *třídy* rozkladu $\{X_i\}_{i \in I}$.



Obrázek 1.6: Rozklad množiny $\{1, 2, 3, 4, 5, 6\}$.

Soubor $\mathcal{S} = \{\{1, 3\}, \{6\}, \{2, 4, 5\}\}$, znázorněný na obr. 1.6, je například rozkladem množiny $X = \{1, 2, 3, 4, 5, 6\}$, zatímco soubory

$$\{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 5, 6\}\} \text{ a } \{\{1, 2\}, \{3, 4, 5\}\}$$

nikoli. Zdůrazněme, že u rozkladu nezáleží na pořadí, ve kterém jsou jeho třídy uvedeny, takže soubor $\{\{2, 4, 5\}, \{6\}, \{1, 3\}\}$ je totožný s rozkladem $\mathcal{S}$.

Věta 1.15 *Ekvivalence na X jednoznačně odpovídají rozkladům X.*

Důkaz. Ukážeme, jak dané ekvivalenci $\sim$ na množině X bijektivně přiřadit rozklad $X/\sim$ množiny X. Pro $x \in X$ definujme *třídu prvku* x předpisem

$$[x]_\sim = \{y \in X : x \sim y\}.$$

Místo $[x]_\sim$ budeme psát stručněji $[x]$.

Tvrdíme, že pro $x, y \in X$ jsou třídy $[x]$, $[y]$ buď shodné nebo disjunktní. Dejme tomu, že nejsou disjunktní, tedy existuje $z \in [x] \cap [y]$.

Vezměme libovolný prvek $x' \in [x]$. Máme $x \sim x'$ a ze symetrie také $x' \sim x$. Protože $z \in [x]$, je rovněž $x \sim z$, takže z tranzitivity plyne $x' \sim z$. Konečně z faktu $z \in [y]$ dostaneme $y \sim z$, takže $z \sim y$ a z tranzitivity $x' \sim y$. Jinými slovy $x' \in [y]$. Ukázali jsme, že každý prvek x' třídy $[x]$ je rovněž prvkem třídy $[y]$. Totéž ale platí i naopak (důkaz je stejný), takže $[x] = [y]$. To jsme chtěli dokázat.

Vezmeme-li tedy soubor množin $X/\sim = \{[x] : x \in X\}$ (který obsahuje každou třídu pouze jednou!), dostaneme systém disjunktních podmnožin množiny x. Díky reflexivitě je každá třída neprázdná (protože $x \in [x]$) a sjednocením všech tříd je množina X. Jedná se tedy o rozklad množiny X.

Je-li naopak dán rozklad $\{X_i : i \in I\}$ množiny X, definujme relaci R předpisem

$$x\,R\,y, \quad \text{pokud } x \text{ a } y \text{ jsou prvky téže množiny } X_i.$$

Relace R je takřka z triviálních důvodů ekvivalencí (proč?).

K dokončení důkazu zbývá si všimnout, že pokud podle výše uvedených předpisů přiřadíme nějaké ekvivalenci $\sim$ rozklad a tomu zase ekvivalenci, dostaneme právě výchozí ekvivalenci $\sim$. Podobně je tomu, vyjdeme-li od rozkladu. Popsaná korespondence mezi rozklady a ekvivalencemi tedy opravdu představuje bijektivní vztah. □

Je-li $\sim$ ekvivalence, pak se třídy příslušného rozkladu nazývají *třídy ekvivalence* $\sim$.

Příklad 1.16 Uvažme relaci R na množině $\{1, \ldots, 6\}$ s následujícím maticovým znázorněním:

$$M(R) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

(Řádky i sloupce odpovídají po řadě prvkům 1, ... ,6.) Ověřte, že se jedná o ekvivalenci. Sestrojíme-li příslušný rozklad jako v důkazu věty 1.15, dostaneme právě rozklad na obr. 1.6.

Cvičení

▶ **1.42** Definujme relaci $\sim$ podobně jako $\equiv$ v příkladu 1.12, s jedním malým rozdílem:

$$x \sim y \quad \text{právě když existuje } \textit{přirozené } k \text{ tak, že } x - y = kp,$$

kde k přirozeným číslům řadíme i nulu. Je relace $\sim$ ekvivalence?

▶ **1.43** Dokažte, že průnik libovolného souboru ekvivalencí na dané množině X je rovněž ekvivalence.

▶ **1.44** Nechť R a S jsou ekvivalence na množině X. Rozhodněte, které z následujících relací jsou nutně také ekvivalence:

(a) $R \cup S$,

(b) $R - S$,

(c) $R \circ S$.

▶ **1.45** Dokažte: složení $R \circ S$ ekvivalencí R a S je ekvivalence, právě když R a S jsou záměnné (tj. $R \circ S = S \circ R$).

▶ **1.46** Zjistěte, zda následující relace na množině $\mathbf{R}^2$ jsou ekvivalence, a případně najděte geometrickou interpretaci jejich tříd. U každého případu je uvedena podmínka pro to, aby dvojice (x, y) a (z, w) z množiny $\mathbf{R}^2$ byly spolu v relaci.

(a) $y - x = w - z$,

(b) $y - kx = w - kz$ (kde $k \in \mathbf{R}$),

(c) $x^2 + 4y^2 = z^2 + 4w^2$.

▶ **1.47** Nechť $\mathbf{R}^{n\times n}$ je množina všech reálných matic o rozměrech $n \times n$. Pro dvě takové matice A, B definujme[5]

$$A \approx B, \quad \text{pokud } A \text{ a } B \text{ mají stejnou hodnost,}$$
$$A \simeq B, \quad \text{pokud } A \text{ a } B \text{ jsou podobné matice.}$$

Ukažte, že obě tyto relace jsou ekvivalence na $\mathbf{R}^{n\times n}$, a určete počet jejich tříd.

▶ **1.48** Nakreslete relaci R z příkladu 1.16 jako orientovaný graf.

▶ **1.49** Matici $M(R)$ z příkladu 1.16 je možné prohozením dvou řádků a dvou sloupců převést do velmi speciálního 'blokového' tvaru. Pokuste se tento tvar definovat, a na tomto základě formulovat obecnou charakterizaci ekvivalencí ve tvaru 'R je ekvivalence, právě když $M(R)$ má přerovnání do blokového tvaru'. Jak souvisí blokový tvar s třídami ekvivalence?

[5] Připomeňme, že A a B jsou *podobné*, pokud existuje matice P s vlastností $B = PAP^{-1}$, a že *hodnost* matice je maximální počet lineárně nezávislých řádek.

Kapitola 2

Algebraické struktury

Řada algebraických objektů má podobu množiny s nějakou dodatečnou strukturou. Například vektorový prostor je množina vektorů, ty však nejsou 'jeden jako druhý': jeden z nich hraje význačnou roli nulového vektoru, pro každé dva vektory je dán jejich součet, je definována operace násobení vektoru skalárem atd. Právě tuto dodatečnou informaci, která vektorový prostor odlišuje od pouhé množiny vektorů, máme na mysli, když mluvíme o 'struktuře'. Často se i samotné tyto objekty označují pojmem *algebraické struktury*.

2.1 Grupy a tělesa

V tomto oddílu představíme dva význačné příklady algebraických struktur: grupu a těleso. Jsou definovány jako množina s jednou resp. dvěma operacemi, které mají (v porovnání s většinou ostatních algebraických struktur) poměrně silné vlastnosti. Příkladů grup i těles je přesto podivuhodná řada, a to v nejrůznějších oblastech matematiky.

Pojem tělesa ostatně čtenář obeznámený s vektorovými prostory možná zná. Každý vektorový prostor totiž existuje nad určitým tělesem, jehož prvky jsou právě ony skaláry, jimiž můžeme vektory násobit. Vektorové prostory nad tělesem reálných čísel (probírané v přednášce z lineární algebry) jsou tak jen jedním speciálním případem.

Nechť M je množina. Zobrazení $\star$ z $M \times M$ do M se nazývá *(binární) operace na množině* M. Taková operace může mít různé vlastnosti. Řekneme, že $\star$ je *komutativní* operace, pokud pro každé $x, y \in M$ je $x \star y = y \star x$ (tedy pokud výsledek nezáleží na pořadí operandů). Operace $\star$ je *asociativní*, pokud pro $x, y, z \in M$ je $x \star (y \star z) = (x \star y) \star z$ (výsledek nezáleží na uzávorkování).

Příklad asociativní operace jsme již viděli u relací. Uvážíme-li množinu všech relací na dané množině X a definujeme-li operaci $\circ$ jako složení dvou relací, bude tato binární operace asociativní, ale nikoli komutativní.

Prvky množiny M mohou mít vzhledem k operaci $\star$ speciální vlastnosti. Prvek

$n \in M$ je *neutrálním prvkem (vzhledem k operaci $\star$)*, pokud pro každé $x \in M$ je $x \star n = x$ a rovněž $n \star x = x$. Všimněme si, že z definice triviálně plyne, že takový prvek je nejvýše jeden. Jsou-li totiž n, n' neutrální prvky, pak na jednu stranu $n \star n' = n'$ (protože n je neutrální), ale na druhou stranu $n \star n' = n$ (protože n' je neutrální), takže $n = n'$.

Nechť n je neutrální prvek vzhledem k operaci $\star$. *Prvek inverzní k prvku $x \in M$* je takový prvek y, pro nějž platí, že $x \star y = y \star x = n$. V případě, že $\star$ je asociativní operace, je opačný prvek k libovolnému prvku $x \in M$ nejvýše jeden. Jsou-li totiž y, y' dva takové prvky, uvažme výraz $y \star x \star y'$. Obě jeho uzávorkování dají stejný výsledek. Přitom $(y \star x) \star y' = n \star y' = y'$, ale $y \star (x \star y') = y \star n = y$, takže $y = y'$.

Nyní již můžeme definovat pojem grupy. *Grupa* je množina M spolu s asociativní binární operací $\star$, ve které existuje neutrální prvek a ke každému prvku existuje prvek inverzní. Pokud je operace $\star$ navíc komutativní, mluvíme o *komutativní* nebo *abelovské*[1] *grupě*. Formálně grupu definujeme jako uspořádanou dvojici $(M, \star)$.

Standardním příkladem grupy je třeba množina všech reálných (celých, komplexních, racionálních) čísel s operací sčítání. Přirozená čísla se sčítáním grupu netvoří (0 je neutrální, ale neexistuje skoro žádný inverzní prvek), a třeba celá čísla s násobením rovněž ne (1 je neutrální, ale inverzní prvky rovněž neexistují). Ani v množině racionálních čísel neexistuje inverzní prvek k číslu 0 vzhledem k operaci násobení (pro žádné racionální y není $0 \cdot y = 1$). Oproti tomu množina všech *nenulových* racionálních čísel již tvoří grupu vzhledem k operaci násobení.

Množina všech matic daných rozměrů je grupou vzhledem ke sčítání. Grupou je rovněž množina všech regulárních čtvercových matic řádu n s operací násobení. Požadavek regularity je podstatný, protože k žádné singulární matici by neexistoval inverzní prvek. Spojité reálné funkce tvoří grupu vzhledem ke sčítání, permutace dané množiny vzhledem ke skládání, atd. Relace na dané množině spolu s operací skládání grupu netvoří.

K popisu grupy na konečné množině prvků je často vhodné použít tabulku, která pro každou dvojici prvků udává výsledek grupové operace. Příkladem je tab. 2.1, která definuje grupu na množině $\{a, b\}$ s operací $*$.

$*$	a	b
a	a	b
b	b	a

Tabulka 2.1: Grupa na množině $\{a, b\}$.

Pojem tělesa zachycuje dvě grupy, definované na téže základní množině. Jeho prototypem je množina všech reálných čísel $\mathbf{R}$ s operacemi $+$ a $\cdot$. Dvojice $(\mathbf{R}, +)$

[1] Používá se též označení *Abelova grupa*. Tato třída grup je nazvána po norském matematikovi Nielsu Henriku Abelovi (1802–1829).

je komutativní grupa s neutrálním prvkem 0, dvojice $(\mathbf{R}, \cdot)$ ale grupa není (stejně jako u racionálních čísel chybí inverzní prvek k číslu 0). Z tohoto důvodu v následující definici tělesa přistupujeme k neutrálnímu prvku první operace s jistou opatrností.

Nechť množina M spolu s operací $\oplus$ tvoří komutativní grupu s neutrálním prvkem (dejme tomu) 0, a nechť na množině $M - \{0\}$ je určena další binární operace $\otimes$. Potom $(M, \oplus, \otimes)$ je *těleso*, pokud $(M - \{0\}, \otimes)$ je rovněž komutativní grupa a navíc platí *distributivní zákon*:

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \tag{2.1}$$

pro každé $x, y, z \in M$.

Mezi tělesa patří množiny všech racionálních, reálných a komplexních čísel, vždy se standardními operacemi sčítání a násobení. V následujícím oddílu budeme hovořit o tělesech, která sestávají jen z konečného počtu prvků.

Všimněme si ještě, že pojem vektorového prostoru není příliš vzdálen od pojmu abelovské grupy. Dá se říci, že vektorový prostor je abelovská grupa (s operací sčítání vektorů), na které je navíc definováno násobení vektorů prvky daného tělesa.

Cvičení

► **2.1** Najděte grupu $(G, \star)$ o 4 prvcích, ve které pro každý prvek x platí $x \star x = 0$.

► **2.2** *Isomorfismus* grup $(G, \star)$ a $(H, \diamond)$ je bijekce $f : G \to H$, které zobrazuje neutrální prvek grupy G na neutrální prvek grupy G a má tu vlastnost, že pro každé $g, g' \in G$ je

$$f(g \star g') = f(g) \diamond f(g').$$

Ukažte, že isomorfismus f zobrazuje inverzní prvek k libovolnému prvku $g \in G$ na inverzní prvek k prvku $f(g)$ (v grupě H).

► **2.3** Najděte dvě konečné grupy stejné velikosti, které nejsou *isomorfní* (tj. neexistuje mezi nimi isomorfismus).

2.2 Aritmetika modulo p

Připomeňme si, že ekvivalence $\sim$ na množině X je relace na X, která je reflexívní, symetrická a tranzitivní. Jsou-li na množině X definovány nějaké operace, může být přirozený požadavek, aby ekvivalence $\sim$ navíc zachovávala tyto dodatečné operace. Takovým ekvivalencím se pak říká kongruence. My se zaměříme na jeden konkrétní příklad: kongruence modulo p.

Nechť $p \geq 1$ je přirozené číslo. Definujme na množině všech celých čísel relaci $\equiv$ (*kongruenci modulo* p) předpisem

$$x \equiv y, \text{ pokud } p \text{ dělí rozdíl } x - y.$$

Je-li potřeba zdůraznit hodnotu čísla p, píšeme $x \equiv y \pmod{p}$.

Fakt, že se jedná o ekvivalenci, není ani třeba dokazovat. Každá z p tříd této ekvivalence je tvořena všemi čísly, která při dělení číslem p dávají tentýž zbytek. Proto se označují jako *zbytkové třídy modulo* p. Třídu obsahující číslo x budeme značit jako $[x]_p$ (jindy se používá značení $\mathcal{Z}_p(x)$) a o prvku x budeme mluvit jako o reprezentantu této třídy. Je-li číslo p zřejmé z kontextu, píšeme místo $[x]_p$ prostě $[x]$. Množina všech zbytkových tříd modulo p se značí $\mathbf{Z}_p$. Třídy $[0]_p$ a $[1]_p$, které mají svým způsobem význačné postavení, budeme značit prostě 0 resp. 1.

Jak je naznačeno v úvodu tohoto oddílu, kongruence modulo p se chová 'slušně' k operacím sčítání a násobení na celých číslech:

Tvrzení 2.1 *Nechť $x \equiv x'$ a $y \equiv y'$ jsou celá čísla. Potom*

$$x + y \equiv x' + y' \quad a \quad xy \equiv x'y'.$$

Důkaz. Z faktu $x \equiv x'$ plyne $x' - x = pm$, kde m je celé. Podobně $y' - y = pn$, n celé. Potom $(x' + y') - (x + y) = pm + pn = p(m + n)$, takže $x + y \equiv x' + y'$. Stejně tak $x'y' - xy = (x + pm)(y + pn) - xy = p(xn + ym + pmn)$, proto $x'y' \equiv xy$. □

Hlavním důvodem, proč je tento fakt důležitý, je, že umožňuje přenést aritmetické operace z celých čísel na zbytkové třídy, kde tak dostaneme tzv. *aritmetické operace modulo* p. Nechť číslo p je pevně dáno, takže je nemusíme explicitně uvádět. Pro třídy $[x]$ a $[y]$, zadané pomocí svých reprezentantů, definujeme jejich součet $\oplus$ a součin $\otimes$ předpisy

$$[x] \oplus [y] = [x + y]\,,$$
$$[x] \otimes [y] = [xy]\,.$$

U podobné definice je však třeba ověřit její *korektnost*: nedostaneme při jiné volbě reprezentantů tříd $[x]$ a $[y]$ jiné výsledky? Kdyby ano, jednalo by se o špatnou definici.

Proto předpokládejme, že $[x] = [x']$ a $[y] = [y']$. To samozřejmě znamená, že $x \equiv x'$ a $y \equiv y'$. Podle Tvrzení 2.1 tedy $x + x' \equiv y + y'$. Pak ovšem musí být $[x + y] = [x' + y']$, takže hodnota přiřazená součtu $[x] \oplus [y]$ je na volbě reprezentantů nezávislá. Podobně je tomu u operace $\otimes$.

Podívejme se pro konkrétnost na případ $p = 7$, třeba na třídy $[2]_7$ a $[6]_7$. Z definice je

$$[2]_7 = \{\ldots, -5, 2, 9, 16, \ldots\},$$
$$[6]_7 = \{\ldots, -1, 6, 13, 20, \ldots\}.$$

Všechny možné součty prvku z třídy $[2]_7$ a prvku z třídy $[6]_7$ tvoří množinu

$$\{\ldots, -6, 1, 8, 15, 22, \ldots\},$$

což je právě třída $[8]_7$, takže je přirozené, že jsme položili $[2]_7 \oplus [6]_7 = [8]_7$. Podobně množina všech součinů prvku ze třídy $[2]_7$ a prvku ze třídy $[6]_7$ je obsažena ve třídě $[12]_7$.

Množina $\mathbf{Z}_7$ má 7 prvků, které lze psát například jako $[0]_7$, $[1]_7$, ... , $[6]_7$. Při počítání modulo p můžeme v praxi vynechat symboly pro třídy a pracovat pouze s čísly $0, 1, \ldots, p-1$ (s tzv. *úplnou soustavou zbytků modulo p*), s tím, že výsledek každé operace nahradíme příslušným zbytkem. Například při počítání modulo 5 bychom tak mohli psát třeba $3 \oplus 4 = 2$ nebo $4 \otimes 3 = 2$. Úplnou informaci o aritmetice modulo 5 podává tabulka 2.2.

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabulka 2.2: Aritmetika nad $\mathbf{Z}_5$ (v tabulce násobení je vynechán řádek a sloupec prvku 0, které sestávají ze samých nul).

Věta 2.2 *Pro libovolné $p \geq 1$:*

(a) dvojice $(\mathbf{Z}_p, \oplus)$ je komutativní grupa,

(b) operace $\otimes$ na $\mathbf{Z}_p - \{0\}$ je komutativní, asociativní a má neutrální prvek,

(c) operace $\oplus$ na $\mathbf{Z}_p$ je distributivní vzhledem k operaci $\otimes$, tj.

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

pro libovolné $a, b, c \in \mathbf{Z}_p$.

Důkaz. Věta snadno plyne z vlastností aritmetických operací na celých číslech. V části (a) je například operace $\oplus$ komutativní, protože

$$[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]\,.$$

Podobně dostaneme asociativitu. Třída $[0]$ je zjevně neutrální vzhledem ke sčítání. Inverzní prvek ke třídě $[a]$ je třída $[-a]$.

Část (b) se dokazuje zcela podobně. Část (c) je opět důsledkem distributivity na celých číslech, protože platí

$$[a] \otimes \Big([b] \oplus [c]\Big) = [a] \otimes [b+c] = [a(b+c)] = [ab+ac] = [ab] \oplus [ac]$$
$$= \Big([a] \otimes [b]\Big) \oplus \Big([a] \otimes [c]\Big).$$

□

Je $\mathbf{Z}_p$ spolu s operacemi $\oplus$ a $\otimes$ tělesem? Podle věty 2.2 k tomu mnoho nechybí: vlastně pouze to, aby ke každé nenulové třídě existoval inverzní prvek vzhledem k násobení. Pak by totiž i $(\mathbf{Z}_p, \otimes)$ byla abelovská grupa. Ptáme se tedy, kdy ke třídě $[x] \in \mathbf{Z}_p$ existuje inverzní prvek vzhledem k násobení. Asi tomu tak nebude vždy; například pro $p = 4$ nenajdeme inverzní prvek ke třídě $[2]_4$. Máme totiž $[2]\otimes[1] = [2]$, $[2]\otimes[2] = [0]$ a $[2]\otimes[3] = [2]$. Na druhou stranu například $\mathbf{Z}_5$ tělesem je, jak se lze přesvědčit z výše uvedené tabulky operace $\otimes$. Úplnou odpověď na naši otázku nabízí následující tvrzení.

Tvrzení 2.3 *Ke třídě $[r] \in \mathbf{Z}_p$ existuje inverzní prvek vzhledem k násobení, právě když r a p jsou nesoudělná čísla.*

Důkaz. Implikaci zleva doprava dokážeme sporem. Dejme tomu, že r i p jsou dělitelná číslem $d > 1$, a nechť $[s]$ je inverzní k $[r]$, to jest $[r]\otimes[s] = [1]$. Z definice je $[rs] = [1]$, takže rozdíl $rs - 1$ je dělitelný číslem p, řekněme $rs - 1 = pn$, kde n je celé. Pak ale

$$rs - pn = 1,$$

přičemž levá strana je dělitelná číslem d (které dělí jak r, tak p). Proto musí číslo d dělit i jedničku na pravé straně, takže $d = 1$. Spor.

K důkazu opačné implikace předpokládejme, že čísla r a p jsou nesoudělná. Uvažme p součinů $1 \cdot r$, $2 \cdot r$, ... , $p \cdot r$. Tvrdíme, že žádné dva z těchto součinů nejsou kongruentní modulo p, tedy že $ir \not\equiv jr$ pro různé i, j. Představme si, že $ir \equiv jr$ pro nějaké $i \neq j$. Pak p dělí $r(i-j)$, a protože s r je nesoudělné, musí p dělit rozdíl $i - j$. (Tento fakt plyne například z jednoznačnosti rozkladu na prvočísla.) Ovšem rozdíl $i - j$ je v absolutní hodnotě menší než p, takže jedinou možností je $i = j$, což je spor s předpokladem.

V každé zbytkové třídě modulo p tím pádem leží nejvýše jeden součin $i \cdot r$, kde $i = 1, \ldots, p$. Tříd je ale (stejně jako součinů) přesně p, takže dokonce v každé třídě leží právě jeden tento součin. Speciálně pro nějaké i je $ir \in [1]$. Pak ale $[i] \otimes [r] = [ir] = [1]$, čili $[i]$ je hledaný inverzní prvek ke třídě $[r]$. □

Z této věty již snadno plyne charakterizace čísel p, pro něž je $\mathbf{Z}_p$ tělesem. Každé prvočíslo p je nesoudělné s libovolným číslem, které není násobkem p. Na druhou stranu, pokud p není prvočíslo, pak se dá psát jako $p = a \cdot b$ (kde $1 < a, b < p$), a potom a, p jsou soudělná čísla. Shrnuto:

Důsledek 2.4 *Množina $\mathbf{Z}_p$ s operacemi $\oplus$ a $\otimes$ je tělesem, právě když p je prvočíslo.*

Nabízí se ještě další otázka. Víme, že $\mathbf{Z}_p$ je těleso pouze pro prvočíselná p. Existuje těleso o neprvočíselném počtu prvků, řekněme čtyřprvkové? Jak ukazuje cvičení 2.8, odpověď zní ano. Obecně platí věta, kterou nebudeme dokazovat, že n-prvkové těleso existuje právě tehdy, když n je mocnina prvočísla.

Nechť p je prvočíslo. Víme-li, že $\mathbf{Z}_p$ je těleso, nic nám nebrání uvažovat o vektorových prostorech nad tímto tělesem. Podobně jako jedním ze základních příkladů vektorového prostoru nad reálnými čísly je prostor $\mathbf{R}^n$, tvořený n-ticemi reálných čísel, zde hraje důležitou roli vektorový prostor

$$\mathbf{Z}_p^n = \{(a_1, \ldots, a_n) : a_i \in \mathbf{Z}_p \text{ pro každé } i\},$$

přičemž sčítání $+$ a násobení skalárem $\cdot$ jsou definovány 'po složkách':

$$\begin{aligned}(a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 \oplus b_1, \ldots, a_n \oplus b_n),\\ c \cdot (a_1, \ldots, a_n) &= (c \otimes a_1, \ldots, c \otimes a_n),\end{aligned}$$

kde $c \in \mathbf{Z}_p$. Všimněme si, že protože jednotlivé složky vektorů jsou prvky $\mathbf{Z}_p$, sčítáme je pomocí operace $\oplus$ a násobíme pomocí operace $\otimes$.

V dalších částech přednášky se setkáme se speciálním případem této konstrukce, vektorovým prostorem $\mathbf{Z}_2^n$ nad $\mathbf{Z}_2$, jehož prvky jsou n-tice nul a jedniček.

Ve vektorových prostorech nad konečnými tělesy lze provádět všechny obvyklé operace jako v reálných vektorových prostorech, například řešit soustavy rovnic. Jako příklad řešme soustavu

$$\begin{aligned}x + 2y + 3z + 4t &= 1\\ x + y + 2z &= 0\end{aligned} \tag{2.2}$$

o 4 neznámých nad tělesem $\mathbf{Z}_5$ (viz tabulka 2.2). Pro přehlednost vynecháváme třídové závorky a aritmetické operace zapisujeme jako $+$, $\cdot$ (a nikoli $\oplus, \otimes$).

Standardním postupem vytvoříme matici a převedeme ji do kanonického tvaru:

$$\left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1\\ 1 & 1 & 2 & 0 & 0 \end{array}\right] \sim \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1\\ 0 & 4 & 4 & 1 & 4 \end{array}\right] \sim \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1\\ 0 & 1 & 1 & 4 & 1 \end{array}\right]$$
$$\sim \left[\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 4\\ 0 & 1 & 1 & 4 & 1 \end{array}\right],$$

přičemž provedené úpravy jsou (po řadě): přičtení čtyřnásobku prvního řádku k druhému, vynásobení druhého řádku 'číslem' 4, a přičtení trojnásobku druhého řádku k prvnímu. Zjišťujeme, že řešení této soustavy mají tvar

$$\{(4 + 4z + 4w, 1 + 4z + w, z, w) : z, w \in \mathbf{Z}_5\}.$$

Jinak řečeno, každé řešení je lineární kombinací

$$(4, 1, 0, 0) + z \cdot (4, 4, 1, 0) + w \cdot (4, 1, 0, 1)$$

kde $z, w \in \mathbf{Z}_5$.

Cvičení

► **2.4** Nechť $x, y \in \mathbf{Z}_2^n$. Kdy je i-tá složka součtu $x + y$ nulová?

► **2.5** Kolik je řešení soustavy (2.2)?

► **2.6** Řešte soustavu nad tělesem $\mathbf{Z}_3$:

$$\begin{aligned} x + 2y + t &= 1 \\ 2x + 2z &= 1 \\ 2x + z + t &= 0 \end{aligned}$$

► **2.7** Napište tabulky sčítání a násobení v tělesech $\mathbf{Z}_2$ a $\mathbf{Z}_7$.

► **2.8** Ověřte, že množina $\{0, 1, 2, 3\}$ spolu s operacemi $\star$ a $\circ$, zadanými pomocí následujících tabulek, je tělesem. Ukažte, že tyto operace se liší od sčítání a násobení na množině $\mathbf{Z}_4$.

$\star$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\circ$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

►► **2.9** Nechť $a \equiv a' \pmod{b}$. Dokažte, že platí

$$(a, b) = (a', b),$$

kde (a, b) je největší společný dělitel čísel a a b. Využijte tento fakt k návrhu algoritmu pro výpočet největšího společného dělitele. (Jeden z takových algoritmů je znám jako *Eukleidův algoritmus*.)

►► **2.10** Nechť a a b jsou celá čísla (alespoň jedno nenulové). Dokažte, že (a, b) je nejmenší kladné číslo tvaru $ax + by$, kde $x, y \in \mathbf{Z}$.

► **2.11** Formulujte algoritmus na nalezení koeficientů x a y v rovnosti $ax + by = (a, b)$. (Užijte Eukleidův algoritmus nebo vlastní algoritmus ze cvičení 2.9.)

► **2.12** Jak je možné užít algoritmus ze cvičení 2.11 k nalezení inverzního prvku a^{-1} k prvku $a \in \mathbf{Z}_p$?

► **2.13** Dokažte, že pokud $x \equiv y \pmod{m}$, pak $x^n \equiv y^n \pmod{m}$ pro libovolné přirozené n.

► **2.14** Dokažte, že pokud $x \equiv y \pmod{m}$, celé číslo d dělí x a y, a platí $(d, m) = 1$, pak

$$\frac{x}{d} \equiv \frac{y}{d} \pmod{m}.$$

Je možné předpoklad $(d, m) = 1$ vynechat?

► **2.15** Odvoďte pravidla pro dělitelnost čísly 3, 8, 9 a 11.

Kapitola 3

Uspořádání a svazy

Pojem uspořádání, který je tématem této kapitoly, představuje (vedle zobrazení a ekvivalence) další zajímavý a důležitý speciální případ pojmu relace.

3.1 Uspořádání

Definice 3.1 *Uspořádání* na množině X je libovolná relace na X, která je reflexívní, (slabě) antisymetrická a tranzitivní.

Oproti definici ekvivalence jsme tedy 'pouze' zaměnili symetričnost za antisymetričnost. Účinky této změny jsou však značné.

Je-li R uspořádání na množině X, pak dvojice (X, R) se nazývá *uspořádaná množina*. Jsou-li prvky x, y v relaci R (tedy $x\,R\,y$), interpretujeme to slovy 'prvek x je menší nebo roven prvku y'. To je v souladu se všemi třemi základními vlastnostmi uspořádání. Uspořádáním z naší definice se také říká *neostrá uspořádání*, protože pro každé x platí $x\,R\,x$. (U *ostrého* uspořádání bychom požadavek reflexivity nahradili *antireflexivitou*: pro žádné x neplatí $x\,R\,x$. Nepůjde ovšem o uspořádání ve smyslu definice 3.1.) Neostrá uspořádání často značíme symboly $\leq$ nebo $\preceq$.

Snadno se ověří, že vlastnosti uspořádání má například 'standardní' uspořádání $\leq$ množiny reálných čísel. Poněkud zajímavější je možná fakt, že uspořádáním je i *relace dělitelnosti* definovaná vztahem 'x dělí y' na libovolné množině přirozených čísel (viz cvičení 1.35). Tyto dva příklady se liší v jednom důležitém ohledu, který podrobně rozebereme.

Nechť x, y jsou dva prvky uspořádané množiny $(X, \preceq)$. Platí-li $x \preceq y$ nebo $y \preceq x$, jsou prvky x, y *porovnatelné*, v opačném případě jsou *neporovnatelné*. Uspořádání $\preceq$ se často označuje jako *částečné*, protože definice 3.1 připouští existenci dvojic neporovnatelných prvků. Podobně o množině $(X, \preceq)$ mluvíme jako o *částečně uspořádané množině*[1].

[1] V angličtině se vžil termín *poset*, který vznikl jako zkratka z výrazu *partially ordered set*.

Při standardním uspořádání $\leq$ na množině $\mathbf{R}$ jsou každé dva prvky porovnatelné. Takovým uspořádáním se říká *lineární* nebo *úplné*. Důvodem pro první označení je fakt, že lineární uspořádání řadí prvky dané množiny do jedné linie, 'od nejmenšího k největšímu'. Lépe to uvidíme, až budeme mluvit o Hasseových diagramech. Náš druhý příklad, relace dělitelnosti na přirozených číslech, lineární není, jak ukazuje například neporovnatelná dvojice $\{2, 3\}$. Zdůrazněme ovšem, že *oba* zmíněné příklady spadají do obecnější kategorie částečných uspořádání.

Přidejme ještě třetí příklad uspořádání. Pro libovolnou množinu A můžeme uvážit nějaký soubor $\mathcal{B}$ jejích podmnožin. Na souboru $\mathcal{B}$ je pak přirozeně definováno *uspořádání inkluzí* $\subset$: podmnožiny $B, B' \in \mathcal{B}$ budou v relaci (tedy $B \subset B'$), pokud B je podmnožinou množiny B'. Ani uspořádání $\subset$ obecně není lineární.

Cvičení

► **3.1** Jsou následující relace uspořádání? Pokud ano, vypište dvojice neporovnatelných prvků.

(a) $R = \{(1, 2), (2, 3), (3, 4)\}$,

(b) $S = \{(1, 3), (2, 3), (3, 4), (3, 5), (1, 4), (2, 4), (1, 5), (2, 5)\}$.

► **3.2** Nechť $\leq$ (resp. $<$) je běžné neostré (resp. ostré) uspořádání množiny přirozených čísel $\mathbf{N}$. Definujme relace $\preceq_1$ a $\preceq_2$ na $\mathbf{N} \times \mathbf{N}$ předpisem:

$$(s, t) \preceq_1 (u, v), \text{ pokud } s \leq u \text{ a } t \leq v,$$
$$(s, t) \preceq_2 (u, v), \text{ pokud buďto } s < u, \text{ nebo } s = u \text{ a } y \leq v.$$

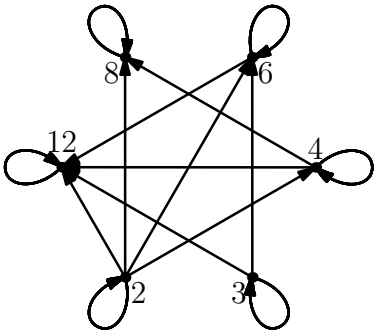
Dokažte, že $\preceq_1$ a $\preceq_2$ jsou částečná uspořádání a že $\preceq_2$ je lineární uspořádání. Poznamenejme, že $\preceq_2$ je známé *lexikografické* uspořádání (běžné ve slovnících). Pokuste se rozšířit jeho definici na množinu slov nad nějakou konečnou abecedou.

3.2 Hasseův diagram

Libovolné uspořádání samozřejmě můžeme, stejně jako každou jinou relaci, znázornit v podobě orientovaného grafu. Obrázek 3.1 je znázorněním uspořádání dělitelností na množině $\{2, 3, 4, 6, 8, 12\}$.

Jako prostředek pro znázornění uspořádání ovšem obrázek 3.1 není příliš vhodný, řada šipek je v něm totiž zbytečných. Smyčky u vrcholů by například nebylo nutné kreslit, protože každé uspořádání je z definice reflexívní. Podobně jsou-li v relaci dvojice $(2, 4)$ a $(4, 12)$, musí z tranzitivity být 2 v relaci s 12 a tuto šipku by rovněž nebylo potřeba kreslit. Efektivní znázornění uspořádání představuje tzv. Hasseův diagram.

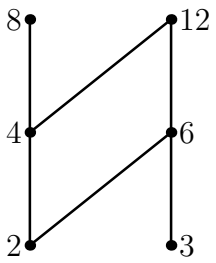
Definujme nejprve jeden pomocný pojem. Nechť x, y jsou prvky uspořádané množiny $(X, \preceq)$. Prvek x je *bezprostředním předchůdcem* prvku y (psáno $x \lhd y$),



Obrázek 3.1: Uspořádání dělitelností na množině $\{2, 3, 4, 6, 8, 12\}$.

pokud $x \preceq y$ a neexistuje žádné $z \in X - \{x, y\}$, pro které by platilo $x \preceq z \preceq y$. Na vztah $\lhd$ se můžeme dívat jako na relaci na množině X (tzv. *relace bezprostředního předcházení*). Tato relace obecně není reflexívní ani tranzitivní.

Hasseův[2] *diagram* uspořádané množiny $(X, \preceq)$ je znázornění, ve kterém pro každou dvojici prvků $x, y \in X$ platí $x \lhd y$, právě když x, y jsou spojeny čarou a prvek y je nakreslen výše než x. Spojnice není nutné opatřovat šipkou, protože směr je jednoznačně dán. Na obr. 3.2 vidíme, že Hasseovým diagramem lze uspořádanou množinu z obr. 3.1 znázornit mnohem přehledněji.

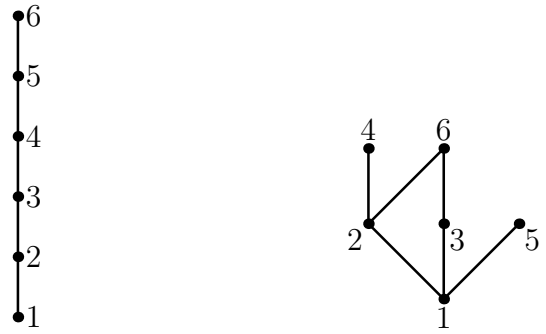


Obrázek 3.2: Hasseův diagram uspořádání z obr. 3.1.

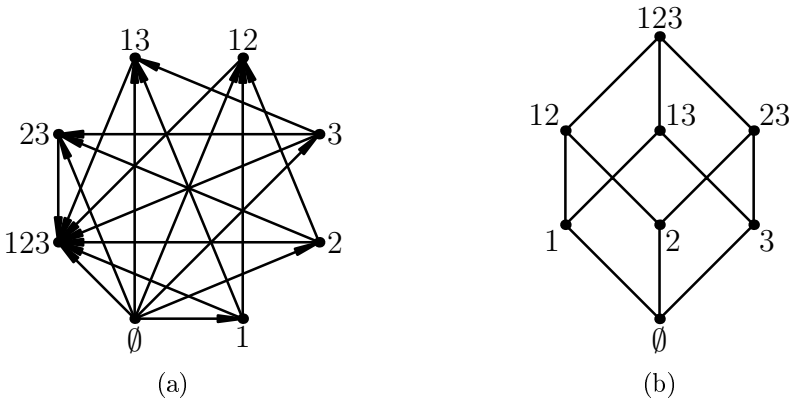
Hasseův diagram lineárně uspořádané množiny vypadá podobně, jako na obr. 3.3a, který zachycuje standardní uspořádání na množině přirozených čísel $\{1, 2, 3, 4, 5, 6\}$. Jiné uspořádání na stejné množině, které lineární není, je určeno dělitelností. Jeho Hasseův diagram je na obr. 3.3b. Jak je vidět, jednu množinu lze uspořádat mnoha různými způsoby.

Jako další příklad uvažme uspořádání inkluzí na množině všech podmnožin množiny $\{1, 2, 3\}$. Běžné zobrazení a nepoměrně přehlednější Hasseův diagram tohoto uspořádání ukazuje obr. 3.4. Podmnožiny jsou popsány zkráceně, například místo $\{1, 3\}$ píšeme prostě 13.

[2]Helmut Hasse (1898–1979).



Obrázek 3.3: (a) Obvyklé lineární uspořádání na množině $\{1, \ldots, 6\}$. (b) Uspořádání dělitelností na téže množině.



Obrázek 3.4: Dvě znázornění uspořádání inkluzí na souboru všech podmnožin množiny $\{1, 2, 3\}$: (a) orientovaný graf (s vynechanými smyčkami), (b) Hasseův diagram.

Cvičení

▶ **3.3** Jak vypadá relace bezprostředního předcházení na uspořádané množině $(\mathbf{R}, \leq)$?

▶ **3.4** Nakreslete Hasseův diagram uspořádání dělitelností na množině $X \subset \mathbf{N}$. Zjistěte, zda tato uspořádaná množina má nejmenší resp. největší prvek.

(a) $X = \{2, 3, 4, 12, 15, 60\}$,

(b) $X = \{2, 4, 8, 12, 20, 28, 56\}$,

(c) $X = \{2, 3, 4, 6, 8, 12, 24, 36, 60\}$.

▶ **3.5** Ve cvičení 1.40 byl definován tranzitivní uzávěr R^+ relace R na množině X. Přidáme-li k relaci R^+ všechny dvojice tvaru (x, x), kde $x \in X$, dostaneme *reflexívně-tranzitivní uzávěr* (nebo prostě *uzávěr*) relace R, označovaný symbolem R^*.

(a) Ukažte, že každé uspořádání na konečné množině X je uzávěrem své relace bezprostředního předcházení.

(b) Najděte příklad nekonečné uspořádané množiny, pro kterou tomu tak není.

3.3 Základní pojmy v uspořádaných množinách

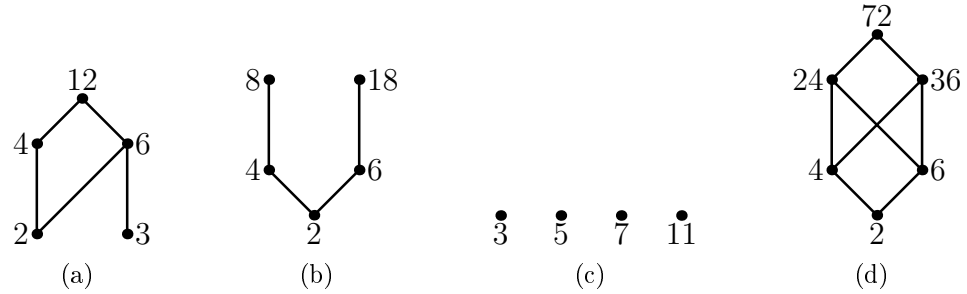
Zaveďme několik pojmů označujících význačné prvky uspořádané množiny. Mějme uspořádanou množinu $(X, \preceq)$. Prvek $a \in X$ je *největším* prvkem množiny X, pokud pro každé $x \in X$ platí $x \preceq a$. Podobně *nejmenší* prvek množiny X je prvek a takový, že $a \preceq x$ pro každé $x \in X$.

Největší prvek obecně nemusí existovat, ale existuje-li, pak je určen jednoznačně. Například na obr. 3.5a–d existuje pouze v případech (a) a (d). Nejmenší prvek existuje pouze v případech (b) a (d).

Prvky 8 a 18 na obr. 3.5b sice nejsou největší, ale mají alespoň tu vlastnost, že žádný prvek není větší. Jedná se o tzv. maximální prvky. Prvek $a \in X$ je *maximálním prvkem*, pokud pro žádné $x \in X$ není $a \preceq x$. Symetricky: *minimální prvek* je takový prvek $a \in X$, že pro žádné $x \in X$ není $x \preceq a$.

Je jasné, že případný největší prvek musí být maximální, a také, že obrácená implikace neplatí. Následující tabulka uvádí maximální a minimální prvky v jednotlivých příkladech na obr. 3.5.

příklad	maximální	minimální
(a)	12	2, 3
(b)	8, 18	2
(c)	3, 5, 7, 11	3, 5, 7, 11
(d)	72	2



Obrázek 3.5: Hasseův diagram dělitelnosti na množině X, kde (a) $X = \{2, 3, 4, 6, 12\}$, (b) $X = \{2, 4, 6, 8, 18\}$, (c) $X = \{3, 5, 7, 11\}$, (d) $X = \{2, 4, 6, 24, 36, 72\}$.

Vraťme se k uspořádání inkluzí na podmnožinách dané množiny. Příklad Hasseova diagramu takového uspořádání je na obr. 3.4b. Dá se z tohoto diagramu vyčíst více, než jenom které podmnožiny jsou ve vztahu inkluze — například jaký je průnik či sjednocení dvou množin? Jinými slovy, je možné definovat sjednocení dvou množin pouze s použitím uspořádání inkluzí?

Sjednocení množin A,B je množina, která obsahuje jak množinu A, tak množinu B (jako podmnožiny), ale 'neobsahuje nic navíc'. Přesněji řečeno, je to nejmenší ze všech množin, které jsou větší než A i než B. Slova 'nejmenší' a 'větší' se tu samozřejmě vztahují k uspořádání inkluzí. Níže definovaný pojem suprema tak lze chápat jako (dalekosáhlé) zobecnění pojmu sjednocení.

Prvek z je *horní závorou* dvojice prvků x, y uspořádané množiny $(X, \preceq)$, pokud platí $x \preceq z$ a $y \preceq z$. *Supremum* (jinak též *spojení*) prvků x, y je nejmenší ze všech jejich horních závor, tedy takový prvek s, který je horní závorou dvojice x, y, přičemž neexistuje jiná horní závora $z \neq s$, pro kterou by bylo $z \preceq s$.

Dvojice prvků obecně žádné supremum mít nemusí: předně nemusí mít ani žádnou horní závoru (jako prvky $8, 18$ na obr. 3.5b), nebo naopak může množina horních závor mít více minimálních prvků, ze kterých pak, jak víme, žádný nebude nejmenší. Tento případ nastává u prvků $4, 6$ na obr. 3.5d, které mají horní závory $24, 36$ a 72, přičemž 24 a 36 jsou minimální prvky v této množině horních závor.

Podobně jako supremum je definováno infimum dvou prvků. *Dolní závora* prvků x, y je prvek z, pro který je $z \preceq x$ a $z \preceq y$, a *infimum* (*průsek*) prvků x, y je největší z jejich dolních závor. K pojmu infima se symetrickým způsobem vztahuje vše, co bylo řečeno o supremu.

Cvičení

► **3.6** Dokažte, že v konečné uspořádané množině existuje nejmenší prvek, právě když v ní existuje přesně jeden minimální prvek. Najděte nekonečnou uspořádanou množinu, ve které tato ekvivalence neplatí.

▶ **3.7** Na množině $X = \{a, b, c, d, e, f\}$ je dána relace R. Zjistěte, zda se jedná o uspořádání a případně určete minimální a maximální prvky, pokud

(a) $R = \{(d, c), (b, a), (c, a), (d, b)\} \cup \Delta$,

(b) $R = \{(b, a), (c, a), (f, d), (b, d), (e, c), (e, a), (b, c), (b, f)\} \cup \Delta$,

kde $\Delta = \{(x, x) : x \in X\}$.

▶ **3.8** Najděte uspořádanou množinu, ve které množina horních závor nějakých dvou prvků má přesně pět minimálních prvků.

▶ **3.9** Uvažme množinu všech přirozených čísel, uspořádanou relací dělitelnosti. Existují v této uspořádané množině suprema a infima? Jaký je jejich význam?

▶ **3.10** Dokažte, že každé uspořádání na konečné množině X se dá rozšířit do lineárního. Jinými slovy: pro libovolné uspořádání R na X existuje lineární uspořádání R' na X tak, že $R \subset R'$.

▶ **3.11** Dokažte, že konečná uspořádaná množina $(L, \leq)$ má minimální prvek x a maximální prvek y tak, že $x \leq y$.

▶ **3.12** Buď U_n množina všech částečných uspořádání na n-prvkové množině X. Uvažme U_n jako uspořádanou množinu s uspořádáním daným inkluzí (uspořádání S, T jsou v relaci, pokud T *rozšiřuje* S, tedy $S \subset T$). Charakterizujte minimální a maximální prvky uspořádané množiny U_n.

3.4 Svazy

Svaz je uspořádaná množina $(X, \preceq)$, ve které existuje supremum i infimum pro libovolnou dvojici prvků. Ve svazu můžeme na supremum a infimum pohlížet jako na binární operace (protože je zaručeno, že jejich hodnoty jsou definovány pro každou dvojici). Supremum prvků x, y zde značíme $x \vee y$, infimum jako $x \wedge y$.

Příkladem svazu, na který jsme již narazili, je množina všech podmnožin libovolné množiny (uspořádaná inkluzí). Supremum dvou množin zde odpovídá jejich sjednocení, infimum odpovídá jejich průniku.

Pojmy suprema a infima jsme definovali pomocí uspořádání. Je možné postupovat v opačném směru a z pouhé znalosti binárních operací suprema a infima na množině X rekonstruovat původní uspořádání? Následující jednoduché tvrzení ukazuje, že to možné je (a dokonce stačí znát jenom suprema).

Tvrzení 3.2 *Pro libovolné dva prvky a, b svazu $(X, \preceq)$ platí*

$$a \preceq b \quad \textit{právě když} \quad a \vee b = b \quad \textit{právě když} \quad a \wedge b = a.$$

Důkaz. Nechť $a \preceq b$. Pak b je zjevně horní závorou dvojice a, b. Dejme tomu, že pro nějakou horní závoru $z \neq b$ této dvojice platí $z \preceq b$. Z faktu, že z je horní závora, plyne $b \preceq z$. Díky antisymetričnosti máme $z = b$, což je spor. Taková závora z tedy nemůže existovat, takže z definice suprema je $a \vee b = b$. Tvrzení o infimu se dokazuje symetricky. □

Jednu polovinu minulého důkazu jsme si ušetřili poukazem na symetrii mezi pojmy supremum a infimum. Jde o speciální případ tzv. principu duality, který ukážeme dále.

Inverzní relace $\preceq^{-1}$ k uspořádání $\preceq$ je opět uspořádání (cvičení 3.13). Není těžké si všimnout, že jeho Hasseův diagram získáme, když otočíme Hasseův diagram uspořádání $\preceq$ vzhůru nohama. Při této změně se suprema mění na infima a naopak. (Přesněji, supremum prvků a,b vzhledem k uspořádání $\preceq$ je jejich infimem vzhledem k uspořádání $\preceq^{-1}$.) Z toho snadno dostáváme následující *princip duality*:

> Pokud v nějakém tvrzení, které platí ve všech svazech, důsledně zaměníme symboly $\vee$ a $\wedge$ a otočíme směr všech nerovností, dostaneme opět tvrzení platné ve všech svazech.

Věta 3.3 *Pro operaci $\vee$ v libovolném svazu $(X, \preceq)$ platí:*

(i) je asociativní,

(ii) je komutativní,

(iii) $a \vee a = a$ pro $a \in X$,

(iv) $a \vee (b \wedge a) = a$ pro $a, b \in X$.

Důkaz. Část (ii) (komutativita operace $\vee$) plyne přímo z definice suprema. Část (iii) plyne z faktu, že $a \preceq a$ (reflexivita) a z tvrzení 3.2. V části (iv) víme, že $b \wedge a \preceq a$ (protože $b \wedge a$ je dolní závora dvojice a, b), takže z tvrzení 3.2 plyne, že $a \vee (b \wedge a) = a$.

Zbývá část (i), tedy asociativita operace $\vee$. Mějme prvky $a, b, c \in X$. Chceme ukázat, že $a \vee (b \vee c) = (a \vee b) \vee c$. Označme levou stranu této rovnice jako ℓ. Z definice víme, že ℓ je horní závorou pro prvky a, $b \vee c$, přičemž druhý z těchto prvků je zase horní závorou pro prvky b, c. Odtud určitě $a, b, c \preceq \ell$. Vzhledem k tomu, že $a \vee b$ je *nejmenší* horní závorou prvků a, b, musí být $a \vee b \preceq \ell$. Pak ovšem ℓ je horní závorou dvojice $(a \vee b), c$, takže pro supremum této dvojice máme

$$(a \vee b) \vee c \preceq \ell = a \vee (b \vee c).$$

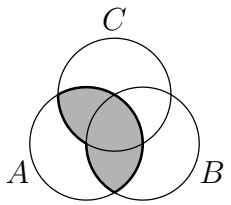
Zcela obdobně lze ukázat opačnou nerovnost $a \vee (b \vee c) \preceq (a \vee b) \vee c$. Z antisymetričnosti pak dostaneme požadovanou rovnost. □

Podobné vlastnosti jako operace $\vee$ má díky principu duality samozřejmě i operace $\wedge$ (speciálně je asociativní a komutativní).

Vlastnosti (i) a (ii) ve větě 3.3 jsou stejné, jako má operace sčítání a násobení v tělese. Může nás napadnout otázka, zda tato analogie jde ještě dál, například zda platí *distributivita* mezi operacemi $\wedge$ a $\vee$, tedy

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad \text{pro libovolné prvky } a, b, c. \tag{3.1}$$

Každý svaz, ve kterém platí (3.1), se nazývá *distributivní*. Příkladem takového svazu je svaz podmnožin libovolné množiny. Jsou-li totiž A, B, C nějaké množiny, pak z obr. 3.6 je vidět, že $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.



Obrázek 3.6: Distributivita u množin: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Na druhou stranu obr. 3.7 ukazuje dva příklady svazů, které distributivní nejsou (viz cvičení 3.14).

(a) M_5. (b) N_5.

Obrázek 3.7: Nedistributivní svazy.

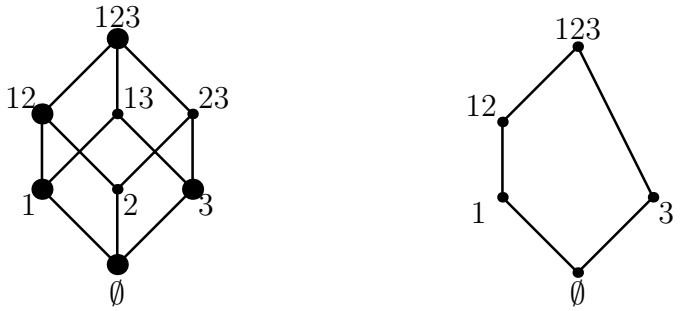
Dá se dokonce ukázat, že svazy M_5 a N_5 z obr. 3.7 jsou v jistém smyslu obsaženy v každém nedistributivním svazu. Abychom mohli tento fakt precizně vyjádřit, potřebujeme ještě jednu definici.

Podsvazem svazu $(X, \preceq)$ je libovolný svaz $(Y, \leq)$ takový, že

(1) $Y \subset X$ a uspořádání $\leq$ je *zúžením* uspořádání $\preceq$ na množinu Y (jinými slovy platí $a \leq b$, právě když $a \preceq b$ a prvky a, b leží v množině Y),

(2) suprema (infima) ve svazu $(Y, \leq)$ se shodují se supremy (infimy) ve svazu $(X, \preceq)$.

Příklad 3.4 Uvažme znovu svaz X všech podmnožin množiny $\{1,2,3\}$ s uspořádáním inkluzí, jehož Hasseův diagram známe z obr. 3.4b. Na obr. 3.8a je zvýrazněna množina $Y \subset X$. Svaz $(Y,\subset)$ na obr. 3.8b *není podsvazem* svazu $(X,\subset)$ (i když se tak při zběžném čtení definice může jevit). Prvky $\{1\}$ a $\{3\}$ totiž ve svazu $(X,\subset)$ mají supremum $\{1,3\}$, zatímco ve svazu $(Y,\subset)$ je jejich supremem prvek $\{1,2,3\}$. Přidáme-li však k množině Y prvek $\{1,3\}$ a označíme výslednou množinu Y', pak svaz $(Y',\subset)$ již je podsvazem svazu $(X,\subset)$. Poučení z uvedeného příkladu je, že ne každá množina prvků svazu určuje podsvaz.



Obrázek 3.8: (a) Svaz $(X,\subset)$ se zvýrazněnou množinou prvků Y. (b) Svaz $(Y,\subset)$.

Nyní můžeme vyslovit zajímavou charakterizaci distributivních svazů, tzv. Birkhoffovo[3] kritérium distributivity, jehož důkaz lze nalézt v [5]. Všimněme si, že jedna z implikací je triviální.

Věta 3.5 (Birkhoffovo kritérium distributivity) *Svaz je distributivní, právě když neobsahuje ani jeden ze svazů M_5, N_5 jako podsvaz.* □

Všimněme si, že svaz $(Y,\subset)$ z příkladu 3.4 je totožný se svazem M_5. Není však podsvazem distributivního svazu $(X,\subset)$ (a nedostáváme tak spor s větou 3.5).

Fakt, že 'zakázané podsvazy' z věty 3.5 jsou symetrické podle vodorovné osy, naznačuje, že při otočení distributivního svazu 'vzhůru nohama' bychom mohli opět dostat distributivní svaz. V trochu jiné formulaci to potvrzuje následující věta.

Věta 3.6 *V libovolném distributivním svazu $(X,\preceq)$ platí také duální forma distributivity:*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

pro libovolné $x,y,z \in X$.

[3] George David Birkhoff (1884–1944).

Důkaz. Položme v definici (normální) distributivity $a = x \vee y$, $b = x$, $c = z$. Dostaneme, že $p := (x \vee y) \wedge (x \vee z) = a \wedge (b \wedge c) = (a \wedge b) \vee (a \wedge c) = [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z]$. Podle duální verze věty 3.3d upravíme levou z hranatých závorek na $(x \vee y) \wedge x = x$. V pravé závorce ještě jednou uplatníme distributivitu a dostaneme $p = x \vee [(x \wedge z) \vee (y \wedge z)]$. To lze s použitím asociativity upravit na $[x \vee (x \wedge z)] \vee (y \wedge z)$ a z věty 3.3d je konečně $p = x \vee (y \wedge z)$. □

Musí ve svazu vždy existovat největší prvek? Příklad množiny reálných čísel s běžným uspořádáním ukazuje, že nikoli. Platí však následující věta:

Věta 3.7 *V konečném svazu vždy existuje největší a nejmenší prvek.*

Důkaz. Očíslujme prvky uvažovaného svazu $(X, \preceq)$ jako $X = \{a_1, \ldots, a_n\}$ a definujme posloupnost $s_1, \ldots, s_n$ induktivně předpisem $s_i = s_{i-1} \vee a_i$ pro $i = 2, \ldots, n$, přičemž $s_1 = a_1$. Tato posloupnost 'roste', přesněji $s_i \preceq s_{i+1}$ pro každé $i = 1, \ldots, n-1$. Navíc je z definice $a_i \preceq s_i$ pro každé $i = 1, \ldots, n$ (s_i je totiž horní závorou pro a_i a s_{i-1}). Pro prvek s_n musí tím pádem být $a_i \preceq s_n$, kde $i = 1, \ldots, n$, a je tedy největším prvkem množiny X. Nejmenší prvek najdeme podobně. □

Implikaci v předcházející větě není možné obrátit: uspořádaná množina s největším a nejmenším prvkem ještě zdaleka nemusí být svaz. Příkladem je množina z obr. 3.5d.

Největší prvek svazu (existuje-li) se obvykle značí jako 1, nejmenší prvek jako 0. Následující tvrzení ukazuje, že se jedná o neutrální prvky operací $\wedge$ resp. $\vee$.

Tvrzení 3.8 *Má-li svaz $(X, \preceq)$ prvky 0 a 1, pak pro každé $x \in X$ platí*

$$x \wedge 1 = x \quad a \quad x \vee 0 = x.$$

Důkaz. Prvek 1 je největší, takže pro libovolné $x \in X$ máme $x \preceq 1$. Podle tvrzení 3.2 je $x \wedge 1 = x$. Podobně pro operaci $\vee$ a prvek 0. □

Svaz podmnožin libovolné množiny A největší a nejmenší prvek má. Největším prvkem je celá množina A, nejmenším pak prázdná množina $\emptyset$.

Cvičení

► **3.13** Dokažte, že inverzní relace $\preceq^{-1}$ k libovolnému uspořádání $\preceq$ je opět uspořádání.

► **3.14** Ověřte, že uspořádané množiny M_5, N_5 na obr. 3.7 jsou svazy, a ukažte, že v nich neplatí rovnost (3.1).

► **3.15** Dokažte, že svaz $(X, \preceq)$ je distributivní, právě když pro každé $a, b, c \in X$ s vlastností $a \wedge b = a \wedge c$ a $a \vee b = a \vee c$ platí $b = c$. (Můžete použít větu 3.5.) Nalezněte příklad nedistributivního svazu, kde uvedená ekvivalence neplatí.

▶ **3.16** Nechť R je lineární uspořádání na množině X. Musí (X, R) být svaz?

▶ **3.17** Ukažte, že množina všech přirozených čísel $\mathbf{N}$ uspořádaná dělitelností je svaz. Rozhodněte, zda je tento svaz distributivní. Jaký je největší a nejmenší prvek?

▶ **3.18** (a) Nechť $D(n)$ je množina dělitelů přirozeného čísla n, uspořádaná relací dělitelnosti. Dokažte, že $D(n)$ je svaz (tzv. *svaz dělitelů* čísla n).

(b) Nechť X je konečná množina přirozených čísel, která při uspořádání relací dělitelnosti tvoří svaz. Musí tento svaz být distributivní?

▶ **3.19** Množina X je uspořádána relací dělitelnosti. Rozhodněte:

- které jsou maximální a minimální prvky množiny X,
- zda existuje největší a nejmenší prvek množiny X,
- zda X je svaz,
- zda X je distributivní svaz.

Množina X sestává z těchto prvků:

(a) $X = \{2, 4, 6, 14, 42\}$,

(b) $X = \{2, 3, 7, 14, 42\}$,

(c) $X = \{1, 2, 3, 5, 30\}$,

(d) $X = \{1, 2, 3, 12, 18, 36\}$,

(e) $X = \{1, 2, 3, 4, 12, 20, 60\}$,

(f) $X = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

▶ **3.20** Určete všechny podmnožiny X svazu dělitelů $D(12)$ čísla 12 s vlastností, že množina X (uspořádaná relací dělitelnosti) je svaz, ale není to podsvaz svazu $D(12)$.

▶ **3.21** Navrhněte algoritmus, který zjistí, zda je daná uspořádaná množina svazem. Součástí návrhu je reprezentace vstupní uspořádané množiny.

▶ **3.22** *Pevný bod* zobrazení $f : X \to X$ (kde X je nějaká množina) je každé $x \in X$, pro které je $f(x) = x$. Dokažte, že v konečném svazu L má množina pevných bodů každého zobrazení $f : L \to L$ zachovávajícího uspořádání největší a nejmenší prvek.

► **3.23** Ukažte, že v libovolném svazu $(X, \preceq)$ pro libovolnou trojici prvků x, y, z platí

$$(x \wedge y) \vee (x \wedge z) \preceq x \wedge (y \vee z).$$

►► **3.24** Platí-li pro prvky a, b, c svazu L rovnost

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c),$$

pak se hodnotě na každé straně této rovnice říká *medián* prvků a, b, c. Dokažte, že L je distributivní svaz, právě když každá trojice jeho prvků má medián.

► **3.25** Mějme svaz $(X, \preceq)$. Obdržíme opět svaz, přidáme-li k $(X, \preceq)$ nový největší prvek $1'$ a nejmenší prvek $0'$?

Kapitola 4

Booleovy algebry

Z minulé kapitoly víme, že soubor podmnožin libovolné množiny má strukturu distributivního svazu. Jeho struktura je ale bohatší o operaci, která každé podmnožině přiřazuje její doplněk. Distributivním svazům s podobnou operací se říká Booleovy algebry.

4.1 Definice

Definice 4.1 Nechť $(X, \preceq)$ je svaz s nejmenším prvkem[1] 0 a největším prvkem 1. *Komplement* prvku $x \in X$ je každý prvek y, pro který platí

$$x \vee y = 1, \quad x \wedge y = 0.$$

Jak jsme naznačili výše, představu o pojmu komplement poskytuje svaz podmnožin libovolné množiny A, kde komplementem množiny $B \subset A$ je prostě množinový doplněk $A - B$. (Je totiž jasné, že sjednocením množiny B a jejího doplňku je celá množina A, zatímco jejich průnik je prázdný.)

V tomto případě je komplement určen jednoznačně. Obecně tomu tak být nemusí, ale v případech, o které se budeme zajímat, platí, že komplement libovolného prvku je nejvýše jeden:

Tvrzení 4.2 *Je-li $(X, \preceq)$ distributivní svaz s 0 a 1, potom každý prvek $x \in X$ má nejvýše jeden komplement.*

Důkaz. Nechť $x \in X$ má komplementy y a y'. Podívejme se na prvek

$$p := y \wedge (x \vee y').$$

[1] Podle věty 3.7 má každý *konečný* svaz nejmenší a největší prvek. Protože v kapitole 4 budeme příležitostně hovořit i o nekonečných svazech, zahrnujeme požadavek existence nejmenšího a největšího prvku do této a dalších definic.

Na jednu stranu je $x \vee y' = 1$, a tedy $p = y$. Na druhou stranu z distributivity máme $p = (y \wedge x) \vee (y \wedge y') = 0 \vee (y \wedge y') = y \wedge y'$. Zkrátka a dobře $y = y \wedge y'$, což podle tvrzení 3.2 znamená, že $y \preceq y'$. Zcela symetrickým způsobem ale dostaneme $y' \preceq y$, takže $y = y'$ a důkaz je u konce. □

Svazům s 0 a 1, kde každý prvek má nějaký komplement, se říká *komplementární* svazy.

Definice 4.3 *Booleova*[2] *algebra* je distributivní komplementární svaz s prvky 0 a 1. Používá se také pojmu *Booleův svaz*.

V Booleově algebře má tedy každý prvek x právě jeden komplement, který se značí $\bar{x}$.

U Booleových algeber je rovněž často přijímána konvence, které se přidržíme i my, totiž značit operaci suprema jako + a operaci infima jako · (přičemž tečka se stejně jako u běžného součinu obvykle vynechává). Přepíšeme-li tedy například definici komplementu v tomto novém značení, dostaneme $x + \bar{x} = 1$ a $x\bar{x} = 0$. Zákony distributivity v novém hávu vypadají takto:

- $x(y + z) = (x \cdot y) + (x \cdot z)$,
- $x + (y \cdot z) = (x + y) \cdot (x + z)$.

První z nich vypadá jako 'stará známá' distributivita u číselných operací, prosté roznásobení závorky. Druhá rovnost, která neplatí o nic méně, ale u čísel žádnou obdobu nemá.

Cvičení

► **4.1** Rozhodněte, zda množina $X \subset \mathbf{N}$ spolu s uspořádáním daným dělitelností je (1) svaz, (2) distributivní svaz, (3) komplementární svaz, (4) Booleova algebra.

(a) $X = \{1, 2, 3, 12, 18, 30, 180\}$,

(b) $X = \{1, 2, 4, 6, 7, 10, 60, 420\}$,

(c) $X = \{1, 2, 3, 7, 6, 14, 21, 42\}$,

(d) množina všech dělitelů čísla 90 uspořádaná dělitelností.

►► **4.2** Označme množinu všech dělitelů čísla n, uspořádanou relací dělitelnosti, symbolem $D(n)$. Dokažte, že $D(n)$ je pro libovolné n distributivním svazem (viz také cvičení 3.18). Určete, pro která n je $D(n)$ Booleovou algebrou.

[2] George Boole (1815–1864).

► **4.3** Nechť u, v jsou prvky lineárního prostoru $\mathbf{Z}_2^n$ nad $\mathbf{Z}_2$. Definujme $\min(u, v)$ jako vektor, jehož i-tá souřadnice je rovna minimu z i-tých souřadnic vektorů u a v. Dokažte, že $\mathbf{Z}_2^n$ je Booleova algebra vzhledem k operacím

$$u \wedge v = \min(u, v),$$
$$u \vee v = u + v + \min(u, v).$$

4.2 Booleovské počítání

Věta 4.4 (De Morganovy zákony) *V Booleově algebře A platí pro každou dvojici prvků $x, y \in A$:*

(a) $\overline{x + y} = \bar{x} \cdot \bar{y}$,

(b) $\overline{xy} = \bar{x} + \bar{y}$.

Důkaz. Dokažme část (a), tedy že prvek $\bar{x} \cdot \bar{y}$ je komplementem prvku $x + y$. Nejprve je třeba ukázat, že $(x+y)+(\bar{x}\cdot\bar{y}) = 1$. K tomu použijeme distributivitu. Ta nám říká, že $p := (x + y) + (\bar{x} \cdot \bar{y}) = (x + y + \bar{x}) \cdot (x + y + \bar{y})$. Z definice komplementu ale je $x + \bar{x} = 1$, a tedy i $x + \bar{x} + y = 1$. Podobně i druhá závorka je rovna jedné, takže $p = 1 \cdot 1 = 1$.

Ve druhé polovině důkazu části (a) musíme ukázat, že prvek $q := (x+y)\cdot(\bar{x}\cdot\bar{y})$ je roven nule. Argument je podobný: z distributivity $q = [x \cdot (\bar{x} \cdot \bar{y})] + [y \cdot (\bar{x} \cdot \bar{y})]$, a protože $x\bar{x} = y\bar{y} = 0$, jsou obě hranaté závorky nulové a $q = 0 + 0 = 0$.

Část (b) se dokazuje symetricky. □

Pravidla počítání v Booleových algebrách shrnuje následující věta:

Věta 4.5 *Pro libovolné prvky a, b, c Booleovy algebry B platí:*

(1) $a + a = a$,

(2) $a + b = b + a$ *(komutativita)*,

(3) $a + (b + c) = (a + b) + c$ *(asociativita)*,

(4) $a + (ab) = a$,

(5) $a(b + c) = (ab) + (ac)$ *(distributivita)*,

(6) $a + 0 = a$,

(7) $a \cdot 0 = 0$,

(8) $\bar{1} = 0$,

(9) $a + \bar{a} = 1$,

(10) $\overline{\bar{a}} = a$,

(11) $\overline{a+b} = \bar{a} \cdot \bar{b}$ *(De Morganovy zákony),*

a rovněž ***duální formy*** *všech těchto tvrzení (ve kterých zaměníme symboly* $+$ *a* $\cdot$ *a symboly* 0 *a* 1*).*

Důkaz. Většinu těchto tvrzení jsme již dokázali nebo plynou přímo z definic. Část (10) plyne z toho, že definice komplementu je symetrická: je-li $\bar{x}$ komplementem prvku x, je také x komplementem prvku $\bar{x}$, a tedy $x = \overline{\bar{x}}$. □

Cvičení

► **4.4** Ukažte, že bod (1) věty 4.5 plyne z bodů (2), (3) a (4).

4.3 Booleovy algebry podmnožin

Důležitým příkladem Booleových algeber jsou již zmíněné svazy podmnožin. Víme, že soubor všech podmnožin množiny X (spolu s uspořádáním inkluzí) tvoří svaz. Je to dokonce svaz distributivní (proč?), a na začátku kapitoly jsme zjistili, že je i komplementární. Jedná se tedy o Booleovu algebru. Budeme ji označovat symbolem $\mathbf{2}^X$. (Pro jistotu upozorněme, že se zde nejedná o umocňování čísla 2.) Nulovým prvkem v této Booleově algebře je prázdná množina $\emptyset$, prvek 1 je celá množina X.

Podívejme se pro malá n podrobněji na Booleovu algebru tvořenou všemi podmnožinami nějaké zvolené n-prvkové množiny. Tato algebra má 2^n prvků. Obr. 4.1 ukazuje Hasseovy diagramy Booleových algeber $\mathbf{2}^X$, kde X probíhá množiny $\{a\}$, $\{a,b\}$, $\{a,b,c\}$ a $\{a,b,c,d\}$. Pro větší přehlednost u obrázků 4.1c a 4.1d vynecháváme množinové závorky. Například zápis bcd tak představuje podmnožinu $\{b,c,d\}$, nikoli součin $b \cdot c \cdot d$ (ten je ostatně nulový).

Je-li množina X jednoprvková, pak Booleova algebra $\mathbf{2}^X$ má pouze dva prvky, totiž 0 a 1. Později uvidíme, že tato algebra, kterou budeme značit symbolem $\mathcal{B}_2$, přes svou jednoduchost hraje mezi Booleovými algebrami prominentní úlohu.

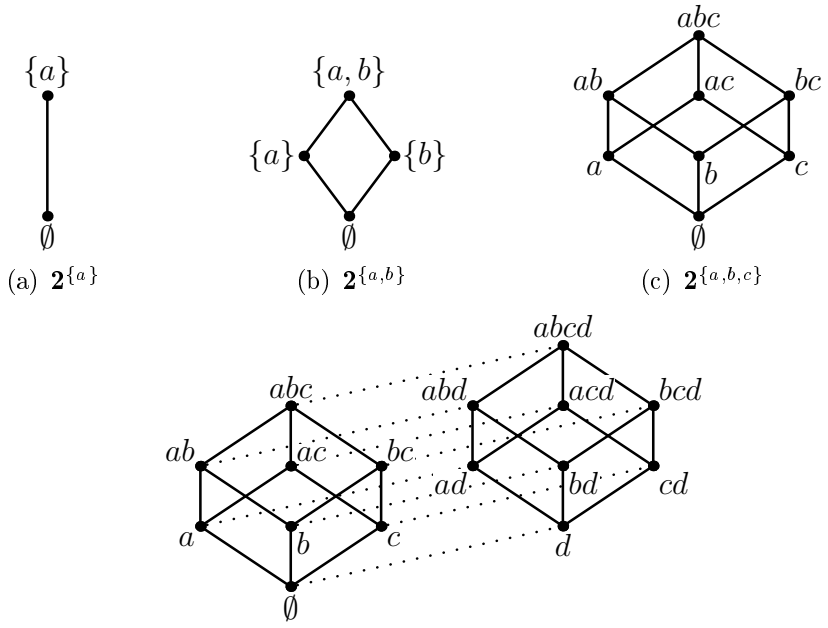
Operace součtu, součinu a komplementu v libovolné Booleově algebře můžeme zapsat tabulkou, podobně jako např. u operací v tělese. Ve zmíněné algebře $\mathcal{B}_2$ je výsledkem tab. 4.1.

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

x	$\bar{x}$
0	1
1	0

Tabulka 4.1: Operace v Booleově algebře $\mathcal{B}_2$: sčítání, násobení a komplement.



(a) $\mathbf{2}^{\{a\}}$ (b) $\mathbf{2}^{\{a,b\}}$ (c) $\mathbf{2}^{\{a,b,c\}}$

(d) $\mathbf{2}^{\{a,b,c,d\}}$

Obrázek 4.1: Čtyři Booleovy algebry tvaru $\mathbf{2}^X$.

Operace ve čtyřprvkové Booleově algebře $\mathbf{2}^{\{a,b\}}$ zachycuje tab. 4.2, kde místo $\{a,b\}$ píšeme 1, místo $\emptyset$ píšeme 0 a u množin $\{a\}$, $\{b\}$ vynecháváme množinové závorky.

$+$	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

$\cdot$	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

x	$\bar{x}$
0	1
a	b
b	a
1	0

Tabulka 4.2: Operace v Booleově algebře $\mathbf{2}^{\{a,b\}}$.

Cvičení

► **4.5** Rozhodněte, zda relace S na množině $\mathbf{2}^{\{a,b,c\}}$ je (1) reflexívní, (2) symetrická, (3) antisymetrická, (4) tranzitivní, (5) ekvivalence, (6) uspořádání:

(a) $x\,S\,y \iff x \subsetneqq y$ (tedy $x \subset y$ a $x \neq y$),

(b) $x\,S\,y \iff x \cap y = \emptyset$,

(c) $x\,S\,y \iff x \cup y = \{a,b,c\}$.

► **4.6** Proč množina $\{0, a, b, 1\}$ spolu s operacemi + a · v tab. 4.2 *netvoří* těleso?

► **4.7** Napište tabulky operací v Booleově algebře $\mathbf{2}^{\{a,b,c\}}$.

► **4.8** Buď $\mathcal{B}$ množina všech podmnožin množiny přirozených čísel $\mathbf{N}$, které jsou konečné nebo mají konečný doplněk v $\mathbf{N}$. Uspořádání na $\mathcal{B}$ je definováno množinovou inkluzí. Ukažte, že $\mathcal{B}$ je Booleova algebra.

4.4 Dva pohledy na Booleovu algebru

Definovali jsme Booleovu algebru jako speciální případ svazu, obecněji uspořádané množiny. Z daného uspořádání na této množině jsme teprve dodatečně odvodili operace součtu, součinu a komplementu (pomocí pojmů supremum a infimum). Znalost samotného uspořádání nám poskytuje úplnou informaci o těchto operacích.

K věci bychom ale mohli přistoupit i z druhé strany a definovat Booleovu algebru přímo jako množinu M s binárními operacemi + a · a unární operací komplement, které splňují určitá pravidla. Inspirováni tvrzením 3.3.2 bychom pak mohli *definovat* uspořádání $\preceq$ na množině M předpisem

$$a \preceq b, \text{ právě když } a \cdot b = a. \tag{4.1}$$

Pokud byly podmínky kladené na naše operace vhodně zvoleny, bude množina M s tímto uspořádáním distributivní komplementární svaz — jinými slovy Booleova algebra podle naší staré definice. Cvičení 4.9 ukazuje, že vhodnými předpoklady jsou například podmínky ve větě 4.5.

Cvičení

► **4.9** Nechť B je množina s binárními operacemi + a ·, s unární operací komplement (která prvku x přiřazuje prvek $\bar{x}$) a s určenými prvky 0 a 1. Dokažte, že pokud pro tyto operace a prvky platí podmínky (1) až (11) věty 4.5, pak množina M spolu s uspořádáním daným předpisem (4.1) je Booleova algebra podle naší dosavadní definice.

4.5 Atomy

Definice 4.6 *Atom* Booleovy algebry $(\mathcal{A}, \preceq)$ je libovolný prvek $a \in \mathcal{A}$ takový, že jediným prvkem $z \in \mathcal{A}$, pro který platí $z \prec a$, je prvek $z = 0$. Množinu všech atomů Booleovy algebry $\mathcal{A}$ značíme $\mathrm{At}(\mathcal{A})$.

Všimněme si, že ekvivalentně by šlo atomy definovat jako prvky, jejichž bezprostředním předchůdcem je prvek 0. Například Booleova algebra $\mathbf{2}^{\{a,b\}}$ má atomy $\{a\}$ a $\{b\}$.

Snadno se nahlédne, že každá *konečná* Booleova algebra obsahuje aspoň jeden atom: platí dokonce následující silnější tvrzení.

Pozorování 4.7 *Pro každý prvek $x \neq 0$ konečné Booleovy algebry $\mathcal{A}$ existuje atom $a \in \mathrm{At}(\mathcal{A})$ takový, že $a \preceq x$.*

Důkaz. Není-li x atom, zvolme nějakého jeho bezprostředního předchůdce $x_1 \neq 0$. Není-li ani x_1 atom, zvolme jeho bezprostředního předchůdce $x_2 \neq 0$. Iterací tohoto postupu musíme po konečném počtu kroků narazit na nějaký atom a, a pro ten jistě platí $a \preceq x$. □

Na druhou stranu existují *nekonečné* Booleovy algebry, které neobsahují ani jeden atom (viz cvičení 4.12).

Cvičení

► **4.10** Které prvky jsou atomy v následujících Booleových algebrách:

(a) v Booleově algebře podmnožin $2^{\{a,b,c\}}$,

(b) obecněji v algebře $\mathbf{2}^X$, kde X je nějaká množina,

(c) ve svazu dělitelů čísla 30?

► **4.11** Určete atomy Booleovy algebry ze cvičení 4.8.

►► **4.12** Uvažujme následující relaci $\sim$ na množině $\mathcal{P}(\mathbf{N})$ všech podmnožin množiny přirozených čísel $\mathbf{N}$:

$$A \sim B, \text{ právě když symetrický rozdíl } A \mathbin{\triangle} B \text{ je konečná množina.}$$

(a) Dokažte, že $\sim$ je ekvivalence.

(b) Označme třídu ekvivalence $\sim$ obsahující prvek A symbolem $[A]$. Definujme na těchto třídách relaci $\preceq$ předpisem

$$[A] \preceq [B], \text{ právě když } A - B \text{ je konečná množina.}$$

Ukažte, že tato definice je *korektní*, tj. že nezáleží na výběru reprezentantů tříd $[A]$ a $[B]$.

(c) Dokažte, že relace $\preceq$ je uspořádání.

(d) Dokažte, že množina tříd ekvivalence $\sim$ s uspořádáním $\preceq$ je Booleova algebra, která nemá žádné atomy. Popište spojení, průsek a komplement v této Booleově algebře.

4.6 Stoneova věta o reprezentaci

Definujme nejprve pojem isomorfismu mezi uspořádanými množinami. Obecně řečeno je isomorfismus bijekce, která zachovává 'vše podstatné'. U uspořádaných množin musí zachovávat uspořádání, zatímco například u grup jde o jednotkový prvek a grupovou operaci (viz cvičení 2.2).

Definice 4.8 *Isomorfismus* uspořádaných množin $(X, \preceq)$ a $(Y, \sqsubseteq)$ je bijekce $f : X \to Y$ taková, že pro každé $a, b \in X$ platí $a \preceq b$ právě když $f(a) \sqsubseteq f(b)$. Tyto uspořádané množiny jsou *isomorfní* (psáno $(X, \preceq) \simeq (Y, \sqsubseteq)$), pokud mezi nimi existuje isomorfismus.

Jak ukazuje cvičení 4.13, isomorfismus dvou Booleových algeber jakožto uspořádaných množin zachovává i všechny dosud uvažované operace (např. supremum).

Definice 4.9 Nechť $B = \{a_1, \ldots, a_k\}$ je konečná množina prvků svazu $(X, \preceq)$ s nejmenším prvkem 0. Je-li $k > 1$, definujme *supremum množiny* B jako

$$\sup B = \Big(\ldots ((a_1 \vee a_2) \vee a_3) \vee \ldots \Big) \vee a_k. \tag{4.2}$$

Dále definujme $\sup \emptyset = 0$, $\sup \{a\} = a$.

Tvrzení 4.10 *Nechť $(X, \preceq)$ je svaz s nejmenším prvkem 0 a $B = \{a_1, \ldots, a_k\} \subset X$. Potom:*

(1) $\sup B$ *je nejmenší horní závora množiny B, tj. nejmenší prvek $x \in X$ s vlastností $a_i \preceq x$ pro každé i,*

(2) ve vzorci (4.2) nezáleží na pořadí prvků $a_1, \ldots, a_k$ ani na jejich uzávorkování (a má tak smysl psát $\sup B = a_1 \vee \cdots \vee a_k$*).*

Důkaz. Cvičení 4.15. □

Stoneova[3] věta o reprezentaci charakterizuje všechny konečné Booleovy algebry.

Věta 4.11 (Stoneova věta) *Každá* konečná *Booleova algebra $(\mathcal{A}, \preceq)$ je isomorfní s Booleovou algebrou $(\mathbf{2}^{\mathrm{At}(\mathcal{A})}, \subset)$.*

Důkaz. Zkonstruujeme isomorfismus mezi uspořádanými množinami $(\mathcal{A}, \preceq)$ a $(\mathbf{2}^{\mathrm{At}(\mathcal{A})}, \subset)$. Konkrétně pro $x \in \mathcal{A}$ nechť

$$x^* = \{a \in \mathrm{At}(\mathcal{A}) : a \preceq x\}.$$

[3] Marshall Harvey Stone (1903–1989).

Zobrazení $x \mapsto x^*$ přiřazuje každému prvku $x \in \mathcal{A}$ množinu atomů algebry $\mathcal{A}$. Potřebujeme ukázat, že se jedná o bijekci mezi $\mathcal{A}$ a $\mathbf{2}^{\mathrm{At}(\mathcal{A})}$ a že platí $x \preceq y$, právě když $x^* \subset y^*$. Důkaz rozdělíme do čtyř částí.

(1) Pokud $x \preceq y$, pak $x^* \subset y^*$.

Toto je nejlehčí část důkazu. Pro každé $a \in x^*$ platí $a \preceq x \preceq y$ a z tranzitivity je $a \in y^*$. Jinak řečeno, $x^* \subset y^*$.

(2) Pokud $x^* \subset y^*$, pak $x \preceq y$.

Nechť naopak $x \not\preceq y$. Podle tvrzení 3.2 musí být $xy \neq x$. Všimněme si, že

$$x = x \cdot 1 = x(y + \bar{y}) = xy + x\bar{y},$$

z čehož plyne, že $x\bar{y} \neq 0$. Najděme podle pozorování 4.7 atom $a \preceq x\bar{y}$. Z definice infima je $a \preceq x$ a tedy $a \in x^*$. Dále je $a \preceq \bar{y}$ a tím pádem nemůže být $a \preceq y$, protože bychom dostali $a \preceq y\bar{y} = 0$; a je však atom. Takže $a \notin y^*$. Atom a tedy dosvědčuje, že x^* není podmnožinou y^*. Tím je požadovaná implikace dokázána.

(3) Zobrazení $x \mapsto x^*$ je prosté.

Vezměme $x \neq y \in \mathcal{A}$. Z antisymetrie musí být buď $x \not\preceq y$ nebo $y \not\preceq x$; nechť platí první varianta. Podle obměny implikace v bodu (2) dostáváme, že x^* není podmnožinou y^*. Speciálně $x^* \neq y^*$ a tvrzení je dokázáno.

(4) Zobrazení $x \mapsto x^*$ je na.

Hledáme vzor libovolné množiny atomů $B = \{a_1, \ldots, a_k\} \subset \mathrm{At}(\mathcal{A})$, tedy takové $b \in \mathcal{A}$, že $b^* = B$. Dokážeme, že tuto vlastnost má prvek $b = \sup B$.

Pro každý atom $a_i \in B$ jistě platí, že $a_i \preceq b$. Otázkou je, zda tato nerovnost může platit i pro nějaký atom $c \notin B$. Dejme tomu, že ano, tedy $c \preceq b$. Rozepišme $\sup B$ s použitím symbolu $+$ a zjištění, že na závorkách nezáleží a můžeme je vynechat:

$$c \cdot b = c \cdot (a_1 + \cdots + a_k) = ca_1 + \cdots + ca_k = 0 + \cdots + 0 = 0,$$

přičemž předposlední rovnost vychází z faktu, že infimum dvou různých atomů je nutně 0. Dokázali jsme, že $c \cdot b \neq c$, a tedy $c \notin b^*$. Z toho již plyne, že $b^* = B$. Důkaz věty je proveden. □

Důsledek 4.12 *Počet prvků konečné Booleovy algebry $\mathcal{A}$ je vždy mocnina čísla 2, konkrétně 2^m, kde $m = |\mathrm{At}(\mathcal{A})|$.* □

Důsledek 4.13 *Dvě konečné Booleovy algebry se stejným počtem prvků jsou isomorfní.*

Důkaz. Nechť $\mathcal{A}, \mathcal{B}$ jsou Booleovy algebry (s uspořádáním, které nebudeme výslovně zmiňovat) a $|\mathcal{A}| = |\mathcal{B}| = n$. Víme, že $\mathcal{A} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{A})}$ a $\mathcal{B} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{B})}$, kde uvažované algebry podmnožin jsou uspořádány inkluzí. Ovšem množiny $\mathrm{At}(\mathcal{A})$ a $\mathrm{At}(\mathcal{B})$ jsou stejně velké (jejich velikost je $\log_2 n$), takže můžeme zvolit nějakou

bijekci $g : \mathrm{At}(\mathcal{A}) \to \mathrm{At}(\mathcal{B})$. Tato bijekce podle cvičení 4.16 indukuje isomorfismus $\mathbf{2}^g$ mezi Booleovými algebrami $\mathbf{2}^{\mathrm{At}(\mathcal{A})}$ a $\mathbf{2}^{\mathrm{At}(\mathcal{B})}$. Celkem vzato dostáváme

$$\mathcal{A} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{A})} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{B})} \simeq \mathcal{B}$$

a složením těchto tří isomorfismů je isomorfismus mezi $\mathcal{A}$ a $\mathcal{B}$. □

Cvičení

► **4.13** Ukažte, že jsou-li dvě Booleovy algebry isomorfní (jako uspořádané množiny), pak příslušný isomorfismus zachovává i operace suprema, infima a komplementu, tedy například

$$f(x + y) = f(x) + f(y)$$

(kde se ovšem symbol + na každé straně rovnice vztahuje k jiné Booleově algebře!)

► **4.14** Nechť $\mathcal{B}$ a $\mathcal{C}$ jsou Booleovy algebry. Ukažte, že bijekce $f : \mathcal{B} \to \mathcal{C}$ splňující $f(x + y) = f(x) + f(y)$ a $f(\bar{x}) = \overline{f(x)}$ pro všechna $x, y \in \mathcal{B}$ je isomorfismus Booleových algeber.

► **4.15** Dokažte tvrzení 4.10.

► **4.16** Nechť $g : Y \to Z$ je bijekce mezi konečnými množinami. Zobrazení g indukuje zobrazení $\mathbf{2}^g : \mathbf{2}^Y \to \mathbf{2}^Z$, dané předpisem

$$\mathbf{2}^g(A) = \{g(a) : a \in A\}$$

pro libovolné $A \subset Y$. Ukažte, že $\mathbf{2}^g$ je isomorfismus Booleových algeber $(\mathbf{2}^Y, \subset)$ a $(\mathbf{2}^Z, \subset)$.

► **4.17** Ukažte, že jsou-li $g : X_1 \to X_2$ a $h : X_2 \to X_3$ isomorfismy uspořádaných množin $(X_1, \preceq_1)$ a $(X_2, \preceq_2)$, resp. $(X_2, \preceq_2)$ a $(X_3, \preceq_3)$, potom složení $g \circ h : X_1 \to X_3$ je isomorfismem uspořádaných množin $(X_1, \preceq_1)$ a $(X_3, \preceq_3)$.

► **4.18** (a) Najděte všechny navzájem neisomorfní uspořádané množiny o 3 prvcích.

(b) Dokažte, že stejně velké konečné lineárně uspořádané množiny jsou isomorfní.

(c) Najděte dvě neisomorfní lineární uspořádání množiny všech přirozených čísel.

4.7 Direktní součin

Důsledkem Stoneovy věty je, že Booleovy algebry podmnožin jsou vlastně (až na isomorfismus) jedinými představiteli konečných Booleových algeber. Uvidíme, že s pomocí následujícího pojmu lze tento fakt vyjádřit v ještě minimalističtější podobě.

Definice 4.14 *Direktní součin* Booleových algeber $(\mathcal{A}_1, \preceq_1)$ a $(\mathcal{A}_2, \preceq_2)$ je kartézský součin $\mathcal{A}_1 \times \mathcal{A}_2$ s uspořádáním $\leq$ definovaným 'po složkách':

$$(b_1, b_2) \leq (c_1, c_2), \text{ pokud } b_1 \preceq_1 c_1 \text{ a } b_2 \preceq_2 c_2,$$

kde (b_1, b_2) a (c_1, c_2) jsou prvky součinu $\mathcal{A}_1 \times \mathcal{A}_2$. Je-li $\mathcal{A}_1 = \mathcal{A}_2$, mluvíme také o *direktní mocnině* Booleovy algebry $\mathcal{A}_1$.

Direktní součin Booleových algeber je sám Booleovou algebrou. Abychom toto tvrzení dokázali, musíme z definic ověřit, že je to komplementární distributivní svaz. Především je snadné si všimnout, že v součinu $\mathcal{A}_1 \times \mathcal{A}_2$ existují suprema: supremem dvojic (b_1, b_2) a (c_1, c_2) je dvojice $(b_1 \vee c_1, b_2 \vee c_2)$. (Dokažte.) Podobně je tomu s infimy, takže $\mathcal{A}_1 \times \mathcal{A}_2$ je svaz. Má prvek 0, jehož složky jsou nulové prvky v $\mathcal{A}_1$ resp. $\mathcal{A}_2$, a podobně definovaný prvek 1. Distributivita a komplementárnost plynou z faktu, že tyto vlastnosti mají algebry $\mathcal{A}_1$ resp. $\mathcal{A}_2$. Podrobný důkaz necháváme na cvičení 4.19.

Příklad 4.15 Uvažme dvouprvkovou Booleovu algebru $\mathcal{B}_2 = \{0, 1\}$ z obr. 4.1(a). Direktní mocnina $\mathcal{B}_2^2$ sestává ze všech dvojic prvků 0 a 1. Má tedy 4 prvky, které lze psát jako 00, 01, 10 a 11. Obecně n-tou direktní mocninu $\mathcal{B}_2^n$ Booleovy algebry $\mathcal{B}_2$ lze ztotožnit s množinou všech slov, tvořených n-ticí symbolů 0 a 1. Tato slova jsou uspořádána 'po složkách', tj. $(a_1 a_2 \ldots a_n) \leq (b_1 b_2 \ldots b_n)$, pokud $a_i \preceq b_i$ pro každé i.

Tvrzení 4.16 *Je-li X n-prvková množina, pak $\mathbf{2}^X \simeq \mathcal{B}_2^n$.*

Důkaz. Bez újmy na obecnosti (díky cvičení 4.16) můžeme předpokládat, že $X = \{1, \ldots, n\}$. Pro $i \in X$ uvažme 'slovo' $w_i = (0 \ldots 010 \ldots 0)$ s jedničkou právě na i-tém místě. Isomorfismus $f : \mathbf{2}^X \to \mathcal{B}_2^n$ je pak dán předpisem

$$f(Y) = \sum_{i \in Y} w_i,$$

kde $Y \in \mathbf{2}^X$ a symbol $\sum$ označuje sčítání v Booleově algebře $\mathcal{B}_2^n$. Je snadné nahlédnout, že f je opravdu isomorfismus. □

Důsledek 4.17 *Každá konečná Booleova algebra je isomorfní s Booleovou algebrou $\mathcal{B}_2^n$ pro nějaké n.*

Důkaz. Plyne přímo ze Stoneovy věty a tvrzení 4.16. □

Cvičení

▶ **4.19** Ukažte podrobně, že direktní součin Booleových algeber je Booleova algebra. Jaké jsou její atomy?

▶ **4.20** Určete hodnoty operací $+$, $\cdot$ a komplement v Booleově algebře $\mathcal{B}_2^2$. Výsledek porovnejte s tabulkou 4.2.

4.8 Booleovské funkce

Definice 4.18 *Booleovská funkce n proměnných* je libovolná funkce $f : \mathcal{B}_2^n \to \mathcal{B}_2$.

Příkladem booleovské funkce 2 proměnných je funkce $+$, kterou už známe. Její hodnoty ukazuje první část tab. 4.1.

Obvyklejší tvar tabulky má jeden řádek pro každou kombinaci hodnot proměnných, jako v tab. 4.3, která ukazuje kromě funkce $+$ i funkce $\cdot$ a komplement. Jedná se o tzv. *pravdivostní tabulky.*

x	y	$x+y$
0	0	0
0	1	1
1	0	1
1	1	1

x	y	$x\cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

x	$\bar{x}$
0	1
1	0

Tabulka 4.3: Hodnoty booleovských funkcí $+$, $\cdot$ a komplement.

Tvrzení 4.19 *Množina F_n všech booleovských funkcí n proměnných s uspořádáním $\leq$ daným předpisem*

$$f \leq g, \text{ pokud pro každé } x \in \mathcal{B}_2^n \text{ platí } f(x) \preceq g(x),$$

je Booleova algebra.

Důkaz. Cvičení 4.23. □

Základní booleovské funkce je možné kombinovat do funkcí složitějších (třeba $x\bar{y} + \bar{x}y$). To je idea *booleovských polynomů*, definovaných následujícím rekurentním způsobem.

Definice 4.20 (1) Výrazy $0, 1$ a x_i (pro libovolné $i = 1, \ldots, n$) jsou booleovské polynomy v proměnných $x_1, \ldots, x_n$.

(2) Jsou-li f a g booleovské polynomy v proměnných $x_1, \ldots, x_n$, pak výrazy $(f+g), (f \cdot g)$ a $\bar{g}$ rovněž.

(3) Dva booleovské polynomy v proměnných $x_1, \ldots, x_n$ jsou si rovny, pokud určují stejnou booleovskou funkci.

Příklad 4.21 Výraz $x \oplus y := \bar{x}y + x\bar{y}$ (tzv. *symetrický rozdíl x a y*) je booleovský polynom v proměnných x, y. Platí ovšem také $x \oplus y = (x+y)(\bar{x}+\bar{y})$. Můžeme se o tom přesvědčit pravdivostní tabulkou (tab. 4.4).

Další možností je přímý výpočet podle booleovských zásad. Z distributivity totiž máme

$$\begin{aligned}(x+y)(\bar{x}+\bar{y}) &= x\bar{x} + x\bar{y} + y\bar{x} + y\bar{y} \\ &= 0 + x\bar{y} + y\bar{x} + 0 \\ &= \bar{x}y + x\bar{y}. \quad \square\end{aligned}$$

Dalším důležitým příkladem booleovského polynomu je *implikace* $x \to y$, definovaná vztahem $x \to y := \bar{x} + y$.

x	y	$x \oplus y$	$(x+y)(\bar{x}+\bar{y})$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

Tabulka 4.4: Booleovské polynomy se stejnou pravdivostní tabulkou.

Cvičení

► **4.21** Sestrojte pravdivostní tabulky booleovských funkcí, které jsou určeny následujícími polynomy v proměnných x a y:

(a) $x \to y$,

(b) $y + x\bar{y}$.

► **4.22** Je výraz $x_2 + x_2 + x_2$ booleovským polynomem v proměnných $x_1, \ldots, x_5$? Je roven booleovskému polynomu x_2?

► **4.23** Dokažte tvrzení 4.19. Popište suprema, infima a komplementy v Booleově algebře F_n.

► **4.24** Kolik prvků má množina F_2 všech Booleovských funkcí dvou proměnných? Kolik množina F_n?

► **4.25** Nechť $|$ je *Shefferova*[4] *funkce* $\mathcal{B}_2^2 \to \mathcal{B}_2$ definovaná tabulkou

x	y	$x \mid y$
0	0	1
0	1	1
1	0	1
1	1	0

Ukažte, že pomocí Shefferovy funkce je možné vyjádřit komplement, spojení a průsek.

4.9 Součtový a součinový tvar

Definice 4.22 *Literál* v proměnných $x_1, \ldots, x_n$ je libovolný booleovský polynom ve tvaru x_i nebo $\bar{x}_i$, kde $i = 1, \ldots, n$. *Součinová klauzule* je booleovský polynom, který je součinem konečně mnoha literálů. Booleovský polynom p je v *součtovém tvaru*[5], je-li součtem součinových klauzulí. Duální pojmy (součtová klauzule, součinový tvar) jsou definovány následujícím přirozeným způsobem. *Součtová klauzule* je booleovský polynom, který je součtem konečně mnoha literálů. Polynom p je v *součinovém tvaru*, pokud součinem součtových klauzulí.

Příklad 4.23 Polynom $x_1x_2 + x_1\bar{x}_3$ je zapsán v součtovém, nikoli však součinovém tvaru. Polynom $x_1(x_2 + \bar{x}_3)$, který je mu roven, je zapsán v součinovém tvaru. Polynom $x_1(x_2 + \bar{x}_3) + x_1x_2$ není ani v jednom z těchto tvarů.

Naskýtá se otázka, zda každou booleovskou funkci je možné vyjádřit booleovským polynomem v součtovém tvaru. Uvidíme, že platí mnohem víc.

Definice 4.24 Booleovský polynom p v proměnných $x_1, \ldots, x_n$ je v *úplném součtovém tvaru*, jestliže je v součtovém tvaru a každý ze sčítanců (součinových klauzulí) obsahuje pro každé $i = 1, \ldots, n$ buďto literál x_i nebo literál $\bar{x}_i$ (ne však oba). Symetricky: p je v *úplném součinovém tvaru*, jestliže je v součinovém tvaru a každý z činitelů (součtových klauzulí) obsahuje pro každé $i = 1, \ldots, n$ literál x_i nebo $\bar{x}_i$.

Příklad 4.25 Polynom $\bar{x}y + x\bar{y}$ v proměnných x, y je zapsán v úplném součtovém tvaru. Jeho alternativní zápis, $(x + y)(\bar{x} + \bar{y})$, je v úplném součinovém tvaru.

[4] Henry Maurice Sheffer (1882–1964).

[5] Místo 'součtový tvar' se také používá o něco odtažitější termín *disjunktivní normální forma* (DNF); místo 'součinový tvar' pak *konjunktivní normální forma* (KNF).

Věta 4.26 *Každou nekonstantní booleovskou funkci n proměnných lze zapsat booleovským polynomem n proměnných v úplném součtovém (úplném součinovém) tvaru.*

Důkaz. Dokážeme nejprve část o úplném součtovém tvaru. Uvažme libovolné $a = (a_1, \ldots, a_n) \in \mathcal{B}_2^n$. Definujme součinovou klauzuli p_a jako součin literálů x_i přes všechna i taková, že $a_i = 1$, a literálů $\bar{x}_i$ přes všechna i taková, že $a_i = 0$. Každé p_a je tedy booleovský polynom v úplném součtovém tvaru, který je navíc nenulový jen pro jediné $z \in \mathcal{B}_2^n$ (totiž $z = a$).

Mějme nyní booleovskou funkci f, kterou chceme reprezentovat booleovským polynomem v úplném součtovém tvaru, a nechť $A \subset \mathcal{B}_2^n$ je množina všech $z \in \mathcal{B}_2^n$, pro něž je $f(z) = 1$. Položíme-li

$$p_f = \sum_{a \in A} p_a,$$

pak p_f je booleovský polynom v úplném součtovém tvaru a očividně nabývá stejných hodnot jako funkce f. Vzhledem k tomu, že f není konstantní nulová funkce, není součet v definici polynomu p_f prázdný.

Pokud jde o vyjádření v úplném součinovém tvaru, stačí vyjádřit (nekonstantní) funkci $\bar{f}$ polynomem $p_{\bar{f}}$ v úplném součtovém tvaru a upravit komplement $\overline{p_{\bar{f}}}$ podle de Morganova pravidla do součinového tvaru. □

Jednoduchým důsledkem věty 4.26 je odpověď na výše položenou otázku: každá booleovská funkce má vyjádření ve tvaru polynomu v součtovém tvaru (nepožadujeme-li úplný součtový tvar, platí toto tvrzení i pro konstantní funkce).

Příklad 4.27 Vyjádříme v úplném součtovém a součinovém tvaru booleovskou funkci f v proměnných x, y, z, zadanou pravdivostní tabulkou 4.5.

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	0
0	**1**	**0**	**1**
0	**1**	**1**	**1**
1	0	0	0
1	0	1	0
1	**1**	**0**	**1**
1	1	1	0

Tabulka 4.5: Pravdivostní tabulka funkce f.

Řádky tabulky, které v důkazu věty 4.26 odpovídají množině A, jsou znázorněny tučně. První z nich např. odpovídá prvku $(010) \in \mathcal{B}_2^3$, takže příslušná

klauzule $p_{(010)}$ je $\bar{x}y\bar{z}$. (Ověřte, že $\bar{x}y\bar{z}$ nabývá nenulové hodnoty právě pro tento jediný prvek.) Podobnými členy přispějí i zbylé dva tučné řádky, takže vyjádření funkce f v úplném součtovém tvaru je

$$p_f = \bar{x}y\bar{z} + \bar{x}yz + xy\bar{z}.$$

Vyjádříme f ještě v úplném součinovém tvaru. Funkce $\bar{f}$ má hodnotu 1 všude tam, kde f má hodnotu 0. Snadno tedy vidíme, že

$$p_{\bar{f}} = \bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + x\bar{y}\bar{z} + x\bar{y}z + xyz.$$

(Každá z pěti klauzulí zde odpovídá jednomu netučnému řádku.) Nás ale zajímá součinový tvar pro funkci f. Vezmeme tedy komplement $\overline{p_{\bar{f}}}$:

$$\begin{aligned}\overline{p_{\bar{f}}} &= \overline{\bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + x\bar{y}\bar{z} + x\bar{y}z + xyz} \\ &= \overline{\bar{x}\bar{y}\bar{z}} \cdot \overline{\bar{x}\bar{y}z} \cdot \overline{x\bar{y}\bar{z}} \cdot \overline{x\bar{y}z} \cdot \overline{xyz} \\ &= (x+y+z)(x+y+\bar{z})(\bar{x}+y+z)(\bar{x}+y+\bar{z})(\bar{x}+\bar{y}+\bar{z}).\end{aligned}$$

Příklad 4.28 Upravíme do úplného součtového tvaru polynom

$$f(x,y) = (\overline{(\bar{x}y)} \cdot \bar{x}) + y.$$

Mohli bychom sestrojit tabulku a postupovat stejně jako v minulém příkladu, ale ukážeme řešení s využitím booleovského počítání.

Nejprve se zbavíme komplementu v první závorce:

$$\begin{aligned}f(x,y) = (\overline{(\overline{x}} + \bar{y}) \cdot \bar{x}) + y &= (x+\bar{y})\bar{x} + y \\ &= x\bar{x} + \bar{y}\bar{x} + y = \bar{x}\bar{y} + y.\end{aligned}$$

Výsledný polynom je sice v součtovém tvaru, ne však v úplném součtovém tvaru, protože druhá klauzule neobsahuje žádný literál proměnné x. Použijeme trik: vynásobíme tuto klauzuli výrazem $x + \bar{x} = 1$ a upravíme. Hodnoty funkce se tím nezmění.

$$f(x,y) = \bar{x}\bar{y} + y = \bar{x}\bar{y} + y(x+\bar{x}) = \bar{x}\bar{y} + xy + \bar{x}y,$$

a to je také hledané vyjádření polynomu f v úplném součtovém tvaru.

Cvičení

► **4.26** Rozhodněte, zda jsou následující booleovské polynomy v součtovém resp. součinovém tvaru:

(a) $x_1x_2 + \overline{x_3x_4}$,

(b) $x_1(x_1 + \bar{x_1})$,

(c) $x_1 + x_2$,

(d) $x_1\overline{x_2}x_3\overline{x_4}$.

▶ **4.27** Vyjádřete booleovské funkce $f(x, y, z)$ a $g(x, y, z)$ polynomem (a) v úplném součtovém a (b) v úplném součinovém tvaru.

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

x	y	z	$g(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

▶ **4.28** Najděte 2 různá vyjádření v součtovém tvaru pro booleovský polynom $x(\overline{y + z})$.

▶ **4.29** Platí věta 4.26 i pro *konstantní* booleovské funkce? Lze funkci s konstantní hodnotou 1 (v n proměnných) zapsat v úplném součtovém tvaru?

▶ **4.30** Převeďte do úplného součtového a úplného součinového tvaru následující booleovské polynomy v proměnných x, y, z:

(a) $x \to (y \to x)$,

(b) $x \oplus (y \to z)$,

(c) $\overline{y(x + \bar{y}z)}$,

(d) $((\bar{x}y) \oplus z)((xz) \to y)$.

▶ **4.31** Převeďte booleovské polynomy do úplného součinového tvaru, a to (i) pomocí booleovského kalkulu, (ii) pomocí tabulky:

(a) $x \to ((y + \bar{x}z) \oplus \bar{z})$,

(b) $((x\bar{y}) \oplus (y\bar{z})) \oplus (z\bar{x})$.

▶ **4.32** Kolik je Booleovských funkcí n proměnných, jejichž úplný součinový tvar je zároveň tvarem součtovým?

▶▶ **4.33** Dokažte, že pro každou Booleovskou funkci je zápis v *úplném* součtovém tvaru jednoznačný.

Kapitola 5

Grafy

Touto kapitolou začíná druhá část našeho textu, která je věnována teorii grafů. Seznámíme se v ní s některými základními grafovými pojmy.

5.1 Definice

Definice 5.1 *Graf* G je dvojice $G = (V, E)$, kde V je konečná množina a $E \subset \binom{V}{2}$, přičemž

$$\binom{V}{2} = \{\{x, y\} : x, y \in V \text{ a } x \neq y\}$$

je množina všech dvouprvkových množin (*neuspořádaných dvojic*) prvků množiny V. Prvky množiny[1] V nazýváme *vrcholy* (často také *uzly*), prvky množiny E pak *hrany* grafu G. Vrcholy $x, y \in V$ jsou *sousední*, pokud $\{x, y\} \in E$.

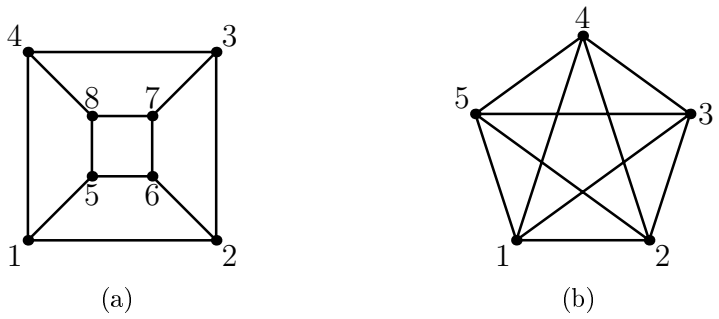
V obvyklém znázornění grafu jsou vrcholy zastoupeny body v rovině a každá hrana $\{x, y\}$ čarou spojující příslušnou dvojici bodů jako na obr. 5.1.

Potřebujeme-li se odkázat na množinu vrcholů resp. hran nějakého grafu G, použijeme zápis $V(G)$ resp. $E(G)$.

Všimněme si, že naše definice grafu neumožňuje, aby mezi dvěma vrcholy vedla více než jedna hrana (tzv. *násobné hrany*). Nepovoluje také tzv. *smyčky*, tj. hrany, které spojují vrchol se sebou samým. V některých situacích je vhodnější uvažovat grafy, které násobné hrany nebo smyčky mají. My se však zatím přidržíme naší jednoduché definice.

Další důležité zjištění je, že naše grafy jsou *neorientované*, jejich hrany nemají směr, protože jsou definovány jako *neuspořádané* dvojice vrcholů. Někdy budeme pro jednoduchost zapisovat hranu $\{x, y\}$ prostě jako xy; je ale třeba mít na paměti, že v neorientovaném grafu není rozdíl mezi hranami xy a yx.

[1] Ustálené označení V, E pochází z anglické terminologie: anglický termín pro vrchol je *vertex*, pro hranu *edge*.



Obrázek 5.1: Příklady grafů.

Budeme také uvažovat především o *konečných* grafech, tedy takových, jejichž množina vrcholů je konečná. (Musí pak být konečná i množina hran?)

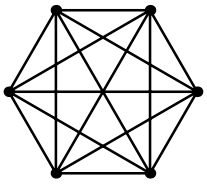
Pojem neorientovaného grafu je velice blízko pojmu symetrické relace. Je-li R antireflexívní[2] symetrická relace na množině X, pak jí lze přiřadit neorientovaný graf G s množinou vrcholů $V(G) = X$, ve kterém prvky $x, y \in X$ jsou spojeny hranou (tedy $\{x, y\} \in E(G)$), pokud $x\,R\,y$. Tato korespondence platí i opačně. Lze dokonce i odstranit požadavek antireflexivity, pokud ovšem v grafu G povolíme smyčky.

5.2 Některé základní grafy

Ukážeme si příklady grafů, které jsou natolik důležité, že si zasloužily vlastní jména a označení. Nechť n je přirozené číslo a označme $[n] = \{1, \ldots, n\}$. Všechny dále definované grafy mají množinu vrcholů $[n]$.

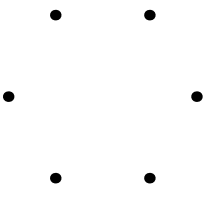
Úplný graf na n vrcholech (značí se K_n) obsahuje jako hrany všechny neuspořádané dvojice prvků $[n]$, takže

$$V(K_n) = [n],$$
$$E(K_n) = \binom{[n]}{2}.$$

K_6 

Diskrétní graf D_n na n vrcholech nemá žádné hrany:

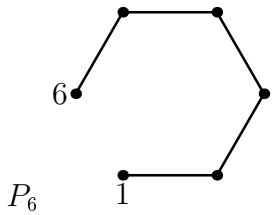
$$V(D_n) = [n],$$
$$E(D_n) = \emptyset.$$

D_6 

[2]Relace R je *antireflexívní*, pokud pro žádné x neplatí $x\,R\,x$.

Cesta P_n na n vrcholech je definována takto:

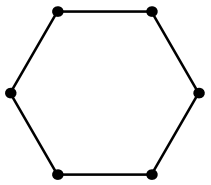
$$V(P_n) = [n],$$
$$E(P_n) = \{\{i, i+1\} : 1 \leq i < n\}.$$



P_6

Kružnice C_n na $n \geq 3$ vrcholech vznikne přidáním jedné hrany:

$$V(C_n) = [n],$$
$$E(C_n) = E(P_n) \cup \{\{1, n\}\}.$$


C_6

5.3 Isomorfismus a podgrafy

Podívejme se na dvojici grafů G, H, znázorněných na obr. 5.2. Jsou to rozhodně různé grafy. Nejde ani tak o to, že se liší způsob nakreslení — každý graf lze nakreslit mnoha způsoby, a nezáleží na tom, zda jsou čáry představující hrany rovné či zda se třeba kříží.

Grafy G, H jsou nicméně různé už proto, že mají různé množiny vrcholů

$$V(G) = \{1, 2, 3, 4, 5\} \quad \text{a} \quad V(H) = \{a, b, c, d, e\}.$$

Nemůže tedy jít o *totožné* grafy.

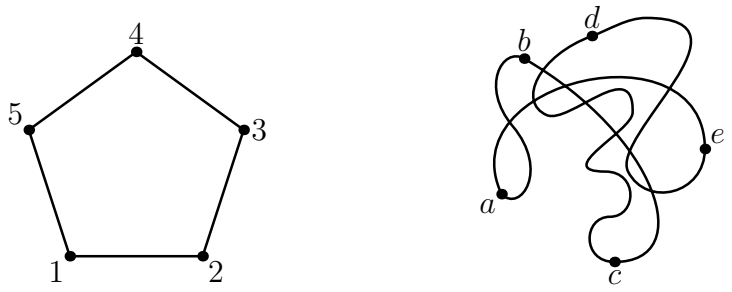
Je to ale jediný rozdíl? Jinými slovy, bylo by možné vrcholy grafu H 'přeznačit' tak, abychom dostali přesně graf G? Tato otázka směřuje k pojmu isomorfismu grafů. Čtenáře, který zná definici isomorfismu grup (kap. 2) nebo uspořádaných množin (kap. 4) by definice pro grafy neměla překvapit.

Definice 5.2 *Isomorfismus* grafů G a H je bijekce $f : V(G) \to V(H)$, pro kterou platí, že dvojice $\{x, y\}$ je hranou grafu G, právě když dvojice $\{f(x), f(y)\}$ je hranou grafu H. Grafy G, H, mezi kterými existuje isomorfismus, jsou *isomorfní* (psáno $G \simeq H$).

Grafy na obr. 5.2 isomorfní jsou: stačí uvážit bijekci, která prvky $1, 2, 3, 4, 5$ zobrazí po řadě na prvky a, b, c, d, e. (Ověřte podmínku v definici isomorfismu.) Tyto grafy ovšem nejsou isomorfní s žádným z grafů na obr. 5.1.

Následující definice popisuje situaci, kdy je jeden graf 'obsažen' v grafu jiném.

Definice 5.3 Graf H je *podgrafem* grafu G (psáno $H \subset G$), pokud $V(H) \subset V(G)$ a $E(H) \subset E(G)$.



(a) (b)

Obrázek 5.2: Různé, ale isomorfní grafy.

Silnější variantou pojmu podgrafu je pojem indukovaného podgrafu, u kterého vyžadujeme, aby obsahoval všechny hrany, které ve 'větším' grafu na dané množině vrcholů existují:

Definice 5.4 Graf H je *indukovaným podgrafem* grafu G, pokud $V(H) \subset V(G)$ a $E(H) = E(G) \cap \binom{V(H)}{2}$. Každá množina $X \subset V(G)$ tedy určuje právě jeden indukovaný podgraf H grafu G takový, že $V(H) = X$. Tomuto podgrafu říkáme *indukovaný podgraf na množině* X.

Graf na obr. 5.2a je například podgrafem grafu na obr. 5.1b, ale není jeho indukovaným podgrafem.

Cvičení

► **5.1** Dokažte, že konečné grafy s různým počtem vrcholů nemohou být isomorfní.

► **5.2** Dokažte, že relace 'býti isomorfní' na množině všech konečných grafů je ekvivalence.

► **5.3** Najděte isomorfismus mezi grafy na obr. 5.3. (Poznamenejme, že graf, který je s nimi isomorfní, se obvykle označuje symbolem $K_{3,3}$.)

► **5.4** Kolik hran mají grafy K_n, D_n, P_n a C_n?

►► **5.5** Buď G neorientovaný graf (bez smyček a násobných hran) na 6 vrcholech. Dokažte, že G obsahuje množinu U tří vrcholů takovou, že indukovaný podgraf na U je diskrétní nebo úplný graf. (Jde o velmi speciální případ slavné *Ramseyovy věty*.)

Obrázek 5.3: Dva isomorfní grafy.

5.4 Stupně

Definice 5.5 *Stupeň* vrcholu v grafu G je počet hran grafu G, které obsahují vrchol v. Značí se $d_G(v)$.

V grafu G_1 na obr. 5.1a je například $d_{G_1}(v) = 3$ pro každý vrchol v.

Pozorování 5.6 *V grafu o n vrcholech je stupeň každého vrcholu nejvýše $n-1$.*

Následující zajímavá věta říká, že žádný graf nemůže mít lichý počet vrcholů lichého stupně. V angličtině se jí někdy říká *Handshaking lemma*, lemma o podání ruky, protože ji můžeme parafrázovat následovně. Dejme tomu, že na nějaké oslavě se hosté navzájem vítají podáním ruky, ne však nutně každý s každým (třeba proto, že se všichni neznají). Pak počet lidí, kteří si potřesou rukou s lichým počtem osob, bude za všech okolností sudý.

Věta 5.7 *Počet vrcholů lichého stupně je v každém grafu sudý.*

Důkaz. Nechť S je součet stupňů všech vrcholů v grafu G:

$$S = \sum_{v \in V(G)} d_G(v).$$

Každá dvojice (v, e), kde e je hrana obsahující vrchol v, k číslu S přispěje jedničkou. Každá hrana má ovšem dva konce a přispívá tak právě dvakrát. Jinak řečeno,

$$S = 2m,$$

kde m je počet hran grafu G. Číslo S je tedy sudé a z toho už plyne tvrzení věty. □

Cvičení

▶ **5.6** Určete stupně vrcholů v grafech K_n, D_n, P_n a C_n.

5.5 Soubor stupňů

Nechť G je graf (i nadále bez smyček a násobných hran). *Soubor stupňů* nebo také *skóre* grafu G je posloupnost čísel, kterou získáme, když seřadíme stupně všech vrcholů v grafu G od největšího k nejmenšímu. Například skóre grafu na obr. 7.1(a) je $(3, 1, 1, 1)$ a graf na obr. 7.1(b) má skóre $(2, 2, 2, 1, 1)$.

Budeme se zabývat především otázkou, které nerostoucí posloupnosti čísel jsou *grafové*, tj. mají tu vlastnost, že jsou souborem stupňů nějakého grafu. Je totiž jasné, že některé nerostoucí posloupnosti čísel grafové nejsou, třeba $(6, 6, 6)$ nebo $(2, 3)$. Na druhou stranu, jak ukazuje cvičení 5.8, jedné grafové posloupnosti může obecně odpovídat několik neisomorfních grafů.

Při letmém pohledu na cvičení 5.10 se ukazuje, že zodpovězení této otázky metodou pokusu a omylu může být náročný úkol (zkuste to!). Účinným nástrojem je však následující věta.

Věta 5.8 *Nechť* $\mathbf{d} = (d_1, \ldots, d_n)$ *je nerostoucí posloupnost a* $n \geq 2$. *Posloupnost* $\mathbf{d}$ *je grafová, právě když je grafová posloupnost*

$$\mathbf{d}' = (d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n).$$

Důkaz. '$\Leftarrow$': Nechť je dána posloupnost $\mathbf{d}$ a nechť $\mathbf{d}'$ je skóre grafu G'. Přidejme ke grafu G' nový vrchol v a spojme jej hranami s d_1 vrcholy nevyšších stupňů. Výsledný graf má skóre $\mathbf{d}$.

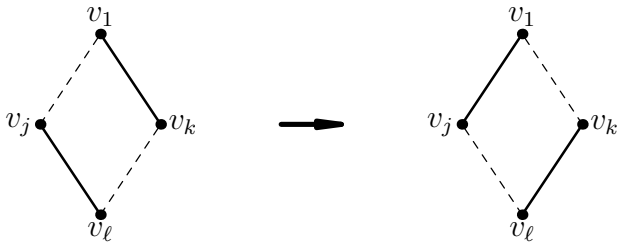
'$\Rightarrow$': Dejme tomu, že $\mathbf{d}$ je skóre grafu G. Přímočarým odstraněním vrcholu w s nejvyšším stupněm bohužel nemusíme dostat graf se skóre $\mathbf{d}'$ — k tomu bychom potřebovali, aby sousedy vrcholu w bylo d_1 vrcholů, jejichž stupně jsou nejvyšší hned po w. Naší strategií proto bude upravit G na graf se stejným skóre, který tuto vlastnost má.

Nechť H je libovolný graf se skóre $\mathbf{d}$. Seřaďme jeho vrcholy do posloupnosti $(v_1, \ldots, v_n)$ tak, že stupeň vrcholu v_i je d_i (jinak na výběru seřazení nezáleží). Definujme *kvalitu* $q(H)$ grafu H jako největší i, pro které platí, že vrchol v_1 sousedí se všemi vrcholy $v_2, \ldots, v_i$. (Pokud jsou nesousední již vrcholy v_1, v_2, položíme $q(H) = 1$.) Nechť H_0 je graf s nejvyšší možnou kvalitou mezi všemi grafy se skóre $\mathbf{d}$.

Předpokládejme nejprve, že $q(H_0)$ je nejvýše d_1. Mezi d_1 vrcholy $v_2, \ldots, v_{d_1+1}$ je tedy vrchol v_j, který nesousedí s vrcholem v_1. Protože stupeň vrcholu v_1 je d_1, musí nutně existovat nějaký jeho soused v_k, kde $k > d_1 + 1$. Tvrdíme, že existuje vrchol v_ℓ s vlastností

$$v_j v_\ell \in E(H), \quad \text{ale} \quad v_k v_\ell \notin E(H). \tag{5.1}$$

Jinak by totiž každý soused vrcholu v_j byl i sousedem vrcholu v_k, a s ohledem na vrchol v_1 bychom dostali $d_j < d_k$. To je nemožné, protože $j < k$ a posloupnost $\mathbf{d}$ je nerostoucí. Vrchol v_ℓ s vlastností (5.1) tedy existuje.



Obrázek 5.4: Zvýšení kvality grafu v důkazu věty 5.8. Hrany jsou znázorněny plně, 'nehrany' čárkovaně.

Vrcholy v_1, v_j, v_k a v_ℓ tvoří 'konfiguraci' na levé straně obr. 5.4. Pokud hrany v_1v_k a v_jv_ℓ nahradíme v grafu H_0 hranami v_1v_j a v_kv_ℓ, stupně vrcholů (a tedy ani skóre) se nezmění, ale kvalita výsledného grafu bude vyšší. To je spor s maximalitou $q(H_0)$.

Dokázali jsme, že $q(H_0) > d_1$, takže vrchol v_1 sousedí s vrcholy $v_2, \ldots, v_{d_1+1}$. Nyní ovšem graf vzniklý odstraněním vrcholu v_1 z grafu H_0 má skóre $\mathbf{d}'$. Posloupnost $\mathbf{d}'$ je tedy grafová, což jsme chtěli dokázat. □

Cvičení

▶ **5.7** Zjistěte skóre grafů:

(a) úplný bipartitní graf $K_{p,q}$ (p červených a q modrých vrcholů, každé dva různobarevné jsou spojeny hranou),

(b) Hasseův diagram Booleovy algebry 2^X, kde $X = \{1, \ldots, k\}$.

▶ **5.8** Najděte dvojici neisomorfních grafů se stejným skóre.

▶ **5.9** Pro která n existuje graf se skóre $(n, n-1, \ldots, 1)$?

▶ **5.10** Rozhodněte, zda následující posloupnost je souborem stupňů nějakého grafu, a případně takový graf najděte:

(a) $(5, 5, 4, 4, 3, 3)$,

(b) $(5, 5, 5, 4, 4, 3, 2)$.

(c) $(7, 6, 6, 5, 4, 4, 4, 3, 3, 3, 2)$,

▶▶ **5.11** Graf je *k-regulární*, pokud všechny jeho vrcholy mají stupeň k.

(a) Dokažte, že na n vrcholech existuje 3-regulární graf, právě když n je sudé.

(b) Charakterizujte dvojice (n, k) s vlastností, že existuje nějaký k-regulární graf na n vrcholech.

Kapitola 6

Cesty v grafu

Tématem této kapitoly jsou cesty v grafech a různé jejich modifikace. Pomocí cest zavedeme souvislé grafy a odvodíme některé jejich vlastnosti. Představíme rovněž eulerovské a hamiltonovské grafy a prozkoumáme překvapivý rozdíl v obtížnosti algoritmického rozpoznávání grafů z těchto dvou tříd.

6.1 Sled, cesta a tah

Definice 6.1 *Sled* (z vrcholu u do vrcholu v) v grafu G je libovolná posloupnost $(u = v_0, v_1, \ldots, v_k = v)$, kde v_i jsou vrcholy grafu G a pro každé $i = 1, \ldots, k$ je $v_{i-1}v_i$ hranou grafu G. Číslo k je *délka* tohoto sledu. Říkáme, že sled *prochází* vrcholy $v_0, \ldots, v_k$ nebo že na něm tyto vrcholy *leží*.

Sled je tedy jakási procházka po grafu, při které v každém kroku přecházíme po hraně mezi sousedními vrcholy. V rámci této procházky můžeme libovolný vrchol navštívit vícekrát, můžeme dokonce i projít vícekrát po téže hraně.

Definice 6.2 *Cesta* z u do v v grafu G je sled $(u = v_0, v_1, \ldots, v_k = v)$, ve kterém se každý vrchol v_i objevuje pouze jednou.

Za zmínku stojí triviální případ uvedených definic, totiž sled (u), kde $u \in V$. Jedná se o sled nulové délky z u do u, který je zároveň i cestou.

Cvičení

▶ **6.1** Uvažme libovolnou cestu $(v_0, \ldots, v_k)$ v grafu G. Nechť $V' = \{v_0, \ldots, v_k\}$ je množina vrcholů, kterými tato cesta prochází, a $E' = \{v_{i-1}v_i : i = 1, \ldots, k\}$ je množina hran, které používá. Dokažte, že podgraf (V', E') grafu G je isomorfní s grafem P_{k+1} definovaným v oddílu 5.2.

6.2 Homomorfismy

Alternativní definice sledu a cesty je založena na pojmu homomorfismus.

Definice 6.3 *Homomorfismus* grafu G do grafu H je zobrazení $f : V(G) \to V(H)$ s vlastností, že pro každou hranu xy grafu G je $f(x)f(y)$ hranou grafu H.

Všimněme si, že oproti pojmu isomorfismus z oddílu 5.3 nemusí f být bijekce, a že namísto ekvivalence je zde vyžadována jediná implikace.

Nyní již můžeme podat alternativní definici sledu v grafu G: je to libovolný homomorfismus nějaké cesty P_k (viz oddíl 5.2) do G. Rozdíl oproti definici 6.1 je jen formální: posloupnost vrcholů a hran je tu nahrazena zobrazením.

Každý homomorfismus f grafu G do grafu H indukuje zobrazení $f^* : E(G) \to E(H)$ předpisem

$$f^*(xy) = f(x)f(y) \in E(H).$$

Definice 6.4 Nechť f je homomorfismus grafu G do grafu H. Řekneme, že f je

- *vrcholový monomorfismus,* pokud $f : V(G) \to V(H)$ je prosté zobrazení,
- *vrcholový epimorfismus,* pokud f je zobrazení na,
- *hranový monomorfismus,* pokud f^* je prosté,
- *hranový epimorfismus,* pokud f^* je na.

Cestu v grafu G nyní můžeme ekvivalentně definovat jako vrcholový monomorfismus z nějaké cesty P_k do grafu G. Později, např. v oddílu 6.5, se seznámíme s dalšími pojmy, které se dají definovat pomocí homomorfismů.

Cvičení

▶ **6.2** Najděte příklad homomorfismu mezi dvěma grafy, který je vrcholovým monomorfismem a hranovým epimorfismem, ale není isomorfismem.

6.3 Souvislé grafy

Definice 6.5 Graf G je *souvislý*, pokud pro každé dva vrcholy x, y existuje v grafu G cesta z x do y. V opačném případě je graf G *nesouvislý*.

Nechť G je graf s množinou vrcholů V. Definujme na V relaci $\sim$ předpisem

$$x \sim y, \quad \text{pokud v } G \text{ existuje cesta z } x \text{ do } y.$$

Jedná se o ekvivalenci? Určitě je to relace reflexívní (díky existenci cesty délky 0) a symetrická (protože přečteme-li cestu pozpátku, bude to podle definice zase

cesta). Pokud jde o tranzitivitu, máme-li cestu z x do y a cestu z y do z, zdá se jako přirozená idea 'složením' těchto cest získat cestu z x do z. Potíž je ovšem v tom, že výsledkem složení nemusí být cesta, protože původní dvě cesty se mohou libovolně protínat. Pomůže nám však následující tvrzení.

Tvrzení 6.6 *Existuje-li v grafu G sled z vrcholu x do vrcholu y, potom $x \sim y$.*

Důkaz. Chceme ukázat, že existuje-li sled z x do y, pak existuje také cesta z x do y. Nechť tedy $(x = v_0, v_1 \ldots, v_{k-1}, v_k = y)$ je sled z x do y, a zvolme jej tak, aby k bylo nejmenší možné (tj. aby žádný sled z x do y neměl menší délku). Tvrdíme, že takovýto minimální sled (označme jej S) již musí být cestou.

Dejme tomu, že není. Pak se v něm musí nějaký vrchol opakovat, tj. pro nějaké $i \neq j$ musí být $v_i = v_j$. Pokud z našeho sledu

$$(x = v_0, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_{j-1}, v_j, v_{j+1}, \ldots, v_k = y)$$

vypustíme část od v_{i+1} do v_j včetně, dostaneme posloupnost

$$(x = v_0, \ldots, v_{i-1}, v_i, v_{j+1}, \ldots, v_k = y),$$

která je podle definice rovněž sledem (vrcholy v_i a v_{j+1} jsou totiž sousední). Navíc jde o sled z x do y, který je kratší než S. To je spor. □

Důsledek 6.7 *Relace $\sim$ na množině V je ekvivalence.*

Důkaz. Povšimli jsme si, že reflexivita a symetričnost platí z jednoduchých důvodů. Dokažme tranzitivitu. Předpokládejme $x \sim y$ a $y \sim z$. Nechť $(x = v_0, \ldots, v_k = y)$ je cesta z x do y a $(y = w_0, \ldots, w_\ell = z)$ je cesta z y do z. Potom posloupnost

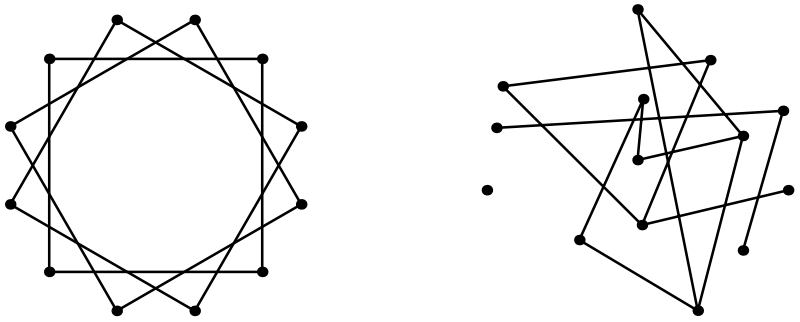
$$(x = v_0, v_1, \ldots, v_{k-1}, v_k = w_0, w_1, \ldots, w_{\ell-1}, w_\ell = z)$$

je sled z x do z (třebaže to nemusí být cesta) a podle tvrzení 6.6 je $x \sim z$. □

Definice 6.8 *Komponenty* grafu G jsou všechny indukované podgrafy grafu G na jednotlivých třídách ekvivalence $\sim$.

Je-li tedy K komponenta grafu G, pak $V(K)$ je jednou ze tříd ekvivalence $\sim$. Je jasné, že K je souvislý graf, protože prvky téže třídy libovolné ekvivalence jsou každý s každým v relaci. Na druhou stranu je K maximální souvislý podgraf grafu G: nejde jej rozšířit o další vrchol, nemá-li ztratit souvislost. Ze žádného vrcholu komponenty K totiž nevede hrana do žádného vrcholu mimo ni (cvičení 6.3).

Mohlo by se zdát, že komponenty grafu lze snadno určit 'na první pohled', ale u větších nebo nepřehledně zadaných grafů to tak triviální být nemusí (viz cvičení 6.5). Přesto je pravda, že z algoritmického hlediska je určení komponent a testování souvislosti grafu snadným problémem. K oběma účelům lze použít např. Dijkstrův algoritmus, který popíšeme v oddílu 12.2 (viz ale také cvičení 6.7).



(a) (b)

Obrázek 6.1: Určete počet komponent.

Cvičení

► **6.3** Dokažte, že je-li K komponenta grafu G, $u \in V(K)$ a $v \notin V(K)$, pak mezi u a v není hrana.

► **6.4** Dokažte, že graf je souvislý právě tehdy, když má jedinou komponentu.

► **6.5** Určete počet komponent grafů na obr. 6.1.

►► **6.6** Cesta P v grafu G je *nejdelší*, pokud G neobsahuje cestu s více vrcholy. Ukažte, že dvě nejdelší cesty v souvislém neorientovaném grafu G mají společný alespoň jeden vrchol.

► **6.7** Formulujte algoritmus, který zjistí, zda je zadaný graf souvislý, a případně určí jeho komponenty. Vstupem algoritmu je seznam vrcholů a hran grafu.

6.4 Vlastnosti souvislých grafů

Definice 6.9 Nechť v je vrchol grafu G. Graf $G-v$, vzniklý *odstraněním* vrcholu v, je definován jako indukovaný podgraf grafu G na množině $V(G) - \{v\}$.

Následující věta ukazuje, že souvislý graf vždy obsahuje vrchol, jehož odstraněním neztratí souvislost. Její důkaz vtipně používá předpoklad maximality.

Věta 6.10 *Každý souvislý graf G obsahuje vrchol v s vlastností, že $G - v$ je souvislý graf.*

Důkaz. Nechť $P = (v_0, \ldots, v_k)$ je cesta maximální možné délky v grafu G. Tvrdíme, že vrchol v_0 má požadovanou vlastnost. Dejme tomu, že $G - v_0$ je nesouvislý graf. Cesta $P - v_0$ musí zjevně celá ležet v jedné komponentě grafu $G - v_0$. Kromě této komponenty existuje alespoň jedna další komponenta C. Z vrcholu v_0 musí vést do komponenty C nějaká hrana, což nám umožňuje prodloužit cestu P. Tím dostáváme spor s maximalitou. □

Všimněme si, že místo vrcholu v_0 jsme stejně tak mohli zvolit druhý konec cesty P, vrchol v_k. Pokud má tedy graf G více než jeden vrchol, pak existují dokonce alespoň dva vrcholy splňující podmínku věty 6.10.

Zaveďme nyní následující konvenci: bude-li z kontextu jasné, o kterém grafu se hovoří, bude n označovat *počet jeho vrcholů* a m *počet jeho hran*.

Věta 6.11 *V souvislém grafu je $m \geq n - 1$.*

Důkaz. Větu dokážeme indukcí. Pro $n = 1$ se jedná o graf na jednom vrcholu, a ten je souvislý. Předpokládejme, že věta platí pro všechny grafy s méně než n vrcholy, kde $n > 1$, a dokažme ji pro libovolný graf G s n vrcholy. Nechť G má m hran. Podle věty 6.10 v grafu G existuje vrchol v, který lze odstranit bez porušení souvislosti. Graf $G - v$ má $n' = n - 1$ vrcholů a počet m' jeho hran je nejvýše $m - 1$ (do vrcholu v vedla alespoň jedna hrana). Z indukčního předpokladu je $m' \geq n' - 1$, a tedy

$$m \geq m' + 1 \geq (n' - 1) + 1 = n - 1,$$

což jsme chtěli dokázat. □

Jaký je vztah souvislosti grafu a počtu jeho hran? Intuitivně je zřejmé, že se zvyšujícím se počtem hran roste šance, že graf bude souvislý. Na druhou stranu: přidáme-li k úplnému grafu na $n - 1$ vrcholech jeden izolovaný vrchol, získáme nesouvislý graf s velmi vysokým počtem hran.

Tomuto příkladu bychom se vyhnuli, kdybychom požadovali, aby každý vrchol měl dostatečně velký stupeň. Zde je extrémním (v teorii grafů se říká také extremálním) příkladem disjunktní sjednocení dvou úplných grafů na $n/22$ vrcholech; to je nesouvislé a každý vrchol má stupeň $n/2 - 1$. Tento příklad ukazuje, že následující větu není možné zlepšit:

Věta 6.12 *Jsou-li stupně všech vrcholů v grafu G alespoň $n/2$, pak je G souvislý graf.*

Důkaz. Dejme tomu, že věta neplatí a G je nesouvislý. Má tedy aspoň dvě neprázdné komponenty A,B. Alespoň jedna z těchto komponent (dejme tomu A) má nejvýše $n/2$ vrcholů, jinak by počet vrcholů v celém grafu nemohl být n. Z libovolného vrcholu v komponenty A vedou hrany jen do ostatních vrcholů této komponenty, kterých je nejvýše $n/2 - 1$. Stupeň vrcholu v tedy musí být menší než $n/2$, což je spor s naším předpokladem. □

Cvičení

► **6.8** Dokažte, že v grafu s k komponentami platí $m \geq n - k$.

►► **6.9** Dokažte, že graf, ve kterém jsou stupně všech vrcholů alespoň δ, má méně než n/δ komponent.

6.5 Kružnice

Definice 6.13 *Uzavřený sled* v grafu G je sled $(v_0, \ldots, v_k)$, ve kterém platí $v_0 = v_k$. *Kružnice v grafu* G je uzavřený sled délky alespoň 3, ve kterém se vrchol v_0 objevuje právě dvakrát a každý ostatní vrchol nejvýše jednou. Číslo k je *délka* dané kružnice.

Kružnici a uzavřený sled v grafu G můžeme ekvivalentně definovat pomocí pojmů z oddílu 6.2: uzavřený sled v grafu G není nic jiného než homomorfismus nějaké kružnice C_k (viz oddíl 5.2) do G. Takový homomorfismus je kružnicí v grafu G, právě když je to vrcholový monomorfismus.

Ve cvičení 6.1 jsme viděli, že cesty délky k v grafu G lze ztotožnit s podgrafy isomorfními s grafem P_{k+1}. Podobně ztotožníme kružnice délky k v grafu G s podgrafy isomorfními s grafem C_k. Můžeme tak mluvit o množině hran nějaké kružnice v grafu G a podobně.

V minulém oddílu jsme definovali operaci odstranění vrcholu z grafu. Její přirozenou obdobou je operace odstranění hrany. Jedná se o pouhé smazání hrany se zachováním jejích koncových vrcholů.

Definice 6.14 Je-li e hrana grafu $G = (V, E)$, potom graf $G - e$ vzniklý *odstraněním hrany* e je definován jako graf $(V, E - \{e\})$.

Věta 6.15 *Je-li e hrana souvislého grafu G, která leží na nějaké kružnici, potom $G - e$ je souvislý graf.*

Důkaz. Nechť $e = xy$ je hranou kružnice C. V kružnici C existují dvě cesty z vrcholu x do vrcholu y; tu z nich, která má délku větší než 1, označme P.

Dokazujeme, že $G-e$ je souvislý graf. K tomu stačí najít sled mezi libovolnými dvěma vrcholy u, v. Nechť S je cesta z u do v v (souvislém) grafu G. Pokud S nepoužívá hranu e, je cestou i v grafu $G-e$. Pokud ji používá, můžeme tuto hranu nahradit cestou P. Přesněji řečeno, pokud $S = (u = s_0, s_1, \ldots, s_i = x, s_{i+1} = y, \ldots, s_k = v)$ a $P = (x = p_0, p_1, \ldots, p_\ell = y)$, vezmeme

$$S' = (u = s_0, s_1, \ldots, s_{i-1}, x = p_0, p_1, \ldots, p_\ell = y, s_{i+2}, \ldots, s_k = v),$$

což je sled v grafu $G - e$. (V případě, že S hranu e používá v opačném směru, tedy $s_i = y$, $s_{i+1} = x$, vložíme i cestu P obráceně.) Důkaz je hotov. □

Implikace ve větě 6.15 se dokonce dá zesílit na ekvivalenci (viz cvičení 6.10).

Cvičení

▶ **6.10** Dokažte, že je-li $G - e$ souvislý graf, pak hrana e grafu G leží na nějaké kružnici.

6.6 Eulerovské a hamiltonovské grafy

Již v 18. století zkoumal Leonhard Euler (1707–1803) následující problém[1]: za jakých podmínek existuje sled, který používá každou hranu daného grafu právě jednou? Touto otázkou se dostáváme k pojmu tah.

Definice 6.16 *Tah* z u do v v grafu G je sled $(u = v_0, v_1, \ldots, v_k = v)$, ve kterém se mohou opakovat vrcholy, ale hrany $v_{i-1}v_i$ jsou pro různá i různé. *Uzavřený* tah je tah, který je uzavřeným sledem. Uzavřený tah je *eulerovský*, pokud používá každou hranu grafu G.

Podobně jako sledy, cesty a kružnice v grafu, i tah se dá snadno ekvivalentně definovat pomocí pojmu homomorfismus (viz cvičení 6.11). V dalším textu se nám bude hodit následující pozorování.

Lemma 6.17 *Nechť T je tah z vrcholu x do vrcholu y v grafu G. Označme počet hran tahu T, obsahujících vrchol $z \in V(G)$, symbolem $d_T(z)$. Pak platí, že $d_T(z)$ je sudé, právě když T je uzavřený tah nebo $z \notin \{x, y\}$.*

Důkaz. Nechť $T = (v_0, \ldots, v_k)$, kde $x = v_0$ a $y = v_k$. Opatřeme každou hranu v_iv_{i+1} tahu T šipkou z vrcholu v_i do vrcholu v_{i+1}. Kolik šipek směřuje do vrcholu z a kolik ven?

Každému výskytu vrcholu z v tahu T odpovídá nějaký index i s vlastností $z = v_i$. Označme výskyt jako *vnitřní*, je-li $0 < i < k$. Každý vnitřní výskyt přispívá jednu šipku směrem do z (na hraně $v_{i-1}v_i$) a jednu šipku ven (hrana v_iv_{i+1}). Vnitřní výskyty zachovávají rovnováhu mezi počty šipek v obou směrech a je při nich tedy použit sudý počet hran. Tyto hrany nemají na paritu čísla $d_T(z)$ vliv a můžeme je tedy ignorovat; ostatní hrany označíme jako *podstatné* (pro z).

Pokud $z \notin \{x, y\}$, pak vrchol z není obsažen v žádné podstatné hraně, takže $d_T(z)$ je sudé. Můžeme tedy předpokládat, že $z = x$ (případ $z = y$ je symetrický a nemusíme jej uvažovat zvlášť). Je-li tah T uzavřený, pak podstatné hrany obsahující vrchol z jsou v_0v_1 a v_kv_0, takže i v tomto případě je $d_T(z)$ sudé číslo. Konečně pokud tah T není uzavřený, pak jedinou podstatnou hranou obsahující vrchol z je hrana v_0v_1, takže $d_T(z)$ je liché. Složením všech tří případů dostaneme požadovanou ekvivalenci. □

[1] Euler ilustroval své výsledky na slavném příkladu: ukázal, že není možné přejít během jediné procházky právě jednou přes každý z mostů ve městě Královci (Königsberg, dnešní Kaliningrad) a vrátit se na stejné místo.

Eulerova odpověď na otázku, které grafy mají eulerovský tah, je obsažena v následující větě.

Věta 6.18 *Souvislý graf G má eulerovský tah, právě když všechny jeho vrcholy mají sudý stupeň.*

Důkaz. '$\Rightarrow$': Eulerovský tah je uzavřený, takže tvrzení plyne z lemmatu 6.17.

'$\Leftarrow$': Nechť M je uzavřený tah maximální možné délky. Dokážeme, že M obsahuje každou hranu grafu G. Pro důkaz sporem předpokládejme, že neobsahuje hranu $e = xy$. Nejprve najdeme hranu e_0, která rovněž není obsažena v tahu M, ale tento tah prochází alespoň jedním z jejích koncových vrcholů. Jak ji najít? Můžeme předpokládat, že tah M neprochází vrcholem x, jinak stačí vzít $e' = e$. Ze souvislosti grafu G existuje cesta z x do nějakého vrcholu, kterým prochází tah M. Nejkratší taková cesta (označme ji P) jistě neobsahuje žádnou hranu tahu M, jinak bychom ji mohli zkrátit. Na druhou stranu je délka cesty P alespoň 1 (protože tah M neobsahuje vrchol x). Zvolme tedy za hranu e_0 poslední hranu cesty P. Ta má požadované vlastnosti: neleží na tahu M, ale ten prochází jedním z jejích koncových vrcholů.

Najdeme nyní uzavřený tah T, který neobsahuje žádnou hranu tahu M. Zkonstruujeme jej postupným přidáváním hran. Nechť z_0 je koncový vrchol hrany e_0, který leží na tahu M. Označme druhý koncový vrchol symbolem z_1 a definujme výchozí (neuzavřený) tah $T_1 = (z_0, z_1)$. Podle lemmatu 6.17 je počet hran tahu M, obsahujících vrchol z_1, sudý. Celkový stupeň tohoto vrcholu je rovněž sudý, takže kromě hrany $e_0 = z_0z_1$ musí existovat ještě nějaká hrana e_1 obsahující vrchol z_1, kterou tah M neprochází. Položme $T_2 = (z_0, z_1, z_2)$, kde z_2 je druhý koncový vrchol hrany e_1.

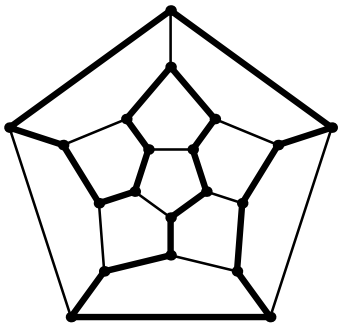
V i-tém kroku konstrukce máme zkonstruován tah T_i, který končí ve vrcholu z_i. Je-li $z_i = z_0$, jsme hotovi, protože T_i je uzavřený tah s požadovanou vlastností. Jinak podle lemmatu 6.17 je z hran obsahujících vrchol z_i sudý počet obsažen v tahu M a lichý počet v tahu T_i. Protože stupeň vrcholu z_i je sudý, existuje hrana e_{i+1}, která z něj vychází a není obsažena z žádném z tahů M a T_i. Přidáním druhého koncového vrcholu z_{i+1} hrany e_{i+1} k tahu T_i získáme delší tah T_{i+1}.

Graf G obsahuje konečný počet hran, a tak po konečném počtu kroků musí nastat situace $z_i = z_0$. Tím je existence tahu T dokázána. Zbývá si všimnout, že tah T lze použít k prodloužení tahu M. Stačí procházet po tahu M až k nějakému výskytu vrcholu z_0, projít celý uzavřený tah T, a poté projít zbývající část tahu M. Výsledný uzavřený tah M' má větší délku než M (víme totiž, že délka tahu T je nenulová!) a to je spor. □

Graf, který má nějaký eulerovský tah, se nazývá *eulerovský* graf. Podle věty 6.18 je snadné poznat, zda je daný graf eulerovský: stačí zkontrolovat, zda je souvislý a zda všechny stupně jsou sudé. Není tedy potřeba např. zkoušet všechny možné tahy a zjišťovat, zda některý náhodou není eulerovský.

Nabízí se malá modifikace uvažovaného pojmu. Eulerovský tah je uzavřený sled, používající každou hranu právě jednou. Co se změní, budeme-li požadovat, aby daný uzavřený sled obsahoval každý *vrchol* právě jednou? Takový sled musí být kružnicí. Kružnice, která prochází všemi vrcholy grafu, se nazývá *hamiltonovská*, a graf obsahující nějakou takovou kružnici je *hamiltonovský graf*.

Název je odvozen od jména irského matematika William Rowana Hamiltona (1805–1865). Ten v roce 1857 vynalezl hlavolam, jehož zadáním bylo najít 'cestu' po hranách tzv. dvanáctistěnu (trojrozměrného mnohostěnu o 20 vrcholech), která navštíví každý vrchol právě jednou a vrátí se na výchozí místo. Úloha je ekvivalentní s nalezením hamiltonovské kružnice v grafu na obr. 6.2, kterému se rovněž říká dvanáctistěn.



Obrázek 6.2: Dvanáctistěn s vyznačenou hamiltonovskou kružnicí.

Existuje nějaké kritérium ve stylu věty 6.18, které by nám umožňovalo snadno a rychle poznat hamiltonovské grafy? Vzhledem k podobnosti pojmů eulerovský tah a hamiltonovská kružnice by se to mohlo zdát pravděpodobné. Odpověď na tuto otázku však poněkud překvapivě není známa a vše nasvědčuje tomu, že takové kritérium neexistuje. Na druhou stranu je známa celá řada postačujících podmínek pro existenci hamiltonovské kružnice. Lze například ukázat, že hamiltonovský je každý graf, pro který je splněn předpoklad věty 6.12 (toto zesílení věty 6.12, tzv. *Diracova věta*, patří ke klasickým výsledkům teorie grafů).

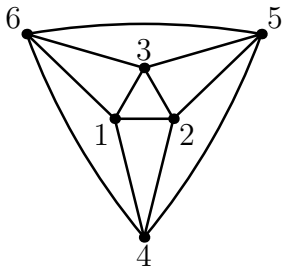
Abychom mohli přesněji popsat rozdíl mezi problémy rozpoznávání hamiltonovských a eulerovských grafů, potřebujeme se stručně zmínit o výpočetní složitosti.

Cvičení

► **6.11** Definujte tah a uzavřený tah pomocí pojmů z oddílu 6.2.

► **6.12** Najděte eulerovský tah v grafu na obr. 6.3.

► **6.13** Dokažte, že souvislý graf G má (uzavřený nebo neuzavřený) tah obsahující každou hranu přesně jednou, právě když G má nejvýše dva vrcholy lichého stupně.



Obrázek 6.3: Graf ve cvičení 6.12.

6.7 Časová složitost algoritmu

Představme si nějaký algoritmus A, který pro libovolný graf G (*vstupní graf*) rozhodne, zda má G určitou vlastnost (třeba zda je eulerovský). Takový algoritmus sestává z množství *elementárních operací* jako je sečtení dvou čísel nebo zjištění, zda mezi určitými dvěma vrcholy grafu G vede hrana.[2] Počet elementárních operací, které si provedení algoritmu vyžádá, samozřejmě závisí na vstupním grafu G; označme tento počet $f(G)$. *Časová složitost* algoritmu A je funkce $f : \mathbf{N} \to \mathbf{N}$, definovaná vztahem

$$f(n) = \max_G f(G),$$

kde G probíhá všechny grafy na n vrcholech. Jde tedy o počet elementárních operací, nutných 'v nejhorším případě' pro zpracování grafu na n vrcholech. Časová složitost může být vyjádřena i pomocí jiných parametrů vstupního grafu, než je počet vrcholů, a lze ji analogicky definovat i pro algoritmy, které pracují s jinými strukturami než s grafy.

Vraťme se k rozpoznávání eulerovských grafů. Navržený algoritmus prochází jeden vrchol po druhém a testuje, zda jeho stupeň je sudý. Pokud jde o vstupní graf G, předpokládejme, že pro každý vrchol grafu G je zadán seznam jeho sousedů. Jaká je časová náročnost tohoto algoritmu? Pro každý z n vrcholů je třeba spočítat stupeň, a to obnáší zjistit existenci nebo neexistenci každé z $n-1$ potenciálních hran vedoucích z tohoto vrcholu. Časová složitost je tedy $n(n-1)$. Je to tedy *kvadratická* funkce proměnné n; pokud nám stačí odhadnout 'řádovou'

[2] Přesné vymezení elementárních operací, tvaru vstupních dat atd. je obecně velmi důležité, nám však bude stačit tento intuitivní pohled na věc.

závislost časové složitosti na n, řekneme, že časová složitost je $O(n^2)$. (Obecně pro dvě funkce $g, h : \mathbf{N} \to \mathbf{N}$ píšeme $g = O(h)$, pokud existuje konstanta c tak, že pro dost velké n platí $g(n) < c \cdot h(n)$.) Náš algoritmus je tedy *polynomiální*, jeho časová složitost je určena polynomem.

Jak testovat, zda je daný graf hamiltonovský? Nejsou k dispozici o mnoho lepší metody než 'hrubá síla', např. zkoušet hamiltonovskou kružnici vybudovat postupným prodlužováním cesty, v případě neúspěchu se vracet zpět a probírat další možnosti (tzv. *backtracking*). Příklad podobného postupu uvidíme v oddílu 12.5. V každém vrcholu máme obvykle několik možností, jak postupovat dále, takže počet všech situací, které je třeba probrat, se s každým dalším vrcholem alespoň zdvojnásobuje. Časová složitost takového algoritmu je katastrofální: je vyšší než libovolný polynom, je to *exponenciální* funkce n, jako je např. funkce 2^n (nebo ještě horší). Zde z teoretického hlediska vede dělicí čára mezi rychlými a pomalými algoritmy: 'rychlý' (neboli *efektivní*) je algoritmus s polynomiální časovou složitostí, 'pomalé' jsou ty ostatní[3]. Rozdíl mezi polynomiální a exponenciální časovou složitostí ilustruje tabulka 6.1, ve které je uvedena doba provádění algoritmu s časovou složitostí n^3 resp. 2^n pro různé velikosti vstupních dat n a za předpokladu, že provedení jedné operace trvá 1 mikrosekundu.

	10	20	50	100	200
n^3	1 ms	8 ms	125 ms	1 s	8 s
2^n	1 ms	1 s	36 let	$4 \cdot 10^{16}$ let	$5 \cdot 10^{46}$ let

Tabulka 6.1: Polynomiální a exponenciální časová složitost.

Přestože se obě úlohy popsané v oddílu 6.6 (rozhodování, zda je graf eulerovský resp. hamiltonovský) zdají velmi podobné, náročnost jejich algoritmického řešení je dramaticky rozdílná. Problém zjišťování hamiltonovskosti totiž patří do velké třídy tzv. *NP-úplných problémů*. Jde o velmi obtížné problémy, pro které není znám efektivní algoritmus, ale zároveň není dokázána jeho neexistence. Otázka, zda takový algoritmus existuje, patří k největším otevřeným problémům současné matematiky.

O časové složitosti algoritmů se lze dozvědět více např. v přednášce [8] nebo v knize [2]. My se k tomuto tématu vrátíme především v oddílu 12.2, kde budeme analyzovat časovou složitost tzv. Dijkstrova algoritmu. S dalším NP-úplným problémem, tzv. problémem obchodního cestujícího, se seznámíme v oddílu 12.5.

[3]Může se samozřejmě stát, že je exponenciální algoritmus pro 'rozumné' hodnoty n rychlejší než třeba polynomiální algoritmus se složitostí $1000000n^8$. Na druhou stranu praxe ukazuje, že se pro úlohy řešitelné efektivním algoritmem zpravidla daří postupně snížit časovou složitost algoritmu do 'rozumných' mezí. Ke vzácným výjimkám zatím patří tzv. *problém lineárního programování*.

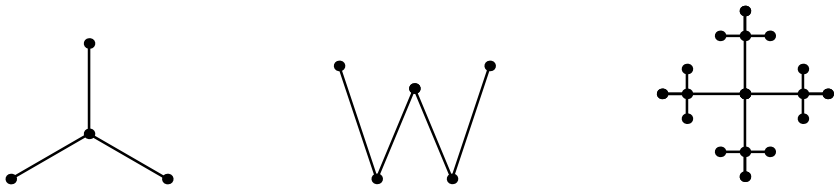
Kapitola 7

Stromy

Stromy jsou jednou z nejdůležitějších tříd grafů. O tom svědčí i množství vět, které je z různých pohledů charakterizují. Několik z nich dokážeme v této kapitole. Představíme také dvě praktické aplikace stromů: první se týká vyhledávání v lineárně uspořádané množině, druhá optimálního kódování symbolů z nějaké abecedy.

7.1 Definice

Definice 7.1 *Strom* je souvislý graf, který neobsahuje žádnou kružnici. *List* stromu T je libovolný vrchol, jehož stupeň v T je 1.



(a) (b) (c)

Obrázek 7.1: Stromy.

Několik příkladů stromů ukazuje obr. 7.1. Tyto stromy mají (zleva doprava) 3, 2 a 12 listů.

Tvrzení 7.2 *Každý strom má alespoň dva listy.*

Důkaz. Vezměme cestu P maximální možné délky ve stromu T. Nechť x je koncový vrchol cesty P. Každý soused vrcholu x musí ležet na cestě P, jinak by bylo možné ji prodloužit. Dejme tomu, že x není list a má tedy alespoň dva

sousedy y_1, y_2. Sled, který dostaneme, pokud vyjdeme z vrcholu x do vrcholu y_1, dále po cestě P do y_2 a zpět do x, je kružnicí v grafu T. Ten je ale stromem a žádnou kružnici neobsahuje, takže x je skutečně list. Dalším listem je druhý koncový vrchol cesty P. □

V tomto oddílu si ukážeme tři důležité věty, z nichž každá charakterizuje stromy z jiného hlediska: věta 7.3 podle počtu cest mezi dvěma vrcholy, věta 7.4 podle počtu hran a konečně věta 7.6 podle nesouvislosti jistých podgrafů (tzv. faktorů).

Z definice je graf souvislý, obsahuje-li alespoň jednu cestu mezi každou dvojicí vrcholů. Pokud podmínku zesílíme a budeme požadovat existenci právě jedné cesty, pak podle následující věty budou této podmínce vyhovovat právě všechny stromy.

Věta 7.3 *Graf G je strom, právě když pro každé dva vrcholy $u, v \in V(G)$ existuje v grafu G právě jedna cesta z u do v.*

Důkaz. '$\Rightarrow$': Strom G je z definice souvislý, takže alespoň jedna cesta mezi každými dvěma vrcholy existuje. Nechť P, Q jsou dvě cesty z vrcholu u do vrcholu v, přičemž

$$P = (u = p_0, p_1, \ldots, p_k = v),$$
$$Q = (u = q_0, q_1, \ldots, q_\ell = v).$$

Nechť i je nejmenší index takový, že $p_i \neq q_i$. Vzhledem k tomu, že cesty P a Q jsou různé, ale začínají v témže vrcholu, platí $1 \leq i \leq k, \ell$. Zvolme j nejmenší takové, že $j > i$ a q_j leží na cestě P. Víme, že přinejmenším q_ℓ na P leží, proto takový index j jistě existuje. Definujme sled S následujícím způsobem: vyjdeme z vrcholu p_{i-1} po cestě P do p_j a odtud po cestě Q zpět do $q_{i-1} = p_{i-1}$. Je jasné, že S je kružnice v grafu G, což je spor s předpokladem, že G je strom. Mezi u a v je tedy jen jediná cesta.

'$\Leftarrow$': Graf G, ve kterém mezi každými dvěma vrcholy existuje nějaká cesta, je jistě souvislý. Pokud by obsahoval kružnici, vedly by mezi libovolnými dvěma vrcholy této kružnice alespoň dvě cesty. Graf G, který splňuje náš předpoklad, je tedy stromem. □

Podle věty 6.11 má souvislý graf na n vrcholech aspoň $n-1$ hran. Následující věta říká, že stromy lze charakterizovat jako grafy, u nichž v tomto dolním odhadu počtu hran platí rovnost.

Věta 7.4 *Graf G je strom, právě když je souvislý a má $n-1$ hran.*

Důkaz. '$\Rightarrow$': Strom je z definice souvislý. Ukážeme indukcí podle počtu vrcholů, že má $n-1$ hran. Pro strom na jednom vrcholu tvrzení jistě platí. Nechť je dán strom G s $n > 1$ vrcholy a nechť v je některý jeho list (existuje podle tvrzení 7.2).

Graf $G - v$ je strom (jak je vidět z definice) a má $n - 1$ vrcholů a $m - 1$ hran. Podle indukčního předpokladu je $m - 1 = (n - 1) - 1$ a tedy $m = n - 1$, což jsme chtěli dokázat.

'$\Leftarrow$': Potřebujeme dokázat, že souvislý graf s n vrcholy a $n - 1$ hranami neobsahuje kružnici. Opět použijeme indukci podle n, přičemž pro $n = 1$ je tvrzení triviální. Nechť souvislý graf G má $n - 1$ hran. Kdyby stupně všech vrcholů byly větší než 1, pak jejich součet je alespoň $2n$ a počet hran (který je přesně polovinou z tohoto čísla) by byl alespoň n. Proto G musí obsahovat nějaký vrchol stupně nejvýše 1. Stupeň 0 však díky souvislosti můžeme vyloučit. Nechť tedy v je vrchol stupně 1. Graf $G - v$ má $n - 1$ vrcholů, $n - 2$ hran a je souvislý. Podle indukčního předpokladu je to strom. Opětovným přidáním vrcholu v nemůže vzniknout kružnice, takže stromem je i celý graf G. □

Před uvedením poslední charakterizace stromů potřebujeme ještě jeden pojem. Obojí se nám bude hodit později, až budeme hovořit o souvislostech mezi grafy a maticemi.

Definice 7.5 *Faktor* grafu G je libovolný jeho podgraf, jehož množina vrcholů je $V(G)$. Faktor je *vlastní*, je-li různý od grafu G.

Věta 7.6 *Graf G je strom, právě když je souvislý a nemá žádný souvislý vlastní faktor.*

Důkaz. '$\Rightarrow$': Nechť strom G má souvislý vlastní faktor F. Protože $F \neq G$, existuje nějaká hrana $e \in E(G) - E(F)$. Podle věty 6.15 musí $G - e$ být nesouvislý graf, protože G neobsahuje žádnou kružnici. Graf F je ovšem faktorem grafu $G - e$ a musí tak být rovněž nesouvislý. To je spor.

'$\Leftarrow$': Nechť G je graf, který nemá souvislý vlastní faktor. Dejme tomu, že obsahuje kružnici C. Pro $e \in E(C)$ je opět podle věty 6.15 $G - e$ souvislý graf. Jedná se však o vlastní faktor grafu G, a to je spor. Vzhledem k tomu, že souvislost grafu G předpokládáme, je věta dokázána. □

Jak lze zjistit, zda je daný graf G stromem? Stejně jako u testování souvislosti je to patrné 'na první pohled' u malých grafů nakreslených přehledným obrázkem. Představíme-li si však třeba graf s desítkami tisíc vrcholů, navíc zadaný maticí, jak to uvidíme v kapitole 9, pak s prvním pohledem možná nevystačíme. Snadný postup však nabízí věta 7.4, podle níž stačí spočítat, zda má graf $n - 1$ hran, a otestovat, zda je souvislý (např. pomocí Dijkstrova algoritmu, se kterým se seznámíme v oddílu 12.2, nebo algoritmu ze cvičení 6.7). Není tedy potřeba zjišťovat, zda graf G obsahuje nějakou kružnici.

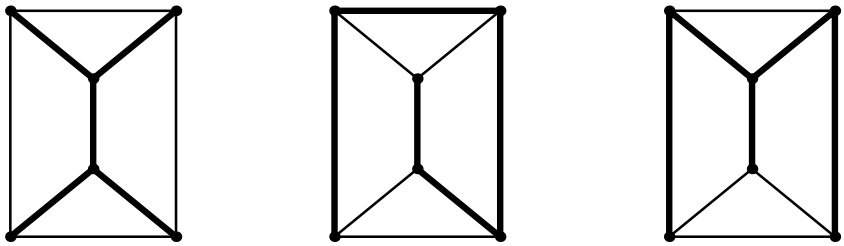
Cvičení

► **7.1** Kolik existuje různých stromů na množině $V = \{1, 2, 3, 4\}$? Kolik existuje navzájem neisomorfních stromů na množině V?

7.2 Kostry

Definice 7.7 *Kostrou* souvislého grafu G je každý jeho faktor, který je stromem. Jinak řečeno, kostra grafu G je souvislý podgraf bez kružnic, který obsahuje všechny vrcholy grafu G.

Obr. 7.2 ukazuje 3 různé kostry téhož grafu. Upozorněme, že dosti častou chybou je záměna pojmů kostra a strom. Rozdíl je ale podstatný: konkrétní graf může nebo nemusí být stromem, ale pojem kostra se vždy váže ještě k dalšímu grafu, např. v otázce 'Je graf G kostrou *grafu* H?'



Obrázek 7.2: Tři kostry téhož grafu (znázorněny tučně).

Má každý graf kostru? Z toho, že každý faktor nesouvislého grafu je nesouvislý, vidíme, že nesouvislý graf žádnou kostru mít nemůže. Na druhou stranu platí následující tvrzení.

Tvrzení 7.8 *Každý souvislý graf má alespoň jednu kostru.*

Důkaz. Nechť $G = (V, E)$ je souvislý graf. Uvažme množinu hran M, která má vlastnost, že

$$\text{faktor } (V, M) \text{ grafu } G \text{ neobsahuje kružnice} \tag{7.1}$$

a je s touto vlastností maximální vzhledem k inkluzi. (Taková množina existuje, protože například i prázdná množina splňuje podmínku (7.1).) Tvrdíme, že faktor (V, M) je souvislý.

Dejme tomu, že to tak není a uvažme komponenty A, B grafu (V, M). V souvislém grafu G mezi A a B jistě vede nějaká hrana e. Přidáním této hrany k množině M kružnice vzniknout nemůže, to by totiž vedlo ke sporu s větou 6.15. Proto množina $M \cup \{e\}$ má rovněž vlastnost (7.1) a dostáváme spor s maximalitou množiny M. □

Stromy a kostry mají řadu praktických aplikací. S některými z nich se v dalším textu seznámíme:

- *binární* a další stromy slouží jako datové struktury algoritmů (oddíly 7.3 a 7.4),

- *minimální kostra* se objevuje v úlohách, kde je cílem najít optimální propojení jistých objektů (oddíl 12.4),
- *rozhodovací strom* se používá k modelování rozhodovacích procesů (je popsán v oddílu 12.5).

Kostry grafů se rovněž uplatňují při analýze elektrických obvodů (tzv. metoda stavových proměnných).

Ve cvičeních k tomuto oddílu je zadáním spočítat kostry různých grafů. K této otázce se vrátíme v kapitole 9, kde odvodíme souvislost mezi počtem koster grafu a determinantem jisté matice.

Cvičení

▶ **7.2** Určete počet koster:

(a) stromu na n vrcholech,

(b) kružnice C_n,

(c) grafu, který vznikne, přidáme-li k C_{2n} tětivu spojující dva vrcholy ve vzdálenosti n.

▶ **7.3** Nechť M_{2n} je graf tvořený n disjunktními hranami na $2n$ vrcholech. Určete počet koster grafu G, který vznikne přidáním nového vrcholu a jeho spojením s každým vrcholem z $V(M_{2n})$. (G je tedy n trojúhelníků slepených "za vrchol".)

▶▶ **7.4** Nechť G je graf na množině vrcholů $\{1,\ldots,n\}\cup\{v,w\}$, v němž je každý vrchol z $\{1,\ldots,n\}$ spojen hranou jak s v, tak s w, a jiné hrany G nemá. Určete

(a) počet koster grafu G,

(b) počet koster grafu $G+vw$, který vznikne z G přidáním hrany vw.

7.3 Binární stromy

Stromy mají široké uplatnění jako datové struktury pro různé algoritmy. Ukážeme si dva příklady použití tzv. binárních stromů. Nejprve jejich definici.

Kořenový strom je dvojice (T,r), kde T je strom a r jeho vrchol, kterému budeme říkat *kořen*. *Hloubka* $h(w)$ vrcholu $w\in V(T)$ je délka cesty $P(w)$ z kořene r do w. Vrchol v je *rodičem* vrcholu w, pokud je jeho sousedem na cestě $P(w)$ (pak také řekneme, že w je *potomkem* vrcholu v). *Binární strom* je kořenový strom, v němž má každý vrchol nejvýše dva potomky a každý potomek je označen jako *levý* nebo *pravý*. Žádný rodič samozřejmě nemá dva potomky stejného typu.

(a) (b)

Obrázek 7.3: Binární stromy.

V obvyklém znázornění binárního stromu je kořen nahoře a levý resp. pravý potomek na příslušné straně pod svým rodičem. Příklady binárních stromů jsou na obr. 7.3.

Binární stromy se dobře hodí k reprezentaci lineárních uspořádání. Dejme tomu, že potřebujeme implementovat algoritmus, který pracuje s abecedně seřazeným seznamem n osob, přičemž každé osobě odpovídá nějaký záznam. Seznam je obsáhlý a vzhledem k častým přístupům potřebujeme, aby čas nutný k nalezení konkrétního záznamu byl co nejmenší. Jako ilustraci použijme jména z jednoho únorového týdne v kalendáři. (Každý záznam obsahuje ještě další informace, kvůli kterým se vlastně vyhledávání provádí. Pro náš výklad však nejsou důležité.)

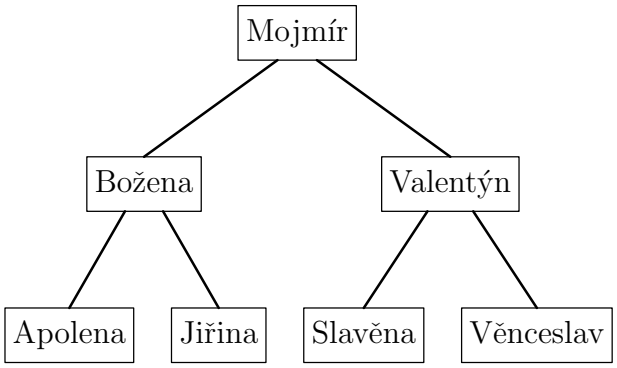
Apolena	Božena	Jiřina	Mojmír	Slavěna	Valentýn	Věnceslav
...	...	...	...	...	...	...

Jak efektivně najít záznam odpovídající určitému jménu? Jednou možností je procházet záznamy od začátku jeden po druhém a hledat ten správný. Pak ovšem v nejhorším případě musíme projít všech n záznamů (a v průměru $n/2$ záznamů).

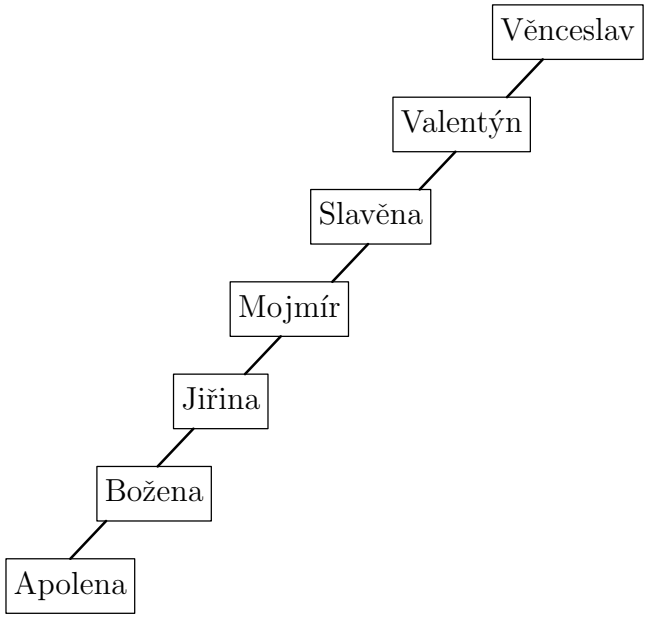
Tento čas však lze výrazně zkrátit s použitím vyhledávacího stromu. *Binární vyhledávací strom* pro lineárně uspořádanou množinu $(X, \leq)$ je binární strom, jehož vrcholy jsou prvky množiny X a v němž pro každý vrchol v platí, že je-li ℓ levý potomek vrcholu v, pak $\ell < v$, a podobně pro pravého potomka p vrcholu v je $p > v$. (Adjektivum *binární* budeme pro stručnost vynechávat.) V našem příkladu je množinou X množina záznamů, uspořádaná podle abecedy. Příklad vyhledávacího stromu pro množinu X je na obr. 7.4.

Označme jméno příslušné vrcholu v symbolem $a(v)$. Jak se v našem stromu vyhledá záznam pro konkrétní jméno x? Začneme od kořene r a porovnáme slova x a $a(r)$ (v abecedním uspořádání). Je-li $x = a(r)$, našli jsme hledaný záznam. Pokud $x < a(r)$, přejdeme k levému potomku vrcholu r, jinak k pravému potomku. Test se opakuje až do nalezení shody.

Ve stromu na obr. 7.4 lze libovolný záznam vyhledat nejvýše ve třech krocích. Bez použití vyhledávacího stromu bychom k vyhledání jména Věnceslav potřebovali 7 kroků. Ne každý vyhledávací strom pro danou množinu nám však nabízí takové zlepšení. Například u stromu na obr. 7.5 potřebujeme v nejhorším případě rovněž 7 kroků.



Obrázek 7.4: Vyhledávací strom pro množinu záznamů.



Obrázek 7.5: Jiný vyhledávací strom.

Kolik kroků tedy trvá vyhledání záznamu v obecném vyhledávacím stromu? Definujme *hloubku* vyhledávacího stromu T jako maximální hloubku $h(v)$ nějakého jeho vrcholu (připomeňme, že hloubka vrcholu je definována na začátku tohoto oddílu). K vyhledání záznamu ve stromu hloubky d je pak v nejhorším případě potřeba d kroků.

Pro danou uspořádanou množinu ale máme na výběr z mnoha stromů. Jaké nejmenší hloubky lze dosáhnout? Řekneme, že *vyhledávací* strom pro množinu X je *optimální*, má-li mezi všemi vyhledávacími stromy pro X minimální hloubku.

Věta 7.9 *Hloubka $h(n)$ optimálního vyhledávacího stromu pro n-prvkovou množinu X je*

$$h(n) = \lceil \log_2(n+1) \rceil - 1, \tag{7.2}$$

kde $\lceil \log_2(\dots) \rceil$ označuje horní celou část z dvojkového logaritmu.

Důkaz. Nejprve dokažme, že $h(n)$ je větší nebo rovno výrazu na pravé straně nerovnosti (7.2). Nechť T je libovolný binární strom na n vrcholech. Označme jeho hloubku d. Pro $0 \leq i \leq d$ je počet vrcholů stromu T s hloubkou rovnou i nejvýše 2^i. Odtud

$$n \leq 2^0 + 2^1 + \cdots + 2^d = 2^{d+1} - 1,$$

takže $d \geq log_2(n+1) - 1$. Protože d je celé číslo, platí dokonce $d \geq \lceil log_2(n+1) - 1 \rceil$. Splňuje-li tuto nerovnost hloubka každého stromu na n vrcholech, musí platit i (7.2).

V opačném směru potřebujeme zkontruovat vyhledávací strom pro množinu X, jehož hloubka bude rovna pravé straně nerovnosti (7.2). Nejprve najdeme strom S, ve kterém

$$\text{každý vrchol o hloubce nejvýše } h(S) - 2 \text{ má oba potomky,} \tag{7.3}$$

a potom ukážeme, že strom S má požadovanou vlastnost.

Označme $X = \{x_1, \dots, x_n\}$, kde $x_1 < \cdots < x_n$. Je-li $n \leq 2$, pak snadno najdeme strom pro X s hloubkou 0 nebo 1, který triviálně splňuje podmínku (7.3). Pro větší n za kořen stromu S zvolme *medián* posloupnosti $x_1, \dots, x_n$, tj. prvek x_m, kde $m = \lceil n/2 \rceil$ (medián je obecně prostřední prvek monotónní posloupnosti). Pro uspořádané množiny $X_1 = \{x_1, \dots, x_{m-1}\}$ a $X_2 = \{x_{m+1}, \dots, x_n\}$ rekurzívním způsobem zkonstruujme binární vyhledávací stromy S_1 a S_2 s vlastností (7.3). Strom S získáme tak, že levým potomkem kořene x_m učiníme kořen stromu S_1 a pravým potomkem kořen stromu S_2. Vidíme, že podmínka (7.3) zůstane zachována.

Zbývá určit hloubku $d = h(S)$ stromu S. Z podmínky (7.3) plyne, že pro $0 \leq i \leq d-1$ obsahuje strom S přesně 2^i vrcholů o hloubce i. Má tedy přesně

$$1 + 2 + 2^2 + \cdots + 2^{d-1} = 2^d - 1$$

vrcholů o hloubce menší než d. Z definice navíc musí obsahovat alespoň jeden vrchol o hloubce d, takže

$$n \geq 2^d.$$

Po přičtení jedničky k oběma stranám a zlogaritmování snadno zjistíme, že platí

$$d \leq \lceil \log_2(n+1) \rceil - 1,$$

čímž je důkaz hotov. □

Důsledkem věty 7.9 je, že s použitím vhodného vyhledávacího stromu lze v n-prvkové uspořádané množině vyhledávat v počtu kroků, který je omezen *logaritmickou* funkcí n. (S použitím formalismu z oddílu 6.7 bychom řekli, že počet kroků je $O(\log n)$.) Oproti *lineárnímu* počtu kroků bez použití vyhledávacího stromu jde o značné zlepšení.

V našem příkladu předpokládáme, že vyhledávací strom je *statický*: stačí jej jednou zkonstruovat a již se nemění. Existují také algoritmy, pomocí kterých lze do vyhledávacích stromů přidávat vrcholy nebo je odebírat, a to při zachování efektivity daného stromu. Více se o těchto tématech lze dozvědět např. v knize [2].

Cvičení

►► **7.5** (a) Určete součet

$$\sum_{k=1}^{n} k \cdot 2^k.$$

(b) Vyhledávací strom T o hloubce d je *úplný*, pokud všechny listy mají hloubku d a každý ostatní vrchol má 2 potomky. Kolik vrcholů má takový strom?

(c) S použitím části (a) spočítejte *průměrný* počet kroků potřebný k vyhledání záznamu v úplném vyhledávacím stromu o hloubce d. (Průměr se počítá přes všechny vrcholy stromu.)

7.4 Huffmanovo kódování

Dostáváme se k další aplikaci binárních stromů, k tzv. Huffmanovu[1] kódování. Nechť je dána konečná *abeceda* Σ. Její prvky budeme nazývat *symboly*. Naším cílem bude zakódovat každý symbol *binárním řetězcem* (posloupností nul a jedniček, tzv. *bitů*), tak, aby bylo splněno několik podmínek, k jejichž zformulování se dostaneme za chvíli. *Kódování* pro abecedu Σ je prostá funkce, která přiřazuje každému symbolu a konečnou posloupnost $c(a)$ symbolů 0 a 1 (*kód symbolu* a).

[1] David A. Huffman (1905–1999).

Nechť je pevně zvoleno kódování c. Pak lze definovat i kód posloupnosti symbolů $a_1 \dots a_k$, a to jako zřetězení kódů

$$c(a_1) \dots c(a_k).$$

Je z tohoto kódu možné rekonstruovat původní posloupnost $a_1 \dots a_k$? Ne vždy. Uvažme například abecedu $\Sigma = \{X, Y, Z\}$ s následujícím kódováním:

symbol	X	Y	Z
kód	0	1	01

Pak např. posloupnosti Z a XY mají stejný kód 01. Této situaci bychom se chtěli vyhnout. To se nám podaří například tehdy, když bude naše kódování *prefixové*, tj. když kód žádného symbolu nebude počátečním úsekem ('prefixem') kódu žádného jiného symbolu.

Pozorování 7.10 *Prefixové kódování přiřazuje různým posloupnostem symbolů různé kódy.*

Důkaz. Cvičení 7.6. □

Prefixové kódování se dá najít snadno: stačí symbolům přiřadit různé kódy stejné délky ℓ.

Nyní se dostáváme k dalšímu požadavku: chtěli bychom minimalizovat průměrnou délku kódu přiřazeného symbolu abecedy Σ. Předpokládáme přitom, že každý symbol a má určenou *váhu* $w(a)$, na kterou se můžeme dívat jako na poměrnou četnost symbolu a v 'typickém textu' nad abecedou Σ, a která se bere v úvahu při výpočtu uvedeného průměru.

Jinak řečeno, označíme-li délku binárního řetězce r symbolem $|r|$, budeme chtít, aby *vážená délka* kódování c,

$$\mathrm{vd}(c) = \sum_{a \in \Sigma} w(a) \cdot |c(a)|, \tag{7.4}$$

byla co nejmenší.

Kódování c pro abecedu Σ je *optimální*, pokud je prefixové a má mezi všemi prefixovými kódováními pro Σ nejmenší váženou délku.

Uvažme jako jednoduchý příklad abecedu $\Sigma = \{A, B, C, D\}$. Jsou-li všechny váhy stejné, pak nelze počítat s lepším řešením, než je kódování s kódy 00, 01, 10 a 11 a s váženou délkou 2 (obecně pro n-prvkovou abecedu bychom potřebovali $\lceil \log_2 n \rceil$ bitů). Předpokládejme ovšem, že symboly mají následující váhy:

symbol	A	B	C	D
váha	0.6	0.3	0.05	0.05

(7.5)

Pak není vyloučeno, že se nám na vážené délce podaří ušetřit, pokud častému symbolu A přiřadíme nejkratší možný kód, i za ceny prodloužení kódů málo frekventovaných symbolů C a D. Skutečně, například kódování

symbol	A	B	C	D
kód	0	10	110	111

je prefixové a jeho vážená délka je pouze

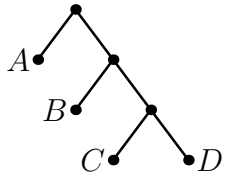
$$1.5 = 0.6 \times 1 + 0.3 \times 2 + 0.05 \times 3 + 0.05 \times 3.$$

S tímto kódováním tedy na jeden symbol potřebujeme průměrně pouze 1.5 bitu! Dá se ukázat, že je to optimální kódování.

Prefixová kódování mají úzký vztah k binárním stromům. Nechť T je binární strom, jehož listům jsou vzájemně jednoznačně přiřazeny symboly z abecedy Σ. Označme list odpovídající symbolu $a \in \Sigma$ jako ℓ_a. Strom T určuje kódování pro abecedu Σ, a to následujícím způsobem. Určíme kód $c(a)$ symbolu $a \in \Sigma$. Označme vrcholy na cestě $P(\ell_a)$ v pořadí od kořene jako $r = v_0, v_1, \ldots, v_d = \ell_a$. Hledaný kód pak bude posloupnost $c(a) = (b_1, \ldots, b_d)$, kde d je hloubka listu ℓ_a, všechny b_i jsou z množiny $\{0, 1\}$ a

$$b_i = 0 \iff \text{vrchol } v_i \text{ je levým potomkem vrcholu } v_{i-1}.$$

V opačném směru lze pro každé prefixové kódování sestrojit odpovídající binární strom (viz cvičení 7.11). Například našemu optimálnímu kódování pro abecedu $\{A, B, C, D\}$ odpovídá strom na obr. 7.6. Pokusme se přeformulovat úlohu hledání optimálního kódování v řeči binárních stromů.



Obrázek 7.6: Binární strom odpovídající optimálnímu kódování pro abecedu $\{A, B, C, D\}$ s váhami 7.5.

Optimální strom pro abecedu $\Sigma = \{a_1, \ldots, a_n\}$ s váhami $w(a_i)$ je binární strom T s listy $\ell_1, \ldots, \ell_n$, jehož *průměrná vážená hloubka* $\mathrm{vh}(T)$, definovaná předpisem

$$\mathrm{vh}(T) = \sum_{i=1}^{n} w(a_i) \cdot h(\ell_i),$$

je nejmenší možná. Je jasné, že optimálnímu stromu odpovídá optimální kódování pro abecedu Σ s danými váhami. (Pozor na rozdíl mezi pojmem 'optimální strom' a termínem 'optimální vyhledávací strom' z oddílu 7.3.)

Než popíšeme Huffmanův algoritmus pro nalezení optimálního stromu, zaveďme ještě dvě definice. Vrchol v binárního stromu T je *následovníkem* vrcholu u, pokud u leží na cestě $P(v)$. Speciálně je tedy každý vrchol svým vlastním následovníkem. *Levý (pravý) podstrom* pod vrcholem v je indukovaný podgraf stromu T na množině všech následovníků levého (pravého) potomka vrcholu v.

Vstupem *Huffmanova algoritmu* je abeceda $\Sigma = \{a_1, \ldots, a_n\}$ spolu s přiřazením vah $w(a_i)$ symbolům $a_i \in \Sigma$. Jeho výstupem je (některý) optimální strom H pro abecedu Σ, tzv. *Huffmanův strom*. Příslušné kódování se označuje jako *Huffmanovo kódování*.

Algoritmus pracuje s posloupností kořenových stromů s váženými listy, která se v každém kroku mění. Výchozí posloupnost $P_0 = (T_1, \ldots, T_n)$ je tvořena triviálními stromy T_i o jediném vrcholu a_i s vahou $w(a_i)$.

Algoritmus skončí, až bude naše pracovní posloupnost obsahovat jediný strom, a tím bude hledaný Huffmanův strom H. Popišme k-tý krok algoritmu. Váha $w(T)$ libovolného stromu T je definována jako součet vah jeho listů.

Najdeme v pracovní posloupnosti P_{k-1} dvojici stromů s minimálním součtem vah. Takových dvojic může být více; abychom se vyhnuli nejednoznačnosti, definujme množinu uspořádaných dvojic

$$M_{k-1} = \{(s,t) : s < t \text{ a součet } w(T_s) + w(T_t) \text{ je minimální možný}\}$$

a najděme v ní nejmenší prvek (i,j) v lexikografickém uspořádání (viz cvičení 3.2). Posloupnost P_k vznikne z posloupnosti P_{k-1} následovně:

(1) vypustíme strom T_j,

(2) nahradíme strom T_i stromem, jehož kořenem je nově přidaný vrchol v_k, levým podstromem pod kořenem je T_i a pravým podstromem pod kořenem je T_j (váhy na listech zůstávají beze změny).

Vidíme, že počet prvků pracovní posloupnosti stromů se provedením k-tého kroku snížil o 1. Algoritmus tedy skončí po $p-1$ krocích.

Ilustrujme jeho průběh na příkladu. Nechť jsou pro abecedu

$$\Sigma = \{A, E, G, I, L, R\}$$

určeny tyto váhy:

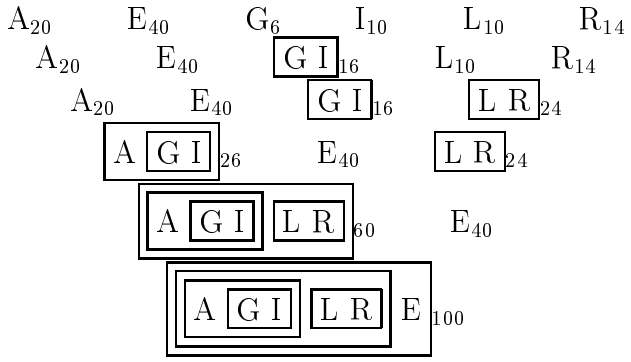
symbol	A	E	G	I	L	R
váha	0.2	0.4	0.06	0.1	0.1	0.14

(7.6)

Najdeme Huffmanův strom pro tuto abecedu.

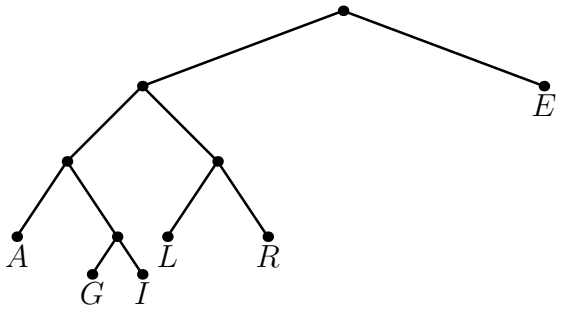
V následujícím schématickém znázornění průběhu Huffmanova algoritmu každý řádek zachycuje stav pracovní posloupnosti stromů v příslušném kroku. Písmena odpovídají stromům na jednom vrcholu. Strom S na více vrcholech je znázorněn symbolem $\boxed{S_1 S_2}$, kde S_1 (resp. S_2) je levý (resp. pravý) podstrom pod

kořenem stromu S. Prvky posloupnosti jsou odděleny mezerami, čísla udávají váhu daného stromu, pro přehlednost násobenou stem.



Výsledný Huffmanův strom (který odpovídá poslednímu řádku v tomto zápisu) je na obr. 7.7. Našli jsme tedy následující optimální kód:

symbol	A	E	G	I	L	R
kód	000	1	0010	0011	010	011



Obrázek 7.7: Huffmanův strom pro abecedu s váhami (7.6).

Pomocí této tabulky není problém zakódovat libovolné slovo v abecedě Σ. Například kód slova ALERGIE je 0000101011001000111.

Korektnost Huffmanova algoritmu zaručuje následující věta, jejíž důkaz ponecháváme jako (těžší) problém na cvičení 7.12.

Věta 7.11 *Nechť $\Sigma = \{a_1, \ldots, a_n\}$ je abeceda s váhami $w(a_i)$. Strom zkonstruovaný Huffmanovým algoritmem je optimálním stromem pro tuto abecedu.* □

Cvičení

▶ **7.6** Dokažte pozorování 7.10.

▶ **7.7** Určete průměrnou váženou hloubku $\mathrm{vh}(T)$ stromu na obr. 7.7.

► **7.8** Zakódujte pomocí Huffmanova kódování z našeho příkladu slova ELEGIE a LILIE. Vyplatí se pro tato slova Huffmanovo kódování použít? Proč?

► **7.9** Určete slovo, jehož Huffmanův kód v kódování z našeho příkladu je

$$01000110010000.$$

► **7.10** Najděte Huffmanův strom pro abecedu $\{A, B, C, D, E\}$ s váhami

symbol	A	B	C	D	E
váha	0.1	0.15	0.5	0.1	0.15

a určete jeho průměrnou váženou hloubku.

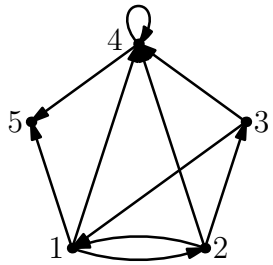
► **7.11** Ukažte, že prefixová kódování pro abecedu Σ jsou ve vzájemně jednoznačném vztahu s binárními stromy, jejichž listy jsou označeny symboly abecedy Σ.

►► **7.12** Dokažte větu 7.11.
[*Nápověda.* Nechť a_i, a_j jsou dva symboly s minimální vahou. Ukažte, že pro abecedu Σ existuje optimální strom, ve kterém symboly a_i a a_j mají stejného předchůdce. Z tohoto lemmatu plyne věta 7.11 indukcí přes n.]

Kapitola 8

Orientované grafy

V této kapitole se budeme zabývat grafy, v nichž má každá hrana určený směr — tzv. orientovanými grafy. Směr (orientace) hran se obvykle znázorňuje šipkami jako na obr. 8.1.



Obrázek 8.1: Orientovaný graf.

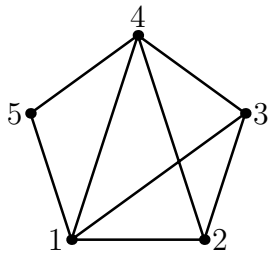
8.1 Definice orientovaných grafů

Definice 8.1 *Orientovaný graf* je dvojice (V, E), kde V je množina vrcholů a $E \subset V \times V$ je množina hran.

Všimněme si, že hrany jsou nyní prvky kartézského součinu $V \times V$, a tedy *uspořádané* dvojice vrcholů. (Orientovaný graf je tedy vlastně totéž, co binární relace na množině V.) Dvojici (u, v) interpretujeme jako hranu, která začíná ve vrcholu u a končí ve vrcholu v. Podle definice může být hranou i dvojice (v, v). Naše orientované grafy tedy mohou mít smyčky. Násobné hrany ve shodném směru nadále nepovolujeme (graf ale může obsahovat dvojici 'protichůdných' hran mezi dvěma vrcholy). Podobně jako u neorientovaných grafů budeme dvojici (u, v) zapisovat prostě jako uv.

Pojmy *podgraf* a *indukovaný podgraf* jsou definovány jako u neorientovaných grafů. Z orientovaného grafu G můžeme snadno vyrobit neorientovaný graf

(tzv. *symetrizaci* grafu G) tak, že 'zapomeneme' orientace všech hran. Případné smyčky odstraníme a násobné hrany nahradíme jednoduchými. (Viz obr. 8.2.) Některé pojmy týkající se neorientovaných grafů tak lze přímo aplikovat na grafy orientované. Řekneme například, že graf G je *(slabě) souvislý*, je-li jeho symetrizace souvislá. *Komponenty* orientovaného grafu G jsou (analogicky k situaci u neorientovaných grafů) maximální slabě souvislé podgrafy. Přesněji řečeno, komponenta je slabě souvislý indukovaný podgraf s vlastností, že žádný indukovaný podgraf na větší množině vrcholů není slabě souvislý.



Obrázek 8.2: Symetrizace grafu z obr. 8.1.

V opačném směru, u přechodu od neorientovaného grafu k orientovanému, máme řadu možností, jak hrany opatřit šipkami. Řekneme, že orientovaný graf G je *orientací* grafu H, je-li H symetrizací orientovaného grafu G. Každý neorientovaný graf má tedy řadu orientací. Orientovaný graf na obr. 8.1 je například jednou z orientací grafu na obr. 8.2.

Definice 8.2 *Vstupní stupeň* $d^+_G(u)$ vrcholu u orientovaného grafu $G = (V, E)$ je počet hran, které končí ve vrcholu u, tedy počet dvojic xu (kde $x \in V$) v množině hran E. Podobně *výstupní stupeň* $d^-_G(u)$ je počet dvojic ux v množině hran.

Cvičení

▶ **8.1** Dokažte, že v orientovaném grafu $G = (V, E)$ s m hranami platí

$$\sum_{v \in V} d^+_G(v) = \sum_{v \in V} d^-_G(v) = m.$$

8.2 Silná souvislost

Pro orientované grafy lze snadno upravit definice pojmů sled, cesta v grafu a kružnice v grafu. Znění definic je vlastně téměř stejné, jediný rozdíl je v tom, že každý krok sledu musí nyní respektovat orientaci příslušné hrany. Místo pojmu 'kružnice' používáme u orientovaných grafů termínu 'cyklus'.

Definice 8.3 *Orientovaný sled* z vrcholu x do vrcholu y v orientovaném grafu G je posloupnost vrcholů $(x = v_0, v_1, \ldots, v_k = y)$, ve které je pro každé $i = 1, \ldots, k$ dvojice $v_{i-1}v_i$ hranou grafu G. *Orientovaná cesta* v G je orientovaný sled, který obsahuje každý vrchol nejvýše jednou. *Cyklus* v G je orientovaný sled, ve kterém je $v_0 = v_k$, tento vrchol je v něm obsažen právě dvakrát a všechny ostatní nejvýše jednou.

Graf G na obr. 8.1 obsahuje například sled $(3, 1, 2, 3, 4, 4)$, naopak posloupnost $(4, 3, 2, 1)$ sledem není. Tento graf obsahuje také cykly $(1, 2, 3, 1)$, $(4, 4)$ (délka tohoto cyklu je 1) a $(1, 2, 1)$.

Slabá souvislost nám neříká mnoho o existenci orientovaných cest v daném grafu. U orientovaných grafů je proto často přirozenější pracovat se silnější variantou pojmu souvislost.

Definice 8.4 Orientovaný graf G je *silně souvislý*, pokud v něm pro každou dvojici vrcholů x, y existuje orientovaná cesta z x do y i orientovaná cesta z y do x,

Následující věta charakterizuje silně souvislé grafy. Jak je asi zřejmé, říkáme, že hrana xy je obsažena v cyklu $(v_0, v_1, \ldots, v_k = x_0)$, pokud pro nějaké i je $x = v_i$ a $y = v_{i+1}$.

Věta 8.5 *Slabě souvislý orientovaný graf je silně souvislý, právě když každá jeho hrana je obsažena v nějakém cyklu.*

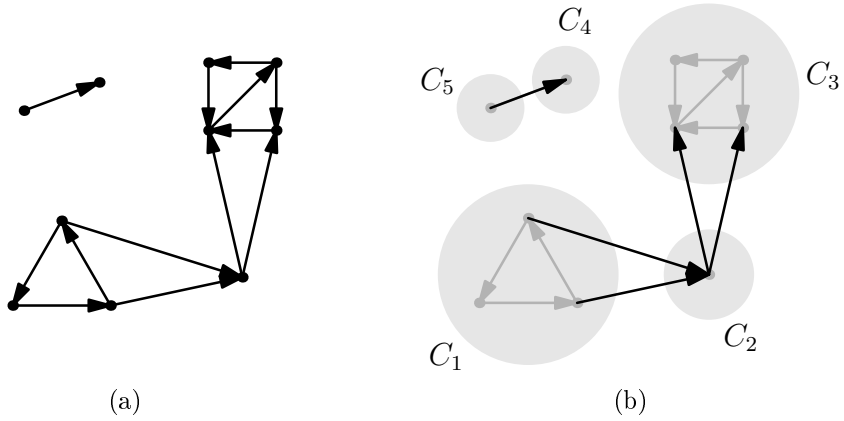
Důkaz. '$\Rightarrow$': Uvažme hranu xy orientovaného grafu G. Ze silné souvislosti plyne existence cesty P z y do x. Připojením hrany xy za tuto cestu vznikne cyklus, který hranu xy obsahuje.

'$\Leftarrow$': Nechť x, y je libovolná dvojice vrcholů, a nechť Q je cesta z x do y v symetrizaci slabě souvislého orientovaného grafu G. Cesta Q je tedy posloupnost vrcholů $(x = q_0, q_1, \ldots, q_k = y)$, kde pro $i = 1, \ldots, k$ je buď $q_{i-1}q_i \in E(G)$ (a řekneme, že jde o dobře orientovanou hranu cesty Q) nebo $q_{i-1}q_i \notin E(G)$ a $q_iq_{i-1} \in E(G)$ (špatně orientovaná hrana). Každá špatně orientovaná hrana q_iq_{i-1} je obsažena v cyklu; speciálně existuje orientovaná cesta R_i z q_{i-1} do q_i. Nahradíme-li v cestě Q každou špatně orientovanou hranu příslušnou cestou R_i, získáme orientovaný sled z x do y. Podle cvičení 8.3 tedy existuje orientovaná cesta z x do y. Vzhledem k tomu, že dvojice x, y byla libovolná, graf je silně souvislý. □

Definujme na vrcholech orientovaného grafu G *relaci oboustranné dosažitelnosti* $\sim$: pro vrcholy x, y platí $x \sim y$, pokud v G existuje orientovaná cesta z x do y i naopak. S použitím cvičení 8.3 je snadné dokázat, že tato relace je ekvivalencí. Tento fakt můžeme použít v definici tzv. kvazikomponent, které jsou obdobou komponent pro silnou souvislost. K jejímu pochopení může pomoci vrátit se k definici pojmu komponenta v kapitole 5.

Definice 8.6 *Kvazikomponenta* orientovaného grafu G je každý jeho indukovaný podgraf na množině vrcholů, která tvoří některou z tříd ekvivalence $\sim$.

Definici ilustruje graf na obr. 8.3(a) s 2 komponentami a celkem 5 kvazikomponentami, znázorněnými na obr. 8.3(b). Podobně orientovaný graf na obr. 8.1 má tři kvazikomponenty, jejichž množiny vrcholů jsou $\{1,2,3\}, \{4\}$ a $\{5\}$.



Obrázek 8.3: Orientovaný graf a jeho kvazikomponenty.

Cvičení

► **8.2** Najděte příklad slabě souvislého orientovaného grafu na 6 vrcholech, který má 3 kvazikomponenty.

► **8.3** Dokažte, že v orientovaném grafu existuje orientovaná cesta z vrcholu x do vrcholu y, právě když v něm existuje orientovaný sled z x do y.

► **8.4** Dokažte, že kvazikomponenty orientovaného grafu G jsou právě jeho maximální silně souvislé podgrafy — jinými slovy, jsou to právě ty podgrafy H, pro které platí, že je-li H vlastním podgrafem jiného grafu $K \subset G$, pak K není silně souvislý.

► **8.5** Formulujte algoritmus na nalezení kvazikomponent orientovaného grafu.

8.3 Acyklické orientované grafy

Definice 8.7 Orientovaný graf je *acyklický*, pokud neobsahuje žádný cyklus.

Slabě souvislé acyklické orientované grafy jsou tedy z jistého hlediska obdobou stromů, tj. souvislých grafů, které neobsahují žádnou kružnici.

Definice 8.8 *Vstupní vrchol* orientovaného grafu G je vrchol, jehož vstupní stupeň $d_G^+(v)$ je nulový. Podobně *výstupní vrchol* je vrchol, pro který je $d_G^-(v) = 0$.

Acyklické grafy lze charakterizovat z hlediska existence vstupních vrcholů v jejich podgrafech.

Věta 8.9 *Orientovaný graf G s konečnou množinou vrcholů je acyklický, právě když každý jeho neprázdný podgraf $H \subset G$ obsahuje vstupní vrchol.*

Důkaz. '$\Rightarrow$': Zvolme vrchol v_0. Není-li vstupní, vede do něj nějaká hrana, dejme tomu z vrcholu v_1. Opakováním této úvahy získáme nejvýše po $n+1$ krocích (kde n je počet vrcholů) buďto vstupní vrchol. nebo posloupnost $n+1$ vrcholů $(v_0, v_1, \ldots, v_n)$, ve které se musí některý vrchol vyskytovat dvakrát, řekněme $v_i = v_j$ a $i < j$. Ve druhém případě by ale podposloupnost $v_j, v_{j-1}, \ldots, v_i$ byla cyklem v acyklickém grafu G.

'$\Leftarrow$': Předpokládejme existenci vstupních vrcholů a dokažme, že orientovaný graf G je acyklický. Nechť obsahuje cyklus C. Tento cyklus určuje podgraf H grafu G, sestávající z hran a vrcholů, kterými C prochází. Všechny vstupní i výstupní stupně v podgrafu H jsou rovny jedné. To je spor. □

Lze očekávat, že podobný výsledek platí i pro výstupní vrcholy.

Důsledek 8.10 *Orientovaný graf G je acyklický, právě když v každém jeho neprázdném podgrafu $H \subset G$ existuje výstupní vrchol.*

Důkaz. Otočíme-li směr každé hrany grafu G, acykličnost zůstane zachována a vstupní vrcholy přecházejí na výstupní a naopak. □

Následující věta charakterizuje acyklické grafy jako takové, na nichž existuje uspořádání vrcholů konzistentní se směry všech hran.

Věta 8.11 *Orientovaný graf G je acyklický, právě když jeho vrcholy lze seřadit do posloupnosti $(v_1, \ldots, v_n)$ tak, že pro každou hranu v_iv_j grafu G platí $i < j$.*

Důkaz. '$\Rightarrow$': Položme $G_1 = G$. Podle věty 8.9 existuje vstupní vrchol v_1 acyklického orientovaného grafu G_1. Nechť $G_2 = G_1 - v_1$ je orientovaný graf vzniklý odstraněním vrcholu v_1 (a všech hran, které ho obsahují). To je podgraf grafu G, a má tedy vstupní vrchol v_2. Opakováním tohoto postupu dostaneme posloupnost vrcholů $(v_1, \ldots, v_n)$. Dejme tomu, že $v_iv_j \in E(G)$, ale přitom $i > j$. Pak ale $v_i \in V(G_j)$ a kvůli hraně v_iv_j nemůže v_j být vstupním vrcholem grafu G_j, což je spor.

'$\Leftarrow$': Mějme vrcholy seřazeny do posloupnosti s uvedenou vlastností a předpokládejme, že G obsahuje cyklus $(v_{i_0}, v_{i_1}, \ldots, v_{i_{k-1}}, v_{i_k} = v_{i_0})$. Pak platí, že $v_{i_0}v_{i_1} \in E(G)$ a tedy $i_0 < i_1$. Obecněji dostáváme

$$i_0 < i_1 < i_2 < \cdots < i_{k-1} < i_0,$$

což není možné. Tím je důkaz hotov. □

V důkazu věty 8.11 se vlastně skrývá efektivní algoritmus pro test acykličnosti orientovaného grafu $G = G_1$. V jeho i-tém kroku postupujeme následovně:

(1) Je-li G_i graf na jediném vrcholu, algoritmus končí. Graf G je acyklický.

(2) Pokud graf G_i obsahuje nějaký vstupní vrchol v_i, položíme $G_{i+1} = G_i - v_i$ a pokračujeme krokem $i + 1$.

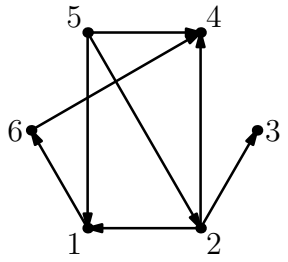
(3) V opačném případě graf G není acyklický a algoritmus končí.

V každém z $O(n)$ kroků tohoto algoritmu je potřeba najít vstupní vrchol v grafu o nejvýše n vrcholech. Při použití postupu, který plyne z důkazu věty 8.9, lze vstupní vrchol najít v čase $O(n)$. Celková časová složitost popsaného algoritmu je tedy $O(n^2)$.

Cvičení

► **8.6** Najděte pro acyklický orientovaný graf na obr. 8.4 posloupnost vrcholů splňujících podmínku věty 8.11.

► **8.7** Najděte (nekonečný) acyklický orientovaný graf, který neobsahuje výstupní vrchol.



Obrázek 8.4: Acyklický orientovaný graf.

8.4 Tranzitivní uzávěr

Víme již, že orientované grafy s množinou vrcholů V jednoznačně odpovídají binárním relacím na množině V (viz cvičení 8.8).

Definice 8.12 *Tranzitivní uzávěr* orientovaného grafu G je orientovaný graf G^+ takový, že $V(G^+) = V(G)$ a

$$xy \in E(G^+), \text{ pokud } \begin{cases} x \neq y & \text{a v } G \text{ existuje orientovaná cesta z } x \text{ do } y, \\ x = y & \text{a vrchol } x \text{ leží na nějakém cyklu v } G. \end{cases}$$

Všimněme si, že graf G je podgrafem grafu G^+ a že G je acyklický, právě když G^+ neobsahuje žádnou smyčku. Následující věta charakterizuje acyklické grafy jako grafy, jejichž (mírně rozšířený) tranzitivní uzávěr je grafem uspořádání na $V(G)$.

Věta 8.13 *Orientovaný graf $G = (V, E)$ bez smyček je acyklický, právě když graf G^*, vzniklý přidáním všech smyček k tranzitivnímu uzávěru G^+, je grafem uspořádání (tj. $E(G^*)$ je relace uspořádání na $V(G^*) = V(G)$).*

Důkaz. '$\Rightarrow$': Nechť G je acyklický. Díky přidaným smyčkám je $E(G^*)$ reflexívní relace. Je také slabě antisymetrická, neboť $xy \in E(G^*)$ a $yx \in E(G^*)$ by pro různé x, y znamenalo, že G obsahuje orientovaný sled z x do y i naopak. Uvažme podgraf H složený z vrcholů a hran obou těchto sledů; v tomto podgrafu je vstupní stupeň každého vrcholu aspoň 1. Neobsahuje tedy vstupní vrchol, což je ve sporu s větou 8.9.

'$\Leftarrow$': Nechť $E(G^*)$ je uspořádání. Pro názornost zapisujme $xy \in E(G^*)$ jako $x \leq y$. Předpokládejme, že G obsahuje cyklus $C = (x_0, x_1, \ldots, x_k = x_0)$. Pak pro každé $i = 0, \ldots, k-1$ platí $x_i x_{i+1} \in E(G)$, jinak řečeno $x_i \leq x_{i+1}$. Z tranzitivity je tedy $x_0 \leq x_{k-1}$. Víme však, že také $x_{k-1}x_0 \in E(G)$, takže $x_{k-1} \leq x_0$. Z antisymetričnosti relace $E(G^*)$ musí být $x_0 = x_{k-1}$. Cyklus C má tedy délku 1 a musí to být smyčka. To je spor s předpokladem, že G je bez smyček. □

Cvičení

► **8.8** Nechť $G = G(R)$ je orientovaný graf binární relace R na množině V. Jak z grafu G poznáme, zda je relace R:

(a) reflexívní,

(b) symetrická,

(c) antisymetrická?

► **8.9** Formulujte algoritmus pro nalezení tranzitivního uzávěru orientovaného grafu.

8.5 Kondenzace

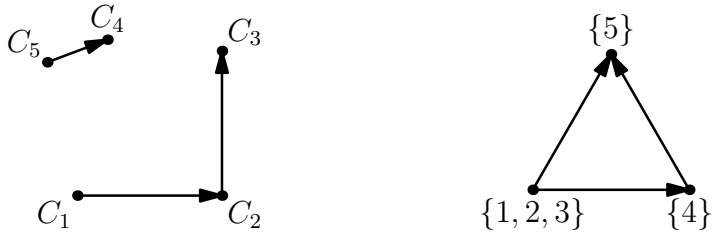
Definice 8.14 *Kondenzace* orientovaného grafu G je orientovaný graf G_c, jehož vrcholy jsou kvazikomponenty grafu G, a pro různé kvazikomponenty $Q_1, Q_2 \in V(G_c)$ platí

$$Q_1Q_2 \in E(G_c), \text{ pokud pro nějaké } x_1 \in V(Q_1), x_2 \in V(Q_2) \text{ je } x_1x_2 \in E(G).$$

Kondenzaci si lze představit také tak, že každou kvazikomponentu grafu G 'stáhneme' do jediného vrcholu; hrany, které vedly mezi různými kvazikomponentami, nyní povedou mezi těmito novými vrcholy. Vynecháme ovšem smyčky. V případě, že mezi dvěma vrcholy povede více hran v témže směru, nahradíme je jedinou hranou.

Vezměme jako příklad opět graf na obr. 8.3. Víme, že má pět kvazikomponent $C_1, \ldots, C_5$. Jeho kondenzací je orientovaný graf na obr. 8.5a.

Kondenzace grafu G z obr. 8.1 je znázorněna na obr. 8.5b. U každého vrcholu je zde uvedena množina vrcholů příslušné kvazikomponenty grafu G.



Obrázek 8.5: Kondenzace (a) grafu z obr. 8.3, (b) grafu z obr. 8.1.

Věta 8.15 (Věta o kondenzaci) *Pro orientovaný graf G platí:*

(i) G_c je acyklický orientovaný graf.

(ii) G je silně souvislý, právě když G_c má jediný vrchol.

(iii) G je acyklický, právě když $G = G_c$.

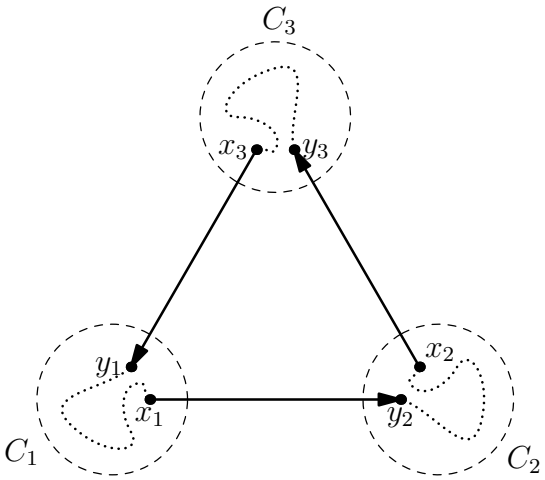
Důkaz. (i) Nechť L je cyklus v G_c, procházející po řadě vrcholy $C_1, C_2, \ldots, C_k$, $C_{k+1} = C_1$ grafu G_c (viz obr. 8.6). Pro $1 \leq i \leq k$ uvažme hranu C_iC_{i+1} cyklu L. Vrcholy C_i, C_{i+1} odpovídají kvazikomponentám grafu G. Z definice kondenzace existují vrcholy $x_i \in V(C_i)$ a $y_{i+1} \in V(C_{i+1})$ tak, že x_iy_{i+1} je hrana grafu G. Položme pro jednoduchost $y_1 := y_{k+1}$.

Máme tedy k-tici hran, které vedou postupně z kvazikomponenty C_1 do C_2, z C_2 do C_3 atd., a nakonec z C_k do C_1. Tyto hrany na sebe nemusí navazovat, ale v každé kvazikomponentě C_i jistě existuje cesta P_i z vrcholu y_i do x_i. Následující posloupnost hran a cest tedy tvoří cyklus L' v grafu G:

$$x_1y_2, P_2, x_2y_3, P_3, \ldots, P_k, x_ky_1, P_1.$$

Všimněme si, že po cyklu L' lze v grafu G dojít z vrcholu y_2 do vrcholu x_1. V opačném směru přitom mezi těmito vrcholy vede hrana. Oboustranná dosažitelnost těchto vrcholů je ve sporu s tím, že vrcholy leží v různých kvazikomponentách.

(ii) a (iii): Snadný důkaz přímo z definic ponecháváme jako cvičení 8.10. □



Obrázek 8.6: Konstrukce cyklu L' v grafu G. Čárkované oblasti jsou kvazikomponenty C_1, C_2, C_3 grafu G (vrcholy cyklu L v G_c).

Cvičení

▶ **8.10** Dokažte body (ii) a (iii) věty 8.15.

▶ **8.11** Najděte kondenzaci grafů na obr. 8.7.

Obrázek 8.7: Grafy ke cvičení 8.11.

Kapitola 9

Matice a počet koster

Graf (orientovaný i neorientovaný) lze popsat maticí, a to hned několika různými způsoby. Tématem této kapitoly jsou incidenční matice orientovaných grafů a to, jak algebraické vlastnosti těchto matic zachycují vlastnosti příslušných grafů.

Ukážeme si především pozoruhodnou, až spektakulární aplikaci incidenčních matic, při které spočítáme všechny kostry libovolného neorientovaného grafu pomocí determinantu jisté jednoduše definované matice. Mimo jiné dostaneme odpověď na následující otázku:

> Kolik existuje různých stromů na pevně dané n-prvkové množině vrcholů?

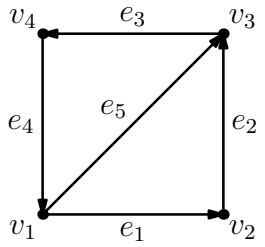
Zdůrazněme, že se jedná o *různé*, nikoli *neisomorfní* stromy. Na tříprvkové množině vrcholů například existují 3 různé stromy, ale všechny jsou navzájem isomorfní. (Viz také cvičení 7.1.)

9.1 Incidenční matice

Nechť G je v celém tomto oddílu orientovaný graf s vrcholy $V = \{v_1, \ldots, v_n\}$ a hranami $E = \{e_1, \ldots, e_m\}$. Budeme také předpokládat, že graf G neobsahuje smyčky.

Definice 9.1 *Incidenční matice* $M(G)$ orientovaného grafu G je reálná matice o rozměrech $n \times m$, definovaná vztahem $M(G) = (m_{ij})$, kde

$$m_{ij} = \begin{cases} +1 & \text{pokud hrana } e_j \text{ vychází z vrcholu } v_i, \\ -1 & \text{pokud hrana } e_j \text{ vchází do vrcholu } v_i, \\ 0 & \text{jinak.} \end{cases}$$



Obrázek 9.1: Orientovaný graf.

Graf na obr. 9.1 má tedy následující incidenční matici:

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & -1 & 1 & 0 \end{bmatrix},$$

v níž řádky odpovídají po řadě vrcholům $v_1, \ldots, v_4$ a sloupce hranám $e_1, \ldots, e_5$.

Všimněme si, že kdyby graf G obsahoval smyčky, nebyla by jeho incidenční matice dobře definována — smyčka totiž z příslušného vrcholu vchází, ale zároveň z něj vychází. Proto náš předpoklad, že G je bez smyček.

Zdůrazněme ještě jednu důležitou vlastnost incidenčních matic, jejímž důsledkem jsou různé jejich speciální vlastnosti, které uvidíme v následujících oddílech (např. Věta 9.6).

V každém sloupci matice $M(G)$ jsou právě dva nenulové prvky, z nichž jeden je $+1$ a druhý je -1.

Důvodem je samozřejmě fakt, že každá hrana obsahuje právě dva vrcholy, přičemž v prvním začíná a ve druhém končí.

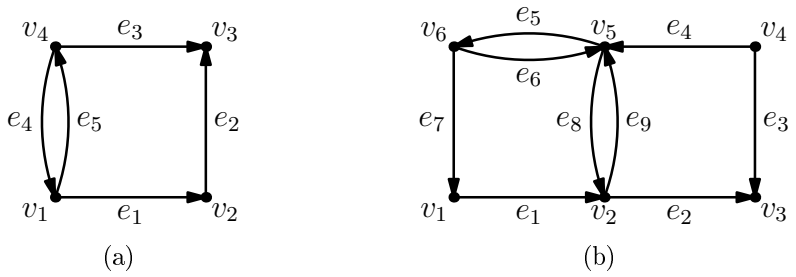
Cvičení

► **9.1** Určete incidenční matice grafů na obr. 9.2 (s daným označením vrcholů a hran).

► **9.2** V jakém vztahu jsou matice $M(G)$ a $M(H)$, jsou-li grafy G a H isomorfní?

9.2 Řádky jako vektory

Incidenční matice $M(G)$ má n řádků a m sloupců. Na každý řádek se tak můžeme dívat jako na *vektor* o m složkách, přesněji prvek vektorového prostoru $\mathbf{R}^m$. Řádky odpovídají vrcholům grafu G, a my budeme řádek odpovídající vrcholu v_i označovat jako $\mathbf{v}_i$. (Sloupec odpovídající hraně e_j budeme značit jako $\mathbf{e}_j$.)



Obrázek 9.2: Určete incidenční matice.

Jako v každém vektorovém prostoru, i v prostoru $\mathbf{R}^m$ je definován pojem lineární závislosti. Pro připomenutí:

> Množina vektorů $w_1, \ldots, w_k$ z vektorového prostoru W (nad tělesem reálných čísel) je *lineárně závislá*, pokud existují reálné koeficienty α_1, $\ldots$,α_k tak, že
>
> $$\sum_{i=1}^{k} \alpha_i w_i = \mathbf{0}$$
>
> a přitom ne všechny koeficienty α_i v této *lineární kombinaci* vektorů w_i jsou rovny nule.

Jaký má význam, je-li určitá množina řádků matice $M(G)$ lineárně závislá? Co to říká o odpovídající množině *vrcholů* grafu G? Klíčem k odpovědím na tyto otázky je následující nenápadné tvrzení.

Tvrzení 9.2 *Nechť K je komponenta orientovaného grafu G, a nechť*

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$$

je nulová lineární kombinace vektorů $\mathbf{v}_i$. Potom pro všechny vrcholy v_k z komponenty K jsou si koeficienty α_k navzájem rovny.

Důkaz. Nejsou-li na komponentě K všechny koeficienty α_k shodné, pak (díky slabé souvislosti) musí existovat *hrana* $e_j \in E(K)$ taková, že její počáteční vrchol v_p a koncový vrchol v_q mají různé koeficienty $\alpha_p \neq \alpha_q$.

Vzpomeňme si, že $M(G)$ obsahuje v j-tém sloupci (ve sloupci hrany e_j) jen dva nenulové prvky: $+1$ v p-tém řádku a -1 v q-tém řádku. Odtud plyne, že j-tá složka vektoru $\sum_{i=1}^{n} \alpha_i \mathbf{v}_i$ je rovna rozdílu $\alpha_p - \alpha_q$. O zmíněném vektoru ale předpokládáme, že je nulový, takže i $\alpha_p = \alpha_q$. To je spor. □

Cvičení

► **9.3** Jsou reálné vektory $(0, 1, -2)$, $(1, -1, 1)$ a $(2, -1, 0)$ lineárně závislé? Jak to lze poznat pomocí determinantu matice?

9.3 Hodnost incidenční matice

Hodnost $h(M)$ matice M je maximální velikost lineárně nezávislé množiny jejích řádků. Lze hodnost incidenční matice $M(G)$ určit z vlastností grafu G?

Především si všimněme, že matice $M(G)$ nikdy nemůže mít plnou hodnost n. Sečteme-li totiž všechny řádky, dva nenulové prvky v každém sloupci se vzájemně vyruší a vyjde nulový vektor. Jedná se tedy o nulovou lineární kombinaci řádků matice $M(G)$ (v níž jsou všechny koeficienty rovny jedné). Množina *všech* řádků matice $M(G)$ je lineárně závislá.

Věta 9.3 *Pro slabě souvislý graf G má matice $M(G)$ hodnost $n-1$. Platí dokonce, že* každá *množina $n-1$ řádků matice $M(G)$ je lineárně nezávislá.*

Důkaz. Nechť G je slabě souvislý a S je množina $n-1$ řádků matice $M(G)$. Ukážeme, že S je lineárně nezávislá. Dejme tomu, že $\sum_{\mathbf{v}_i \in S} \alpha_i \mathbf{v}_i = \mathbf{0}$ je nulová lineární kombinace řádků z S a rozšiřme tuto kombinaci na všechny řádky $M(G)$ tím, že pro (jediný) řádek $\mathbf{v}_k \notin S$ položíme $\alpha_k = 0$. Dostaneme lineární kombinaci

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$$

a podle tvrzení 9.2 musí být všechny koeficienty α_i shodné (protože slabě souvislý graf G má jedinou komponentu). Kvůli koeficientu α_k jsou tedy všechny nulové. Dokázali jsme, že množina S je lineárně nezávislá, a speciálně také $h(M(G)) = n-1$. □

Toto tvrzení lze zobecnit i na grafy, které nejsou slabě souvislé:

Věta 9.4 *Orientovaný graf G má přesně k komponent, právě když $h(M(G)) = n-k$.*

Důkaz. '⇒': Nechť G má k komponent $C_1, \ldots, C_k$. Nejprve dokážeme, že hodnost matice $M(G)$ je nejvýše $n-k$. Nechť S je množina alespoň $n-k+1$ řádků. Musí existovat komponenta C_p s vlastností, že S obsahuje všechny řádky odpovídající vrcholům C_p, protože kdyby S z každé komponenty aspoň jeden řádek vynechala, obsahovala by jich nejvýše $n-k$. Sečteme-li nyní všechny řádky $\mathbf{v}_i$ pro $v_i \in V(C_p)$, dostaneme nulový vektor: každá hrana e_j má v C_p buď oba konce (a příslušný součet je $1+(-1)$), nebo ani jeden (a pak sčítáme samé nuly). Tato nulová lineární kombinace řádků z S ukazuje, že množina S je lineárně závislá. Proto $h(M(G)) \leq n-k$.

Vyberme nyní nějakou množinu řádků S o velikosti $n-k$, která pro každou komponentu L_i obsahuje všechny řádky odpovídající vrcholům L_i kromě jediného. Tvrdíme, že S je lineárně nezávislá. Kdyby tomu tak nebylo, rozšiřme lineární závislost $\sum_{\mathbf{v}_i \in S} \alpha_i \mathbf{v}_i = \mathbf{0}$ na všechny řádky matice $M(G)$ položením $\alpha_i = 0$ pro všechny $\mathbf{v}_i \notin S$:

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}.$$

Podle tvrzení 9.2 jsou všechny koeficienty na každé komponentě L_i shodné. Protože pro každou komponentu existuje vrchol s nulovým koeficientem, musí být $\alpha_i = 0$ pro každé i, takže S je vskutku lineárně nezávislá. Hodnost matice $M(G)$ je tedy právě $n-k$.

'$\Leftarrow$': Nechť $h(M(G)) = n-k$. Podle dokázané implikace je hodnost incidenční matice grafu s i komponentami rovna $n-i$. Graf G tedy musí mít přesně k komponent. □

Cvičení

► **9.4** Určete hodnost incidenční matice orientovaného grafu na $3k$ vrcholech, tvořeného k disjunktními cykly délky 3. Jak vypadají lineárně nezávislé množiny řádků o maximální velikosti?

9.4 Faktory jako množiny sloupců

Víme, že sečtením všech řádků matice $M(G)$ dostaneme nulový vektor. Lze ji tedy rekonstruovat z matice $M_R(G)$, vzniklé vypuštěním posledního řádku matice $M(G)$. Jinak řečeno, matice $M_R(G)$ (kterou nazýváme *redukovaná incidenční matice* grafu G) poskytuje o orientovaném grafu G úplnou informaci.

Sloupce incidenční matice $M(G)$ odpovídají hranám grafu G. Pro nás bude důležité, že množiny sloupců této matice odpovídají určitým podgrafům grafu G.

Připomeňme z definice 7.5, že faktor grafu G je libovolný podgraf $H \subset G$, pro který je $V(H) = V(G)$. Každý faktor grafu G je tedy jednoznačně určen svou množinou hran. Tím je také dán vzájemně jednoznačný vztah mezi těmito faktory a množinami sloupců matice $M_R(G)$: faktor F_S, přiřazený množině sloupců S, obsahuje právě ty hrany e_j, jejichž sloupec $\mathbf{e}_j$ patří do S.

V následující větě figurují čtvercové podmatice matice $M_R(G)$ řádu $n-1$. Vzhledem k tomu, že $M_R(G)$ má právě $n-1$ řádků, je každá taková podmatice určena $n-1$-prvkovou množinou sloupců. Pro množinu sloupců S označíme příslušnou podmatici jako A_S.

Pro neorientované grafy jsme definovali pojem kostry. Do oblasti orientovaných grafů jej přeneseme takto: podgraf H orientovaného grafu G je jeho *kostrou*, pokud symetrizace grafu H je kostrou symetrizace grafu G, a navíc H neobsahuje smyčky ani protichůdné hrany.

Věta 9.5 *Nechť G je slabě souvislý orientovaný graf bez smyček. Potom čtvercová podmatice A_S matice $M_R(G)$ řádu $n-1$ je regulární, právě když odpovídající faktor F_S je kostrou grafu G.*

Důkaz. '$\Rightarrow$': Nechť matice A_S je regulární. Z definice plyne, že A_S je redukovanou maticí incidence faktoru F_S, tedy $A_S = M_R(F_S)$. Protože $h(A_S) = n-1$, musí mít (neredukovaná) matice $M(F_S)$ maximální možnou hodnost $n-1$. Podle věty 9.4 je F_S slabě souvislý. Navíc určitě neobsahuje protichůdné hrany, protože příslušné sloupce by byly až na znaménko shodné a A_S by nebyla regulární matice. Symetrizace faktoru F_S je tedy souvislý graf s $n-1$ hranami. Podle věty 7.4 se musí jednat o strom. Odtud dostáváme tvrzení věty.

'$\Leftarrow$': Nechť faktor F_S je kostrou grafu G. Je tedy slabě souvislý a podle věty 9.3 tvoří prvních $n-1$ řádků matice $M(F_S)$ lineárně nezávislou množinu. Proto $h(M_R(F_S)) = n-1$ a matice $A_S = M_R(F_S)$ je regulární. □

Cvičení

► **9.5** Kolik faktorů má graf o n vrcholech a m hranách?

9.5 Počítání koster

Čtvercové podmatice matice incidence mají zajímavou vlastnost, které se říká *totální unimodularita*:

Věta 9.6 *Je-li $M(G)$ incidenční matice orientovaného grafu G (bez smyček) a je-li B její čtvercová podmatice řádu r (kde $1 \leq r \leq n$), potom determinant matice B je 0 nebo ± 1.*

Důkaz. Indukcí podle r. Pro $r = 1$ je tvrzení jasné z definice incidenční matice. Předpokládejme, že $r > 1$. Pokud matice B obsahuje nulový sloupec, je $\det B = 0$. Pokud obsahuje sloupec s jedinou nenulovou hodnotou b_{ij}, pak z rozvoje podle tohoto sloupce dostáváme

$$\det B = \pm \det B',$$

kde B' vznikne z B odstraněním i-tého řádku a j-tého sloupce. Podle indukčního předpokladu je $\det B' \in \{0, 1, -1\}$, takže totéž musí platit pro matici B.

Můžeme tedy předpokládat, že každý sloupec matice B obsahuje právě dvě nenulové hodnoty (tj. 1 a -1). Sečtením všech řádků nutně dostaneme nulový vektor; to znamená, že matice B je singulární a $\det B = 0$. I v tomto posledním případě tvrzení platí. □

Při počítání koster grafu se neobejdeme bez Cauchy–Binetovy[1] věty, kterou nebudeme dokazovat. Její zhruba dvoustránkový důkaz lze najít např. v knize [4].

[1] Augustin-Louis Cauchy (1789–1857) a Jacques Philippe Marie Binet (1786–1856).

Věta 9.7 (Cauchy–Binetova věta) *Nechť B je matice o rozměrech $r \times s$, kde $r \leq s$. Potom platí, že*

$$\det(B \cdot B^T) = \sum_I (\det B_I)^2,$$

kde I probíhá všechny r-prvkové množiny sloupců a B_I je čtvercová podmatice matice B, určená sloupci z množiny I. □

Nyní již můžeme vyslovit větu, která dává do souvislosti determinanty a počet koster.

Věta 9.8 *Nechť G je slabě souvislý orientovaný graf bez smyček a $A = M_R(G)$. Potom počet koster grafu G je roven determinantu matice $A \cdot A^T$.*

Důkaz. Podle Cauchy–Binetovy věty je

$$\det(A \cdot A^T) = \sum_S (\det A_S)^2, \tag{9.1}$$

kde S probíhá $(n-1)$-tice sloupců matice A. Podle věty 9.5 (ve které má symbol A_S stejný význam jako zde) je $\det A_S \neq 0$ přesně pro ty množiny S, pro něž je faktor F_S kostrou. Ostatní množiny S součet v (9.1) neovlivní.

Je-li F_S kostra, pak podle věty 9.6 je $\det A_S = \pm 1$, takže $(\det A_S)^2 = 1$. Každá kostra tedy v součtu (9.1) přispěje jedničkou a vidíme, že $\det(A \cdot A^T)$ skutečně počítá kostry grafu G. □

Příklad 9.9 Jako aplikaci věty 9.8 spočítejme kostry grafu G, který je definován jako cyklus délky 3. Jeho redukovaná incidenční matice je

$$M_R(G) = \begin{bmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix},$$

takže

$$\det\Big(M_R(G) \cdot (M_R(G))^T\Big) = \det \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix} = 3.$$

Graf G má tedy 3 kostry (což nás asi příliš nepřekvapí).

Cvičení

▶ **9.6** Spočítejte pomocí věty 9.8 kostry grafu na obr. 9.1.

9.6 Počítání koster: neorientované grafy

Nechť je dán *neorientovaný* graf G. Chceme-li 'v praxi' počítat jeho kostry pomocí determinantů, lze to zařídit snadněji než pomocí věty 9.8. K jejímu použití bychom nejprve museli graf G libovolně zorientovat a získat tak orientovaný graf $\vec{G}$, dále spočítat součin $M_R(\vec{G}) \cdot (M_R(\vec{G}))^T$ a konečně zjistit jeho determinant.

Uvedený součin však (jak uvidíme) závisí pouze na grafu G, nikoli na zvolené orientaci, a lze jej navíc snadno odvodit přímo z grafu G. Tím se vyhneme nutnosti násobení matic.

Věta 9.10 *Nechť G je neorientovaný graf s vrcholy $V = \{v_1, \ldots, v_n\}$ a $\vec{G}$ nějaká jeho orientace bez smyček a násobných hran. Dále položme*

$$L = M(\vec{G}) \cdot (M(\vec{G}))^T \qquad \textit{(tzv.} \text{ Laplaceova matice } \textit{grafu } G\textit{)}.$$

Potom pro prvky čtvercové matice $L = (\ell_{ij})$ řádu n platí:

$$\ell_{ij} = \begin{cases} d_G(v_i) & \textit{pokud } i = j, \\ -1 & \textit{pokud } v_i v_j \in E(G), \\ 0 & \textit{jinak.} \end{cases}$$

Navíc platí, že matici $L' = M_R(\vec{G}) \cdot (M_R(\vec{G}))^T$ získáme vypuštěním posledního řádku a sloupce z matice L.

Důkaz. Položku ℓ_{ij} matice L získáme jako skalární součin $\mathbf{v}_i \cdot \mathbf{v}_j$, tedy součin i-tého a j-tého řádku matice $M(\vec{G})$. Pokud $i = j$, pak každá hrana obsahující vrchol v_i (nezávisle na směru) přispěje k tomuto skalárnímu součinu 1, takže $\mathbf{v}_i \cdot \mathbf{v}_i = d_G(v_i)$. Pro $i \neq j$ jsou vrcholy v_i, v_j spojeny nejvýše jednou hranou, tj. vektory $\mathbf{v}_i, \mathbf{v}_j$ jsou nejvýše v jedné souřadnici oba nenulové. Snadno vidíme, že součin $\mathbf{v}_i \cdot \mathbf{v}_j$ je -1 resp. 0 podle toho, zda $v_i v_j$ je hranou nebo ne.

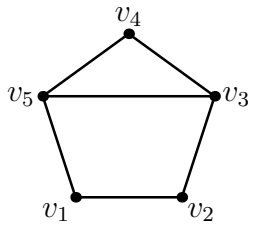
Druhá část věty přímo plyne z definice násobení matic. □

Rychlejší postup počítání koster neorientovaného grafu, založený na této větě, si ukážeme na následujícím příkladu.

Příklad 9.11 Uvažme neorientovaný graf G na obr. 9.3. Napišme přímo jeho Laplaceovu[2] matici:

$$L = \begin{bmatrix} 2 & -1 & 0 & 0 & -1 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 3 & -1 & -1 \\ 0 & 0 & -1 & 2 & -1 \\ -1 & 0 & -1 & -1 & 3 \end{bmatrix}.$$

[2] Pierre-Simon Laplace (1749–1827).



Obrázek 9.3: Graf z příkladu 9.11.

Podle vět 9.10 a 9.8 stačí z matice L vynechat poslední řádek a sloupec, a determinant výsledné matice L' je počet koster grafu G. Přímým výpočtem zjistíme, že

$$\det L' = \det \begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 3 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix} = 11.$$

Graf G má tedy 11 koster.

Vraťme se k otázce, kterou jsme tuto kapitolu zahájili: kolik existuje různých stromů na n-prvkové množině vrcholů? Lze ji formulovat také takto: kolik různých koster má úplný graf na n vrcholech?

Věta 9.12 *Úplný graf na $n \geq 2$ vrcholech má n^{n-2} různých koster.*

Důkaz. Laplaceova matice L_n grafu K_n je čtvercová matice řádu n a vypadá takto:

$$L_n = \begin{bmatrix} n-1 & -1 & -1 & \dots & -1 \\ -1 & n-1 & -1 & \dots & -1 \\ -1 & -1 & n-1 & \dots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \dots & n-1 \end{bmatrix}.$$

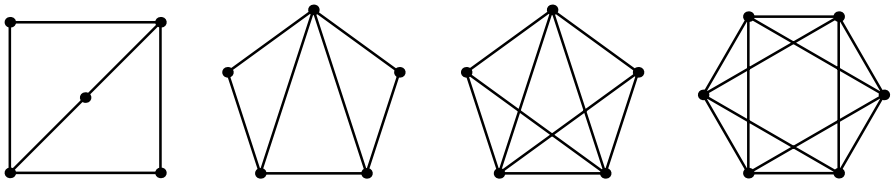
Determinant matice L'_n, která vznikne odstraněním posledního řádku a sloupce, je hledaný počet koster. Přičtěme k prvnímu řádku matice L'_n všechny ostatní řádky, a následně přičtěme tento nový první řádek ke všem ostatním. Determinant se nezmění, takže

$$\det L'_n = \det \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & n & 0 & \dots & 0 \\ 0 & 0 & n & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & n \end{bmatrix}.$$

Matice na pravé straně má $n-1$ řádků, takže rozvojem podle prvního sloupce dostáváme $\det L'_n = n^{n-2}$. □

Cvičení

► **9.7** Určete počet koster grafů na obr. 9.4.



Obrázek 9.4: Určete počet koster.

► **9.8** Osvěžte si potřebné pojmy z lineární algebry a ukažte, že pro Laplaceovu matici $L(G)$ neorientovaného grafu G platí:

(a) $L(G)$ je pozitivně semidefinitní,

(b) vlastní vektor příslušný vlastnímu číslu 0 je vektor s jednotkovými složkami,

(c) je-li G souvislý, pak vlastní číslo 0 má násobnost 1.

Kapitola 10

Lineární prostory grafu

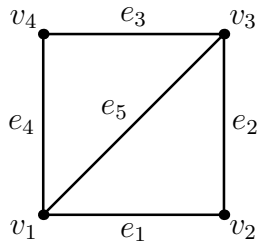
Metoda počítání koster pomocí determinantů není jediným pojítkem mezi teorií grafů a lineární algebrou. V této kapitole uvidíme, jak lze každému neorientovanému grafu přirozeným způsobem přiřadit dva lineární prostory nad tělesem $\mathbf{Z}_2$ (prostor kružnic a prostor řezů) a prozkoumáme vlastnosti těchto prostorů.

10.1 Incidenční matice neorientovaného grafu

Podobně, jako jsme definovali incidenční matici pro orientované grafy, lze ji zavést i pro grafy neorientované. Vzhledem k tomu, že hrany těchto grafů nemají směr, vystačíme zde s hodnotami 0 a 1. Je-li tedy G neorientovaný graf s n vrcholy $v_1, \ldots, v_n$ a m hranami $e_1, \ldots, e_m$, pak jeho *incidenční matice* $M(G)$ je definována předpisem $M(G) = (m_{ij})$, kde

$$m_{ij} = \begin{cases} 1 & \text{pokud } v_i \in e_j, \\ 0 & \text{jinak} \end{cases}$$

pro $i = 1, \ldots, n$ a $j = 1, \ldots, m$.



Obrázek 10.1: Neorientovaný graf H.

Graf na obr. 10.1 má například následující incidenční matici (i-tý řádek od-

povídá vrcholu v_i, j-tý sloupec hraně e_j):

$$M(H) = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Všimněme si, že každý sloupec incidenční matice nyní obsahuje právě dva prvky, které jsou rovny jedné. Stejně jako u orientovaných grafů tak dokážeme jednoznačně zrekonstruovat poslední řádek z řádků předcházejících. Asi bychom proto čekali, že řádky takovéto matice jsou opět lineárně závislé. Výše uvedená matice $M(H)$ má však překvapivě hodnost 4, tedy maximální možnou!

Záhada má jednoduché řešení:

S incidenční maticí neorientovaného grafu
je třeba pracovat nad tělesem $\mathbf{Z}_2$.

Co to přesně obnáší, uvidíme v následujícím oddílu.

10.2 Hodnost nad $\mathbf{Z}_2$

Řádky matice $M(G)$ jsou vektory složené z m nul a jedniček. Můžeme je tedy interpretovat jako prvky vektorového prostoru $\mathbf{Z}_2^m$ dimenze m nad tělesem $\mathbf{Z}_2$. Veškerá aritmetika v tomto prostoru je prováděna 'po složkách' a modulo 2. Připomeňme, že množina vektorů $\{w_1, \ldots, w_k\} \subset \mathbf{Z}_2^m$ je *lineárně závislá nad* $\mathbf{Z}_2$, pokud existují koeficienty $\alpha_1, \ldots, \alpha_k \in \mathbf{Z}_2$ (ne všechny nulové), pro něž je

$$\sum_{i=1}^{k} \alpha_i w_i = \mathbf{0},$$

přičemž samozřejmě stále počítáme nad tělesem $\mathbf{Z}_2$. Vzhledem k tomu, že koeficienty mohou být pouze 0 nebo 1, a nulové koeficienty součet neovlivní, je vidět, že množina vektorů je lineárně závislá nad $\mathbf{Z}_2$, právě když obsahuje neprázdnou podmnožinu s nulovým součtem.

Hodnost matice M nad $\mathbf{Z}_2$ (budeme ji značit $h_2(M)$) je definována jako maximální velikost množiny řádků, která je lineárně nezávislá nad $\mathbf{Z}_2$. Třebaže matice $M(H)$ má hodnost (nad tělesem reálných čísel) rovnou 4, nad $\mathbf{Z}_2$ je součtem jejích řádků nulový vektor a podle očekávání platí $h_2(M(H)) = 3$.

Pro hodnost matice $M(G)$ nad $\mathbf{Z}_2$ platí obdobné vztahy jako pro obyčejnou hodnost v orientovaném případě, a také se velmi podobně dokazují. Shrneme je v následující větě, jejíž důkaz ponecháme jako cvičení.

Věta 10.1 *Pro neorientovaný graf G platí:*

(i) Hodnost $h_2(M(G))$ je rovna $n - k$, právě když G má k komponent.

(ii) Je-li G souvislý, pak dokonce každých $n-1$ řádků tvoří lineárně nezávislou množinu nad $\mathbf{Z}_2$. □

Cvičení

▶ **10.1** Dokažte větu 10.1.

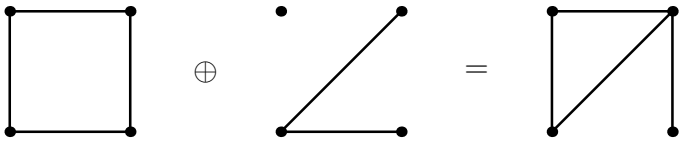
10.3 Vektory a faktory

Každý vektor z prostoru $\mathbf{Z}_2^m$ odpovídá nějaké množině hran grafu G, a ta zase jednoznačně určuje faktor grafu G. Pro jednoduchost proto obvykle nebudeme rozlišovat mezi vektory ze $\mathbf{Z}_2^m$, faktory grafu G a množinami jeho hran. V případě potřeby budeme o vektoru, který odpovídá nějaké množině hran M, hovořit jako o jejím *charakteristickém vektoru*.

V prostoru $\mathbf{Z}_2^m$ je definováno sčítání, které budeme značit symbolem $\oplus$. Co znamená toto sčítání v řeči faktorů? Jsou-li $F, F' \in \mathbf{Z}_2^m$, pak na i-tém místě v součtu $F \oplus F'$ bude 0, právě když F a F' mají na tomto místě oba 0 nebo oba 1. Odtud snadno vidíme, že faktor $F \oplus F'$ je *symetrický rozdíl* faktorů F a F', tj. je definován předpisem

$$F \oplus F' = F \cup F' - \Big(F \cap F'\Big).$$

Příklad 'sčítání' faktorů grafu H na obr. 10.1 ukazuje obr. 10.2.



Obrázek 10.2: Sčítání faktorů.

Řekneme, že faktor $F \subset G$ je *sudý*, má-li v něm každý vrchol sudý stupeň. Tento pojem úzce souvisí s pojmem eulerovského grafu, studovaným v oddílu 6.6: každá komponenta sudého faktoru je totiž eulerovský graf. Bude nás zajímat mimo jiné následující otázka:

Kolik má graf G sudých faktorů?

Alespoň jeden sudý faktor existuje vždy: faktor s prázdnou množinou hran. Je-li ovšem graf G například stromem, pak už žádné další sudé faktory nemá. Každý jeho faktor je totiž sjednocením disjunktních stromů, a my víme, že strom na alespoň dvou vrcholech obsahuje nějaký list, tj. vrchol stupně 1. Jediný sudý faktor stromu je tedy ten, ve kterém jsou všechny komponenty jednobodové.

Oproti tomu každá kružnice C v grafu G určuje sudý faktor s množinou hran $E(C)$ (vrcholy na C mají stupeň 2, ostatní 0). Zdá se tedy, že čím více kružnic, tím více sudých faktorů.

Zásadní pozorování představuje následující věta.

Věta 10.2 *Sudé faktory tvoří podprostor vektorového prostoru* $\mathbf{Z}_2^m$.

Důkaz. Vzhledem k tomu, že pracujeme nad tělesem $\mathbf{Z}_2$, stačí ověřit, že součet (=symetrický rozdíl) sudých faktorů F_1, F_2 je sudým faktorem, tj. že stupeň každého vrcholu $v \in V(G)$ ve faktoru $F_1 \oplus F_2$ je sudý. Nechť A_i je množina hran obsahujících v ve faktoru F_i $(i = 1, 2)$. Víme, že ve faktoru $F_1 \oplus F_2$ je vrchol v obsažen právě ve hranách ze symetrického rozdílu $A_1 \oplus A_2$. Jeho stupeň je tak

$$\begin{aligned} d_{F_1 \oplus F_2}(v) &= |A_1 \oplus A_2| = |A_1 \cup A_2 - (A_1 \cap A_2)| \\ &= |A_1| + |A_2| - 2|A_1 \cap A_2|, \end{aligned}$$

a protože A_i jsou množiny sudé velikosti, je i tento stupeň sudý. Vrchol v byl libovolný, takže $F_1 \oplus F_2$ je sudý faktor. □

Podprostoru z věty 10.2 se říká *prostor kružnic* nebo *prostor cyklů* grafu G. Označuje se $\mathcal{C}(G)$. Název 'prostor kružnic' může být zavádějící, neboť tento prostor obecně obsahuje i sudé faktory, které nejsou kružnicemi (viz cvičení 10.2). Tuto terminologii ospravedlňuje následující pojem, který také umožňuje alternativní, možná intuitivnější pohled na prostor $\mathcal{C}(G)$.

Matice kružnic $C(G)$ sestává z řádků, které vzájemně jednoznačně odpovídají kružnicím v grafu G. Řádek příslušný kružnici C je charakteristický vektor její množiny hran $E(C)$. Matice $C(G)$ má tedy m sloupců a tolik řádků, kolik je kružnic v grafu G. Je určena jednoznačně až na pořadí řádků a sloupců.

Tvrzení 10.3 *Řádky matice* $C(G)$ *generují prostor kružnic* $\mathcal{C}(G)$.

Důkaz. Stačí ukázat, že libovolný sudý faktor F je součtem kružnic. Použijeme indukci podle počtu hran faktoru F. Můžeme předpokládat, že F obsahuje nějaké hrany, jinak je totiž součtem prázdné množiny řádků matice $C(G)$. Zvolme komponentu F_0 faktoru F, která obsahuje aspoň jednu hranu. Potom F_0 je souvislý graf, ve kterém všechny vrcholy mají sudý stupeň, takže podle věty 6.18 má graf F_0 eulerovský tah $T = (v_0, \ldots, v_k = v_0)$. Pro nejmenší index $i > 0$ s vlastností $v_i = v_0$ je počáteční úsek $K = (v_0, \ldots, v_i)$ tahu T nutně kružnicí. Označme množinu hran této kružnice symbolem $E(K)$. Faktor $F' = E(F) \oplus E(K)$ získáme 'odečtením' kružnice K z faktoru F. Je to tedy sudý faktor a má méně hran než F. Z indukce plyne, že F' je součtem kružnic (řekněme) $C_1, \ldots, C_\ell$. Proto také faktor

$$F' = C_1 \oplus \cdots \oplus C_\ell \oplus K$$

je součtem kružnic, což jsme chtěli dokázat. □

Cvičení

▶ **10.2** Najděte příklad grafu, jehož prostor kružnic obsahuje i sudé faktory, které nejsou kružnicemi.

▶ **10.3** Určete matici kružnic grafů na obr. 10.3.

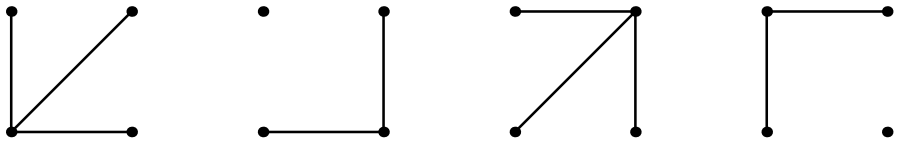
(a) (b)

Obrázek 10.3: Grafy k cvičení 10.3.

10.4 Hvězdy, separace a řezy

Od tohoto oddílu dále budeme předpokládat, že graf G je souvislý. K nesouvislým grafům se vrátíme na konci kapitoly.

Jak vypadají faktory určené řádky incidenční matice grafu G? Pokud se jedná o řádek, který přísluší vrcholu v_i, pak do daného faktoru náleží pouze hrany obsahující vrchol v_i. Tomuto faktoru říkáme *hvězda vrcholu* v_i a označujeme jej H_i. Všechny hvězdy grafu na obr. 10.1 jsou znázorněny na obr. 10.4.



Obrázek 10.4: Hvězdy v grafu na obr. 10.1.

Všimněme si, že hvězdy typicky obsahují izolované vrcholy (vrcholy stupně 0) — konkrétně ve hvězdě vrcholu v_i bude izolovaný každý vrchol, který s ním nesousedí. Všechny tyto vrcholy však do hvězdy patří (je to faktor)!

Pojem hvězda lze zobecnit následujícím způsobem. Pro množinu vrcholů $X \subset V(G)$ nechť ∂X označuje faktor složený ze všech hran, které mají v množině X právě jeden koncový vrchol (tj. z hran, které vedou 'mezi' X a $V(G) - X$). Každý faktor tohoto tvaru označíme termínem *separace*. Například každá hvězda je separace, protože platí $\partial\{v_i\} = H_i$. Separací je i faktor bez hran.

Věta 10.4 *Množina všech separací je podprostorem prostoru* $\mathbf{Z}_2^m$.

Důkaz. Stačí ověřit uzavřenost na součty. Dokazujeme, že pro každé $X, Y \subset V(G)$ je faktor $\partial X \oplus \partial Y$ separací. Všimněme si, že hrana e patří do faktoru $\partial X \oplus \partial Y$, právě když $e \in \partial X$ a $e \notin \partial Y$ nebo naopak. To zase platí právě tehdy, když e má v jedné z množin X, Y jeden konec a v té druhé buď žádný nebo oba konce. Jak lze snadno ověřit, ekvivalentní podmínkou je, že e má právě jeden konec v množině $X \oplus Y$. Dokázali jsme tedy, že

$$\partial(X \oplus Y) = \partial X \oplus \partial Y$$

a z toho plyne tvrzení věty. □

Nechť S je separace, dejme tomu $S = \partial X$. Odstraněním hran faktoru S z grafu G dostaneme jistě nesouvislý graf, protože z žádného vrcholu v množině X v grafu $G - E(S)$ nevede hrana do žádného vrcholu mimo X. Speciálním případem separace je řez, který je definován následovně.

Řezem v souvislém grafu G je množina hran A s vlastností, že graf $G - A$ (vzniklý odstraněním hran v A z grafu G) je nesouvislý, ale přitom žádná vlastní podmnožina množiny A tuto vlastnost nemá.

Podprostor z věty 10.4 se nazývá *prostor řezů* grafu G a označuje se $\mathcal{R}(G)$. Víme, že každá hvězda je jeho prvkem. Platí dokonce následující:

Tvrzení 10.5 *Hvězdy generují celý prostor řezů.*

Důkaz. Musíme ukázat, že každou separaci ∂X lze vyjádřit jako součet hvězd. Tvrdíme, že platí

$$\sum_{v_i \in X} H_i = \partial X.$$

Tato rovnost plyne z faktu, že má-li hrana e_j v množině X oba koncové vrcholy, započítali jsme ji v součtu na levé straně dvakrát; nemá-li v X ani jeden vrchol, nezapočítali jsme ji vůbec. V obou případech vyjde na j-tém místě výsledného vektoru 0. Hodnota 1 tedy na tomto místě vyjde právě tehdy, když e_j je hranou faktoru ∂X. □

Věta 10.6 *Dimenze prostoru řezů je právě* $n - 1$.

Důkaz. Podle předchozího tvrzení je prostor řezů generován hvězdami. Podle věty 10.1(ii) je dimenze tohoto prostoru přesně $n - 1$. □

Stejně jako většina prvků prostoru kružnic nejsou kružnice (ale sudé faktory), také prostor řezů je z větší části tvořen faktory, které nejsou řezy (ale separacemi, viz cvičení 10.4).

Podobně jako u prostoru kružnic můžeme definovat *matici řezů* $R(G)$ grafu G, jejíž každý řádek je charakteristický vektor množiny hran některého řezu v grafu G (a každému řezu odpovídá jeden řádek). Následující fakt je analogií tvrzení 10.3.

Tvrzení 10.7 *Řádky matice $R(G)$ generují celý prostor $\mathcal{R}(G)$.*

Důkaz. Podle tvrzení 10.5 víme, že prostor $\mathcal{R}(G)$ je generován hvězdami. Třebaže ne každá hvězda je řez, není těžké nahlédnout, že různé řezy obsažené v jedné hvězdě H jsou navzájem disjunktní a H je tedy jejich součtem. Všechny hvězdy tak leží v lineárním obalu množiny řádků matice $R(G)$ a z toho plyne dokazované tvrzení. □

Cvičení

▶ **10.4** Najděte příklad separace v nějakém grafu, která není řezem. Najděte příklad hvězdy s touto vlastností.

▶ **10.5** Dokažte, že je-li A řez v souvislém grafu G, pak graf $G - A$ má právě dvě komponenty. Rozhodněte, zda platí opačná implikace.

▶ **10.6** Dokažte, že graf, který obsahuje nějaký řez o velikosti 1, nemůže být eulerovský ani hamiltonovský.

10.5 Ortogonalita

Připomeňme, že ve vektorovém prostoru $\mathbf{R}^n$ je pro každou dvojici vektorů u, v definován skalární součin. Od něj se odvozuje pojem ortogonality vektorů. Podobné pojmy mají smysl i v prostoru $\mathbf{Z}_2^m$.

Jsou-li $u = (u_1 \dots u_m)$ a $v = (v_1 \dots v_m)$ prvky prostoru $\mathbf{Z}_2^m$, pak jejich *skalární součin*[1] $u \cdot v$ je definován předpisem

$$u \cdot v = \sum_{i=1}^{m} u_i v_i,$$

kde sčítání provádíme v tělese $\mathbf{Z}_2$ (výsledek je tedy 0 nebo 1). Vektory u, v jsou *ortogonální* nebo *kolmé* (značíme $u \perp v$), pokud $u \cdot v = 0$. Tento pojem lze rozšířit na množiny vektorů: množiny $U, V \subset \mathbf{Z}_2^m$ jsou *ortogonální* ($U \perp V$), pokud $u \perp v$ pro každé $u \in U$, $v \in V$.

Jaký význam má skalární součin při našem ztotožnění vektorů a faktorů? Kdy jsou dva faktory navzájem kolmé? Přímo z definice plyne jednoduchá odpověď: jsou kolmé, právě když se shodují v sudém počtu hran (tj. jejich průnik má sudou velikost).

Je-li W podprostor prostoru $\mathbf{Z}_2^m$, definujeme jeho *ortogonální doplněk* $W^\perp$ jako množinu všech vektorů, které jsou kolmé na každý prvek podprostoru W.

[1] Pro přesnost upozorněme, že naše definice je v mírném rozporu s obecnou definicí skalárního součinu ve vektorových prostorech. Ta totiž mj. požaduje, aby vztah $x \cdot x = 0$ platil pouze pro nulový vektor. V našem případě ale bude platit pro každý vektor se sudým počtem jedniček.

Z bilinearity skalárního součinu snadno plyne, že $W^\perp$ je opět podprostorem (viz cvičení 10.7). Pro nás bude velmi důležitá následující věta.

Věta 10.8 *Je-li W podprostor prostoru $\mathbf{Z}_2^m$, pak platí*

$$\dim W + \dim W^\perp = m.$$

Důkaz. Označme $\dim W = k$. Nechť M je matice o rozměrech $k \times m$, jejíž řádky jsou prvky nějaké pevné báze podprostoru W. K tomu, aby vektor $x \in \mathbf{Z}_2^m$ byl kolmý na každý vektor z W, stačí, aby byl kolmý na každý prvek zvolené báze. Jinými slovy, $x \in W^\perp$, právě když x je řešením soustavy $Mx = \mathbf{0}$.

Standardní eliminací (a případným přeskupením sloupců) upravíme M na matici M', ve které prvních k sloupců tvoří jednotkovou matici, tedy

$$M' = \left[I_k \;\middle|\; B \right],$$

kde B je nějaká matice o rozměrech $k \times (m-k)$. Je jasné, že libovolně zvolená čísla $x_{k+1}, x_{k+2}, \ldots, x_m$, lze *jednoznačně* doplnit na řešení $x = (x_1 \ldots x_m)$ soustavy $Mx = \mathbf{0}$. Dimenze prostoru, tvořeného řešeními této soustavy (kterým je shodou okolností prostor $W^\perp$), je tedy $m - k$. Věta je dokázána. □

Dokončíme nyní výpočet dimenzí prostoru kružnic a prostoru řezů. Nechť F je nějaký faktor grafu G. Podle toho, co bylo řečeno o ortogonalitě faktorů, je stupeň vrcholu v_i ve faktoru F sudý, právě když je F kolmý na hvězdu H_i. To znamená, že F je sudý faktor, právě když je kolmý na všechny hvězdy. Jinak řečeno:

Věta 10.9 *Prostor kružnic $\mathcal{C}(G)$ je ortogonálním doplňkem prostoru řezů $\mathcal{R}(G)$.*

Důkaz. Prvky prostoru $\mathcal{C}(G)$ jsou právě sudé faktory. Víme, že $F \in \mathcal{C}(G)$, právě když F je kolmý na každou hvězdu. Protože prostor řezů $\mathcal{R}(G)$ je hvězdami generován, platí, že $F \in \mathcal{C}(G)$, právě když $F \perp S$ pro každou separaci $S \in \mathcal{R}(G)$. Jinými slovy $\mathcal{C}(G) = \mathcal{R}(G)^\perp$. □

Podle věty 10.6 je $\dim \mathcal{R}(G) = n - 1$. Podle věty 10.8 platí $\dim \mathcal{C}(G) + \dim \mathcal{R}(G) = m$. V důsledku dostáváme:

Věta 10.10 *Dimenze prostoru kružnic je $m - n + 1$.* □

Důsledek 10.11 *Souvislý graf G má 2^{m-n+1} sudých faktorů.* □

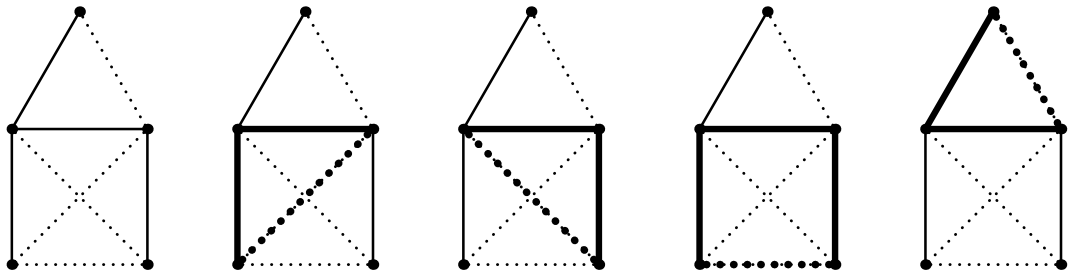
Cvičení

► **10.7** Dokažte, že ortogonální doplněk $W^\perp$ podprostoru $W \subset \mathbf{Z}_2^m$ je rovněž podprostorem.

10.6 Fundamentální soustavy kružnic a řezů

Určili jsme přesně dimenzi prostoru kružnic a prostoru řezů. V tomto odstavci ukážeme způsob, jak snadno najít báze těchto prostorů, navíc v pěkném speciálním tvaru. Nechť G je souvislý graf. Zvolme pevně nějakou jeho kostru T. Hrany $e \in E(G) - E(T)$ se nazývají *tětivy* kostry T. Je jich $m - n + 1$, protože každý strom na n vrcholech má $n - 1$ hran, přičemž počet všech hran grafu G je m.

Víme, že stromy jsou charakterizovány vlastností, že každé dva jejich vrcholy jsou spojenu právě jednou cestou. Odtud plyne, že přidáme-li ke kostře T tětivu e_j, výsledný graf $T + e_j$ bude obsahovat právě jednu kružnici. Označme tuto kružnici C_j. Soubor všech kružnic C_j, kde e_j probíhá tětivy kostry T, se nazývá *fundamentální soustava kružnic* grafu G vzhledem ke kostře T. Příklad takové soustavy je na obr. 10.5.



Obrázek 10.5: (a) Graf s plně vyznačenou kostrou, (b)–(e) jeho fundamentální soustava kružnic (kružnice tučně).

Tvrzení 10.12 *Fundamentální soustava kružnic vzhledem ke kostře T tvoří bázi prostoru kružnic $\mathcal{C}(G)$.*

Důkaz. Nechť $\mathcal{F}$ je fundamentální soustava kružnic vzhledem ke kostře T. Všimněme si, že každá tětiva e_j kostry T je obsažena v jediném prvku systému $\mathcal{F}$ (totiž ve faktoru C_j). Množina $\mathcal{F}$ tedy musí být lineárně nezávislá, protože pro každý člen C_k v součtu $\sum_j C_j$ (kde e_j probíhá některé tětivy) je k-tá složka výsledného vektoru nenulová.

Našli jsme tedy $m-n+1$ lineárně nezávislých prvků prostoru $\mathcal{C}(G)$, a protože víme, že dimenze tohoto prostoru je $m - n + 1$, musí jít o bázi. □

Podobný postup lze aplikovat v případě prostoru řezů. Nechť e_j je některá z hran kostry T. Odstraníme-li ji, výsledný graf $T-e_j$ bude nesouvislý (to snadno plyne z vlastností stromů) a bude mít právě 2 komponenty. Definujme R_j jako faktor sestávající ze všech hran grafu G, které vedou mezi komponentami grafu $T - e_j$. Snadno se nahlédne, že jeho množina hran je řez. Kostra T má $n - 1$

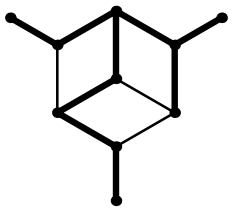
hran, takže tímto způsobem dostaneme $n-1$ faktorů, které dohromady tvoří *fundamentální soustavu řezů* vzhledem ke kostře T.

Každá hrana $e_j \in E(T)$ je hranou jediného faktoru z této fundamentální soustavy řezů, totiž faktoru R_j (cvičení 10.9). Odtud opět plyne, že fundamentální soustava řezů je lineárně nezávislá, a protože $\dim \mathcal{R}(G) = n-1$, dostáváme:

Tvrzení 10.13 *Fundamentální soustava řezů vzhledem ke kostře T tvoří bázi prostoru řezů $\mathcal{R}(G)$.*

Cvičení

▶ **10.8** Určete fundamentální soustavu kružnic a fundamentální soustavu řezů grafu na obr. 10.6 vzhledem k vyznačené kostře.



Obrázek 10.6: Graf ke cvičení 10.8 s tučně vyznačenou kostrou.

▶ **10.9** Dokažte, že každá hrana kostry T je obsažena v právě jednom faktoru z příslušné fundamentální soustavy řezů.

10.7 Nesouvislé grafy

Doposud jsme se zabývali souvislými grafy. Naše úvahy lze uplatnit i na grafy nesouvislé. Nechť graf G má k komponent $C_1, \ldots, C_k$. Zvolme v každé z nich nějakou její kostru T_i $(i = 1, \ldots, k)$. Graf G tak bude obsahovat $n-k$ hran, které patří do nějakého T_i, a $m-n+k$ hran, které do žádné ze zvolených 'koster' nepatří. Stejně jako dříve obdržíme fundamentální soustavu kružnic o $m-n+k$ prvcích a fundamentální soustavu řezů o $n-k$ prvcích. (Ta již není tvořena řezy, které jsme definovali jen v souvislých grafech, ale obecněji separacemi.)

Protože věta 10.9 platí beze změny, dostáváme, že naše fundamentální soustavy jsou i zde bázemi příslušných prostorů.

Věta 10.14 *Má-li graf G k komponent, pak* $\dim \mathcal{C}(G) = m-n+k$ *a* $\dim \mathcal{R}(G) = n-k$. □

Cvičení

▶ **10.10** Proveďte podrobně důkaz věty 10.14.

Kapitola 11

Vzdálenost v grafech

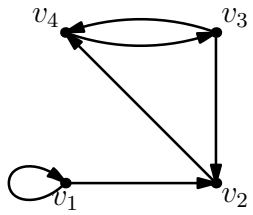
V každém grafu lze přirozeným způsobem definovat vzdálenost libovolné dvojice vrcholů. Hlavním výsledkem této kapitoly je překvapivé tvrzení, podle kterého lze vzdálenosti v grafu zjistit z mocnin jeho matice sousednosti.

11.1 Matice sousednosti a počty sledů

Definice 11.1 Nechť G je orientovaný graf na vrcholech $\{v_1, \ldots, v_n\}$. *Matice sousednosti* grafu G je reálná matice o rozměrech $n \times n$, definovaná předpisem $S(G) = (\sigma_{ij})$, kde

$$\sigma_{ij} = \begin{cases} 1 & \text{pokud } v_i v_j \in E(G), \\ 0 & \text{jinak} \end{cases}$$

pro $i, j = 1, \ldots, n$.



Obrázek 11.1: Orientovaný graf.

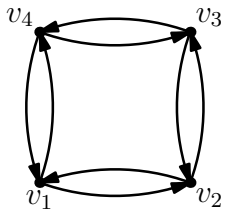
Například graf na obr. 11.1 má matici sousednosti

$$S(G) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Matice sousednosti *neorientovaného* grafu je definována jako matice sousednosti jeho symetrické orientace. (Připomeňme, že symetrická orientace je orientovaný graf, který vznikne, pokud každou hranu nahradíme dvojicí protichůdných orientovaných hran.)

Při počítání matice sousednosti například pro neorientovaný cyklus C_4 o délce 4 musíme tedy přejít k orientovanému grafu na obr. 11.2 a zjistíme, že matice sousednosti je

$$S(C_4) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$



Obrázek 11.2: Symetrická orientace cyklu délky 4.

Z matice $S(G)$ lze poměrně jednoduše zjistit počet všech sledů se zadaným začátkem, koncem a délkou v orientovaném grafu G. Pro $k > 0$ budeme symbolem $\sigma_{ij}^{(k)}$ označovat prvek na pozici (i, j) v k-té mocnině matice $S(G)$. Nultá mocnina této matice je definována jako identická matice E_n. Pro vrcholy $x, y \in V(G)$ budeme pojmem *xy-sled* rozumět sled z x do y v grafu G.

Věta 11.2 *Nechť G je orientovaný graf a $k \geq 0$. Prvek $\sigma_{ij}^{(k)}$ matice $(S(G))^k$ je roven počtu v_iv_j-sledů délky přesně k v grafu G.*

Důkaz. Označme počet v_iv_j-sledů délky k jako P_{ij}^k. Dokazujeme tedy, že $P_{ij}^k = \sigma_{ij}^{(k)}$. Pro stručnost budeme psát $E = E(G)$. Důkaz provedeme indukcí podle k.

Pro $k = 0$ je matice $(S(G))^k$ rovna identické matici, takže $\sigma_{ij}^{(0)} = 1$, právě když $i = j$. Na druhou stranu sled délky 0 z v_i do v_j existuje, právě když $i = j$, a pak je právě jeden. Odtud $P_{ij}^0 = \sigma_{ij}^{(0)}$. Případ $k = 0$ je tedy probrán.

Nechť je tvrzení dokázáno pro $k' < k$. Uvažme libovolný v_iv_j-sled

$$(z_0, z_1, \ldots, z_{k-1}, z_k)$$

délky k (takže $z_0 = v_i$ a $z_k = v_j$). Vynecháme-li poslední vrchol, dostaneme v_iz_{k-1}-sled délky $k - 1$, z jehož posledního vrcholu vede hrana do v_j. Naopak každý sled délky $k - 1$, který začíná ve vrcholu v_i a končí ve vrcholu, ze kterého

vede hrana do v_j, určuje v_iv_j-sled délky k. Jak lze snadno ověřit, jedná se o bijektivní vztah mezi sledy těchto dvou typů.

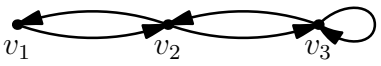
Počet v_iv_j-sledů délky k je tedy roven celkovému počtu v_iv_ℓ-sledů délky $k-1$, kde v_ℓ probíhá všechny vrcholy s vlastností $v_\ell v_j \in E$. Proto platí

$$\begin{aligned} P_{ij}^k &= \sum_{v_\ell:\ v_\ell v_j \in E} P_{i\ell}^{k-1} = \sum_{v_\ell:\ v_\ell v_j \in E} \sigma_{i\ell}^{(k-1)} \\ &= \sum_{\ell=1}^{n} \sigma_{i\ell}^{(k-1)} \cdot \sigma_{\ell j}^{(1)} \\ &= \sigma_{ij}^{(k)}, \end{aligned}$$

kde druhá rovnost plyne z indukčního předpokladu a poslední z definice násobení matic $(S(G))^{k-1}$ a $S(G)$. □

Uvažme jako příklad sledy délky 3 v orientovaném grafu G na obr. 11.3. Jeho matice sousednosti a třetí mocnina této matice vypadají takto:

$$S(G) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \qquad (S(G))^3 = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 3 \end{bmatrix}.$$



Obrázek 11.3: Orientovaný graf na 3 vrcholech.

Z matice $(S(G))^3$ lze například vyčíst, že v grafu G existuje jeden v_3v_1-sled délky 3 (totiž $v_3v_3v_2v_1$) nebo tři v_2v_3-sledy délky 3: jsou to $v_2v_1v_2v_3$, $v_2v_3v_2v_3$ a $v_2v_3v_3v_3$.

Příklad 11.3 Uvažme neorientovanou kružnici C_4 délky 4 s vrcholy očíslovanými proti směru hodinových ručiček. Určeme počty sledů délky 4 mezi různými dvojicemi vrcholů v tomto grafu. Matici sousednosti grafu C_4 jsme našli na začátku kapitoly (přechodem k symetrické orientaci). Snadno spočítáme, že

$$(S(C_4))^4 = \begin{bmatrix} 8 & 0 & 8 & 0 \\ 0 & 8 & 0 & 8 \\ 8 & 0 & 8 & 0 \\ 0 & 8 & 0 & 8 \end{bmatrix}.$$

Vidíme, že pro sousední vrcholy v_i, v_j neexistuje žádný v_iv_j-sled délky 4, zatímco pokud $i = j$ nebo v_i a v_j jsou protilehlé, pak počet takových sledů je 8. Například (uzavřené) sledy z v_1 do v_1 délky 4 jsou: $v_1v_2v_1v_2v_1$, $v_1v_4v_1v_4v_1$, $v_1v_2v_3v_4v_1$, $v_1v_4v_3v_2v_1$, $v_1v_2v_3v_2v_1$, $v_1v_4v_3v_4v_1$, $v_1v_2v_1v_4v_1$ a $v_1v_4v_1v_2v_1$.

Cvičení

► **11.1** Nechť $L(G)$ je Laplaceova matice neorientovaného grafu G (viz kapitola 9). Určete součet $L(G) + S(G)$.

► **11.2** Kolik sledů délky 4 z v_2 do v_2 existuje v grafu na obr. 11.3? Najděte je.

►► **11.3** Nechť F_k je počet xy-sledů délky k v grafu na obr. 11.4. Určete rekurentní vztah pro posloupnost $(F_1, F_2, \dots)$.

Nápověda: Tato posloupnost se nazývá *Fibonacciho posloupnost*, podrobnosti viz [7].

Obrázek 11.4: Určete počet xy-sledů.

11.2 Vzdálenost

Definice 11.4 *Vzdálenost* $d(x, y)$ vrcholů x, y orientovaného grafu G je délka nejkratší cesty z x do y. Pokud taková cesta neexistuje, položíme $d(x, y) = \infty$.

Pojem vzdálenosti je zde definován pro orientované grafy. Pro grafy neorientované jej můžeme definovat prostřednictvím symetrické orientace. Vzdálenost vrcholů v neorientovaném grafu G je tak jejich vzdálenost v symetrické orientaci tohoto grafu. (Podobně je tomu i u dalších pojmů v tomto oddílu, které nebudeme explicitně definovat pro neorientované grafy.)

Vzdálenost v neorientovaných grafech má vlastnosti metriky.

Tvrzení 11.5 *Nechť G je souvislý neorientovaný graf. Pak funkce $d(x, y)$ je* metrikou *na množině $V(G)$, tj. má následující vlastnosti:*

(1) $d(x, y) \geq 0$, *přičemž* $d(x, y) = 0$, *právě když* $x = y$,

(2) $d(x, y) = d(y, x)$,

(3) $d(x, y) + d(y, z) \geq d(x, z)$ *('trojúhelníková nerovnost').*

Důkaz. Cvičení 11.4. □

Definice 11.6 *Distanční matice* orientovaného grafu G s vrcholy $v_1, \dots, v_n$ je matice

$$D(G) = \Big(d(v_i, v_j)\Big)_{i,j=1}^{n}$$

o rozměrech $n \times n$.

Například distanční matice grafu G na obr. 11.1 je

$$D(G) = \begin{bmatrix} 0 & 1 & 3 & 2 \\ \infty & 0 & 2 & 1 \\ \infty & 1 & 0 & 1 \\ \infty & 2 & 1 & 0 \end{bmatrix}.$$

Distanční matice neorientovaného grafu je definována jako distanční matice jeho symetrické orientace.

Viděli jsme, že matice sousednosti a její mocniny umožňují zjistit počet sledů dané délky mezi dvěma vrcholy. Snadno odvodíme následující tvrzení, ve kterém symbol $\sigma_{ij}^{(k)}$ nadále představuje prvek na pozici (i, j) v k-té mocnině matice sousednosti $S(G)$.

Tvrzení 11.7 *Prvek $d(v_i, v_j)$ distanční matice $D(G)$ je roven nejmenšímu k, pro které $\sigma_{ij}^{(k)} \neq 0$ (případně ∞, pokud takové k neexistuje).*

Důkaz. Nechť M je množina všech k, pro které $\sigma_{ij}^{(k)} \neq 0$. Cesta z v_i do v_j existuje právě tehdy, když existuje nějaký sled z v_i do v_j. Řečeno obráceně, $d(v_i, v_j) = \infty$, právě když $M = \emptyset$. Jsou-li splněny tyto podmínky, tvrzení platí.

Nechť tedy délka nejkratšího sledu z v_i do v_j je k_0. Je jasné, že k_0 je nejmenší prvek množiny M. Z cvičení 8.3 víme, že nejkratší sled z v_i do v_j je nutně cestou, takže také $d(v_i, v_j) = k_0$. Důkaz je hotov. □

Z uvedeného tvrzení dostáváme horní odhad časové složitosti nalezení distanční matice (připomeňme, že o časové složitosti jsme hovořili v oddílu 6.7). Vzhledem k tomu, že vzdálenost libovolných dvou vrcholů je buď menší než n, nebo nekonečná (graf na n vrcholech neobsahuje žádnou cestu délky $\geq n$), stačí pro zjištění matice $D(G)$ spočítat $n - 1$ mocnin matice sousednosti $S(G)$. Výpočet každé mocniny spočívá ve vynásobení dvou matic o rozměrech $n \times n$, které vyžaduje $O(n^3)$ aritmetických operací. Celková doba výpočtu tak bude $O(n^4)$.

Ukažme si aplikaci tvrzení 11.7 na grafu G z obr. 11.1. Jeho distanční matici jsme sice odvodili i přímo z definice, u větších grafů je však mnohem jednodušší použít následující obecný postup. Spočítáme první čtyři mocniny matice sousednosti (včetně nulté). Jednotlivé prvky jsou zvýrazněny v nejnižší mocnině, kde jsou nenulové:

$$(S(G))^0 = \begin{bmatrix} \underline{1} & 0 & 0 & 0 \\ 0 & \underline{1} & 0 & 0 \\ 0 & 0 & \underline{1} & 0 \\ 0 & 0 & 0 & \underline{1} \end{bmatrix}, \qquad (S(G))^1 = \begin{bmatrix} 1 & \underline{1} & 0 & 0 \\ 0 & 0 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & \underline{1} \\ 0 & 0 & \underline{1} & 0 \end{bmatrix},$$

$$(S(G))^2 = \begin{bmatrix} 1 & 1 & 0 & \underline{1} \\ 0 & 0 & \underline{1} & 0 \\ 0 & 0 & 1 & 1 \\ 0 & \underline{1} & 0 & 1 \end{bmatrix}, \qquad (S(G))^3 = \begin{bmatrix} 1 & 1 & \underline{1} & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Pro každý prvek nyní zapíšeme, ve které mocnině je zvýrazněn; dostaneme distanční matici $D(G)$. Všimněme si, že u prvků, které jsou nulové ve všech $(S(G))^k$ pro $k < n$, můžeme psát ∞.

$$D(G) = \begin{bmatrix} 0 & 1 & 3 & 2 \\ \infty & 0 & 2 & 1 \\ \infty & 1 & 0 & 1 \\ \infty & 2 & 1 & 0 \end{bmatrix}.$$

Z mocnin matice sousednosti lze algebraickým způsobem určit, zda je daný graf acyklický.

Tvrzení 11.8 *Orientovaný graf G je acyklický, právě když nějaká mocnina jeho matice sousednosti je nulová.*

Důkaz. '$\Rightarrow$': V acyklickém grafu je každý sled cestou. Má-li graf n vrcholů, pak v něm neexistuje cesta na $n+1$ vrcholech (cesta délky n), a tedy ani žádný sled délky n. Podle věty 11.2 je $(S(G))^n = \mathbf{0}$.

'$\Leftarrow$': Nechť $(S(G))^k = \mathbf{0}$. Podle věty 11.2 v grafu G neexistuje žádný sled délky k. Pokud ovšem G obsahuje nějaký cyklus C, obsahuje také sledy všech délek (stačí obcházet C kolem dokola). Graf G tedy musí být acyklický. □

Časová složitost testování acykličnosti grafu s využitím tvrzení 11.8 je zhruba n^4 (každé z n násobení matic vyžaduje přibližně n^3 operací), takže tento postup je pomalejší než algoritmus popsaný v oddílu 8.3. Tvrzení je zajímavé spíše z opačného hlediska: umožňuje použít grafy ke zjištění, zda matice s prvky 0 a 1 má nějakou nulovou mocninu, a to rychleji než pomocí násobení matic.

Cvičení

► **11.4** Dokažte tvrzení 11.5.

► **11.5** Určete distanční matici neorientované kružnice C_n a orientovaného cyklu $\vec{C}_n$ na n vrcholech.

► **11.6** Dokažte, že leží-li vrcholy v_i, v_j v různých kvazikomponentách orientovaného grafu G, pak $d(v_i, v_j) = \infty$ nebo $d(v_j, v_i) = \infty$.

► **11.7** Jak lze z distanční matice orientovaného grafu poznat, zda je graf silně souvislý?

Kapitola 12

Ohodnocené grafy

V praktických aplikacích teorie grafů zpravidla graf slouží jako nástroj k popisu nějaké struktury. Jednotlivé prvky této struktury mají často přiřazeny nějaké hodnoty (může jít např. o parametry součástek v elektrickém obvodu, délky železničních tratí, ceny za přepravu jednotky zboží nebo propustnosti datových spojů). Zadáním pak je realizovat nějaký cíl (třeba přepravit zboží) optimálním způsobem. Úlohy tohoto typu se nazývají *optimalizační úlohy* a my se v této kapitole s několika z nich seznámíme. Popíšeme přitom několik důležitých algoritmů, zejména Dijkstrův algoritmus pro hledání minimální cesty a hladový algoritmus pro hledání minimální kostry.

12.1 Definice ohodnocených grafů

Uvažme graf, jehož vrcholy jsou evropská města a hrany jsou železniční tratě, které je spojují. Chceme-li najít nejkratší cestu vlakem dejme tomu z Budapešti do Paříže, není ani tak důležité, kolik hran našeho grafu bude tato cesta obsahovat — zajímá nás spíše, kolik kilometrů bude měřit. Bude tedy nutné přidat do grafu dodatečnou informaci o 'délce' jednotlivých hran. Dostaneme tzv. ohodnocený graf.

Definice 12.1 *Ohodnocený orientovaný graf* (G, w) je orientovaný graf G spolu s reálnou funkcí $w : E(G) \to (0, \infty)$. Je-li e hrana grafu G, číslo $w(e)$ se nazývá její *ohodnocení* nebo *váha*.

Podobně je definována neorientovaná verze ohodnoceného grafu. I v tomto oddílu budeme hovořit především o orientovaných grafech, s tím, že k neorientovanému případu lze vždy přejít přes symetrickou orientaci. Ohodnocení hran symetrické orientace grafu (G, w) je přirozeně odvozeno z původního ohodnocení (obě protichůdné hrany vzniklé z neorientované hrany e dostanou ohodnocení $w(e)$).

Často je vhodné uvažovat grafy bez ohodnocení jako speciální případy ohodnocených grafů, v nichž je váha každé hrany rovna jedné. V rámci této představy můžeme definovat následující zobecnění matice sousednosti.

Definice 12.2 *Vážená matice sousednosti* ohodnoceného orientovaného grafu (G, w) s vrcholy $v_1, \ldots, v_n$ je matice $W(G) = (w_{ij})$, kde

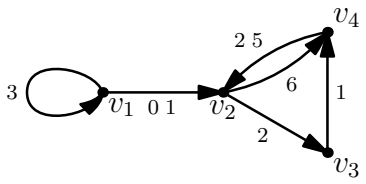
$$w_{ij} = \begin{cases} w(v_i v_j) & \text{pokud } v_i v_j \in E(G), \\ 0 & \text{jinak,} \end{cases}$$

pro $i, j = 1, \ldots, n$.

Všimněme si jedné důležité věci: nezáporné čtvercové matice jednoznačně odpovídají ohodnoceným orientovaným grafům. Například matici

$$W = \begin{bmatrix} 3 & 0.1 & 0 & 0 \\ 0 & 0 & 2 & 6 \\ 0 & 0 & 0 & 1 \\ 0 & 2.5 & 0 & 0 \end{bmatrix}$$

odpovídá graf na obr. 12.1.



Obrázek 12.1: Ohodnocený orientovaný graf G popsaný maticí W.

Přirozeným zobecněním délky cesty v neohodnoceném grafu je její váha.

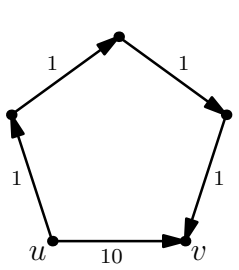
Definice 12.3 Nechť M je množina hran ohodnoceného orientovaného grafu (G, w). *Váha* $w(M)$ množiny M je součet vah jednotlivých hran $e \in M$. Pro stručnost definujeme *váhu* $w(P)$ *cesty* P jako váhu její množiny hran.

Jsou-li u, v vrcholy grafu G, pak *minimální cesta* z u do v je každá cesta, jejíž váha je minimální (tj. žádná cesta z u do v nemá menší váhu). *Vážená vzdálenost* $d^w(u, v)$ vrcholů u, v je váha minimální cesty z u do v.

Poznamenejme, že podle této definice je speciálně $d^w(u, u) = 0$. Dále si všimněme, že minimální cesta z u do v zdaleka nemusí být nejkratší, pokud jde o počet hran. Příkladem je graf na obr. 12.2.

Cvičení

▶ **12.1** Které matice odpovídají ohodnoceným neorientovaným grafům?



Obrázek 12.2: Minimální cesta z u do v nemusí být nejkratší.

12.2 Dijkstrův algoritmus

Jak lze najít váženou vzdálenost vrcholů v ohodnoceném grafu? Asi nejznámějším postupem je *Dijkstrův*[1] *algoritmus*, který si ukážeme v tomto oddílu. Vstupem algoritmu je ohodnocený orientovaný graf (G, w) a vrchol $v \in V(G)$. Jeho výstupem je pro každý vrchol x:

(1) vážená vzdálenost $d^w(v, x)$ vrcholů v a x,

(2) (nějaká) minimální cesta P_x z v do x.

'Počítá' tedy mnohem víc než jen váženou vzdálenost dané dvojice vrcholů.

Algoritmus proběhne v nejvýše n krocích. V celém jeho průběhu bude definován strom T, jehož vrcholy tvoří podmnožinu $V(G)$ (na počátku to bude jediný vrchol v, postupně se T rozšíří až na kostru grafu G). Pro každý vrchol $x \in V(G)$ bude dále určen *odhad vzdálenosti* $c(x)$. I toto číslo se typicky bude měnit a po dokončení algoritmu bude rovno vážené vzdálenosti $d^w(v, x)$. Pro všechny vrcholy z s konečnou nenulovou hodnotou $c(z)$ bude definován jejich *předchůdce* $\bar{z}$.

I. Příprava: T budiž strom na jediném vrcholu v. Položíme $c(v) := 0$. Pro sousedy z vrcholu v položíme

$$c(z) = w(vz) \text{ a } \bar{z} = v.$$

Pro všechny ostatní vrcholy $x \in V(G)$ definujeme $c(x) := \infty$. Předchůdce není určen pro žádný z těchto vrcholů x ani pro vrchol v.

II. Jeden krok algoritmu: Pokud T je kostra grafu G nebo každý vrchol $z \notin V(T)$ má $c(z) = \infty$, přejdeme na bod III. Jinak mezi vrcholy $z \notin V(T)$ vybereme vrchol x, který má minimální hodnotu $c(x)$. Je-li jich víc, zvolíme mezi nimi libovolně. Přidáme do stromu T vrchol x a hranu $\bar{x}x$ (předchůdce vrcholu x je jistě definován, protože $c(x)$ je konečné).

Dále pro všechny vrcholy $z \notin V(T)$, pro něž je xz hranou grafu G, přepočítáme odhad vzdálenosti: je-li $c(x) + w(xz) < c(z)$, položíme $c(z) := c(x) + w(xz)$ a rovněž $\bar{z} = x$. Opakujeme bod II.

[1] Edsger W. Dijkstra (1930–2002).

III. Konec: Pro každý vrchol $x \in V(T)$ je hledanou minimální cestou P_x cesta z v do x ve stromu T (která je jednoznačně určena). Její váha určuje váženou vzdálenost $d^w(v,x)$. Pro ostatní vrcholy x žádná cesta z v do x neexistuje a $d^w(v,x) = \infty$.

Odhadněme nyní pro Dijkstrův algoritmus jeho časovou složitost, jak jsme ji definovali v oddílu 6.7. Přípravná fáze bude pro graf na n vrcholech vyžadovat čas $O(n)$ (pro každý z n vrcholů potřebujeme nastavit odhad vzdálenosti a předchůdce). Krok II. bude proveden maximálně n-krát, protože pro každý vrchol se provádí nejvýše jednou. Jakou časovou složitost má jedno jeho provedení?

Nejprve vybíráme vrchol $x \in V(G) - V(T)$ s minimálním konečným odhadem vzdálenosti. K tomu stačí n operací. Dalších $O(n)$ operací nám zabere přepočítání odhadů vzdálenosti a úprava předchůdců u sousedů vrcholu x. Na jeden krok II. tak stačí $O(n)$ operací. Zjišťujeme tedy, že časová náročnost Dijkstrova algoritmu je $O(n^2)$.

Dijkstrův algoritmus lze použít i pro testování souvislosti neohodnoceného grafu G. Stačí každou hranu symetrické orientace ohodnotit vahou 1 a libovolně zvolit vrchol v. Strom T, nalezený Dijkstrovým algoritmem, je kostrou grafu G, právě když G je souvislý graf. (Platí dokonce, že vrcholy stromu T tvoří komponentu obsahující vrchol v.) Podobným postupem lze testovat i silnou souvislost.

Cvičení

► **12.2** Najděte Dijkstrovým algoritmem minimální cestu z vrcholu u do vrcholu v v grafech na obr. 12.3.

► **12.3** Najděte Dijkstrovým algoritmem minimální cestu z vrcholu u do vrcholu v v grafech na obr. 12.4.

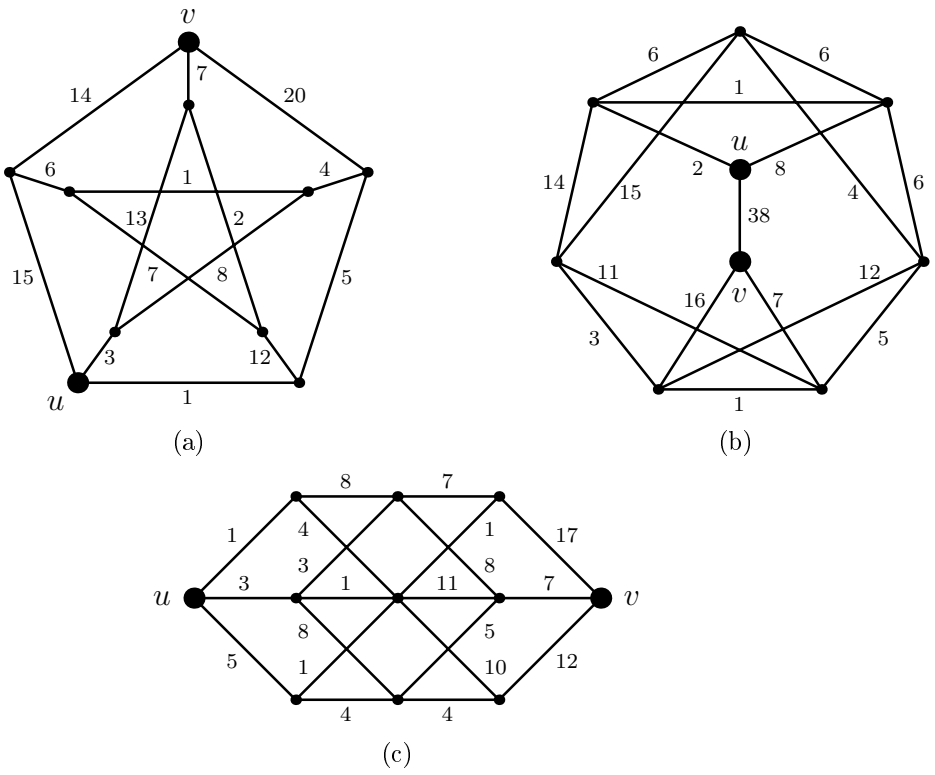
12.3 Matice vážených vzdáleností

K zachycení vážených vzdáleností všech dvojic vrcholů v ohodnoceném orientovaném grafu slouží následující matice.

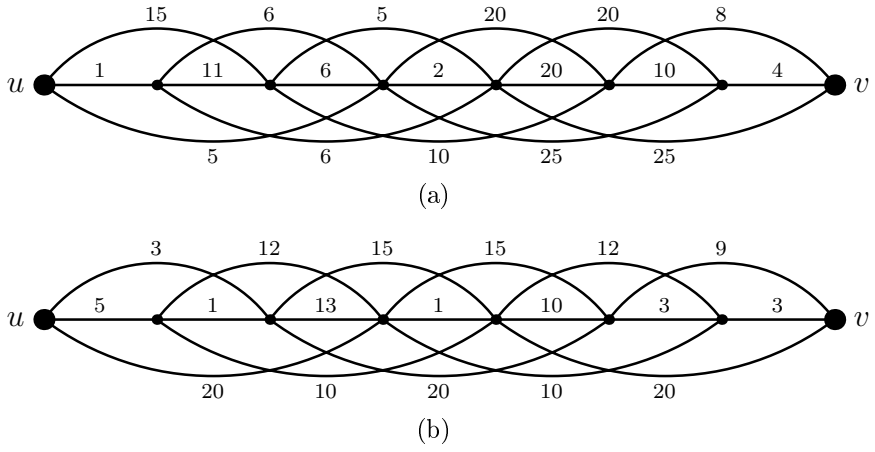
Definice 12.4 *Matice vážených vzdáleností* (též *w-distanční matice*) ohodnoceného orientovaného grafu (G,w) s vrcholy $v_1, \ldots, v_n$ je matice $D^w(G)$ o rozměrech $n \times n$, kde

$$D^w(G) = (d^w(v_i, v_j))_{i,j=1}^n.$$

Jednou možností, jak ji sestrojit, je použít Dijkstrův algoritmus. Ten nám libovolný její řádek najde v čase $O(n^2)$, takže celkový čas výpočtu je $O(n^3)$.



Obrázek 12.3: Najděte minimální cestu z u do v.



Obrázek 12.4: Najděte minimální cestu z u do v.

Ukážeme si jinou jednoduchou metodu, která pracuje v o něco horším čase $O(n^4)$. Nejprve pomocná definice. Nechť je dáno $k \geq 1$. Cesta z v_i do v_j je *k-minimální*, pokud její délka je nejvýše k a pokud žádná jiná cesta z v_i do v_j o délce nejvýše k nemá menší váhu.

Označme jako D_k matici, jejíž prvek d_{ij}^k na pozici (i,j) je roven váze k-minimální cesty z v_i do v_j (případně má hodnotu ∞, pokud taková cesta neexistuje). Vzhledem k tomu, že každá cesta má délku nejvýše $n-1$, musí být matice D_{n-1} rovna hledané w-distanční matici $D^w(G)$. Otázkou tedy je, jak matice D_k sestrojit. Pro $k=1$ je to snadné — pro prvky d_{ij}^1 zjevně platí:

$$d_{ij}^1 = \begin{cases} 0 & \text{pro } i=j, \\ w(v_iv_j) & \text{pro } ij \in E(G), \\ \infty & \text{jinak.} \end{cases}$$

Matice D_1 tedy bude téměř shodná s váhovou maticí $W(G)$, až na to, že nuly *mimo hlavní diagonálu* jsou v matici D_1 nahrazeny hodnotami ∞.

Dejme tomu, že již známe matici D_k a chceme sestrojit matici D_{k+1}. Začněme pozorováním. Nechť P je k-minimální cesta z v_i do v_j. Odebráním posledního vrcholu vznikne cesta P' z v_i řekněme do v_p. Tato cesta musí být $(k-1)$-minimální, jinak bychom dostali spor s k-minimalitou cesty P. Odtud vidíme, že pro délku d_{ij}^k k-minimální cesty z v_i do v_j platí

$$d_{ij}^k = d_{ip}^{k-1} + w(v_pv_j)$$

pro nějaký vrchol v_p s vlastností $v_pv_j \in E(G)$. Přestože předem nevíme, o který vrchol v_p se jedná, můžeme psát

$$d_{ij}^k = \min_{\ell=1}^{n} \left(d_{i\ell}^{k-1} + d_{\ell j}^1 \right), \tag{12.1}$$

přičemž využíváme fakt, že pokud $v_\ell v_j \notin E(G)$, pak $d_{\ell j}^1 = \infty$, takže v minimu bude daný součet zanedbán.

Všimněme si, že vzorec (12.1) nápadně připomíná definici násobení matic — pouze obsahuje minimum na místě sumy a součet na místě součinu. Skutečně, pokud na reálných číslech 'předefinujeme' sčítání a násobení předpisem

$$x \boxplus y = \min(x,y),$$
$$x \boxdot y = x + y,$$

pak platí, že matice D_{k+1} je součinem matic D_k a D_1 vzhledem k operacím $\boxplus$ a $\boxdot$. Indukcí snadno dostaneme následující větu.

Věta 12.5 *Matice D_k je k-tou mocninou matice D_1 vzhledem k operacím $\boxplus$ a $\boxdot$.* □

Vidíme, že ke spočítání matice $D^w(G)$ stačí provést $n-2$ 'vynásobení' maticí D_1. Následující tvrzení říká, že tento proces lze navíc přerušit již v okamžiku, kdy se 'vynásobením' matice poprvé nezměnila.

Tvrzení 12.6 *Pokud pro nějaké $q \geq 1$ platí $D_{q+1} = D_q$, pak D_q je hledanou maticí $D^w(G)$.*

Důkaz. Dokážeme indukcí, že za daného předpokladu pro všechna $k > q$ platí

$$D_k = D_q. \qquad (*)$$

Pro $k = q + 1$ je tvrzení pravdivé. Dejme tomu, že je chceme dokázat pro dané $k \geq q + 1$ za předpokladu, že pro $k - 1$ tvrzení (*) platí.

Podle indukčního předpokladu můžeme člen $d_{i\ell}^{k-1}$ ve vzorci (12.1) nahradit hodnotou $d_{i\ell}^{q}$. Dostáváme tak rovnost $d_{ij}^{k} = d_{ij}^{q+1}$. Proto $D_k = D_{q+1}$ a tím pádem $D_k = D_q$. Tvrzení (*) je tak dokázáno pro všechna $k > q$.

Důkaz je u konce, jakmile si všimneme, že pro každé $k \geq n-1$ je $D_k = D^w(G)$. □

Cvičení

► **12.4** Najděte matici vážených vzdáleností $D^w(\vec{G})$ ohodnoceného orientovaného grafu $\vec{G}$, který je dán následující maticí sousednosti:

(a)
$$W(\vec{G}) = \begin{bmatrix} 0 & 3 & 1 & 0 \\ 1 & 0 & 0 & 3 \\ 8 & 2 & 0 & 2 \\ 0 & 7 & 6 & 0 \end{bmatrix},$$

(b)
$$W(\vec{G}) = \begin{bmatrix} 0 & 0 & 1 & 9 & 7 \\ 9 & 0 & 10 & 3 & 3 \\ 4 & 7 & 0 & 4 & 11 \\ 0 & 5 & 2 & 0 & 0 \\ 6 & 6 & 0 & 1 & 0 \end{bmatrix},$$

(c)
$$W(\vec{G}) = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}.$$

(d)

$$W(\vec{G}) = \begin{bmatrix} 0 & 2 & 4 & 0 & 6 \\ 6 & 0 & 1 & 6 & 14 \\ 9 & 2 & 0 & 3 & 6 \\ 0 & 3 & 4 & 0 & 1 \\ 8 & 5 & 8 & 2 & 0 \end{bmatrix}.$$

12.4 Minimální kostra

Téma tohoto oddílu úzce souvisí s pojmem minimální cesta. Omezíme se na ohodnocené *neorientované* grafy.

Dejme tomu, že potřebujeme propojit n měst rozvodem elektrické energie. Pro každá dvě sídla známe náklady na přímé spojení a chceme, aby celková cena byla co nejnižší. Situaci lze modelovat grafem G, jehož vrcholy odpovídají městům a váhy hran cenám spojení. Uvažované rozvody energie odpovídají souvislým faktorům grafu G (musí totiž být také 'souvislé' a pokrývat všechna města). Faktor, který obsahuje nějakou kružnici, nemůže určovat nejlevnější řešení, neboť odstraněním libovolné hrany této kružnice snížíme cenu a faktor zůstane souvislý. Hledaný faktor F je tedy kostrou grafu G, a to kostrou, která má nejmenší možnou váhu.

Definice 12.7 Kostra T ohodnoceného neorientovaného grafu G je *minimální*, pokud má mezi všemi kostrami minimální váhu $w(T) = w(E(T))$ (viz definice 12.3).

Uvedeme tzv. *hladový algoritmus* pro hledání minimální kostry souvislého grafu G, který jako první formuloval český matematik Otakar Borůvka (1899–1995). Zaveďme následující označení: je-li H graf a e hrana s koncovými vrcholy z $V(H)$, pak $H + e$ je graf, který vznikne přidáním hrany e ke grafu H.

Algoritmus pracuje v $n - 1$ krocích. V i-tém kroku je definován faktor L_i, který neobsahuje kružnice. (Protože graf bez kružnic je disjunktním sjednocením stromů, označujeme ho jako *les*.) Výsledný faktor L_{n-1} je, jak uvidíme, minimální kostrou.

Výchozí les L_0 sestává z izolovaných vrcholů, tj. $E(L_0) = \emptyset$. Uvažme i-tý krok algoritmu. Naší snahou je rozšířit faktor L_{i-1} přidáním jedné hrany na faktor L_i. Některé hrany ale přidat nemůžeme, protože bychom vytvořili kružnici. Z hran, které přidat lze, vyberme hranu e_i s nejmenší vahou[2] a položme

$$L_i = L_{i-1} + e_i.$$

Musíme ještě ukázat, že hrana e_i s požadovanou vlastností vůbec existuje. To je snadné: graf L_{i-1} má n vrcholů a méně než $n - 1$ hran. Podle věty 6.11 je

[2]Algoritmus bere v každém kroku 'nejlehčí' hranu, která přichází v úvahu — odtud název *hladový*.

tedy nesouvislý. Graf G je ovšem souvislý, takže mezi některými dvěma komponentami grafu L_{i-1} vede alespoň jedna hrana. Přidáním této hrany kružnici jistě nevytvoříme.

Popsali jsme způsob nalezení kostry L_{n-1}. Dokažme nyní, že tato kostra je minimální.

Věta 12.8 *Nechť G je ohodnocený neorientovaný graf. Kostra L_{n-1}, nalezená hladovým algoritmem, je minimální kostrou grafu G.*

Důkaz. Nechť $L = L_{n-1}$ je kostra grafu G, získaná hladovým algoritmem. Pro důkaz sporem předpokládejme, že není minimální kostrou, a ze všech minimálních koster zvolme takovou kostru M, která má s kostrou L společný největší počet hran.

Vezměme nejmenší i, pro které platí, že $e_i \notin E(M)$ (připomeňme, že e_i je hrana přidávaná v i-tém kroku algoritmu). Pak jistě $E(L_{i-1}) \subset E(M)$. Protože koncové vrcholy x, y hrany e_i jsou ve stromu M spojeny právě jednou cestou (věta 7.3), graf $M + e_i$ obsahuje právě jednu kružnici C.

Nechť f je libovolná hrana kružnice C, která není obsažena ve stromu L. Graf $L_{i-1} + f$ je podgrafem kostry M, a neobsahuje tedy kružnice. Přidání hrany f tak přichází v úvahu v i-tém kroku hladového algoritmu. Protože byla místo ní přidána hrana e_i, musí být

$$w(e_i) \leq w(f). \tag{12.2}$$

Odstraněním hrany f z grafu $M + e_i$ zanikne jediná jeho kružnice. Výsledný graf M' je tedy stromem, a tím pádem kostrou grafu G. Díky nerovnosti (12.2) není jeho váha větší než váha minimální kostry M. Přitom platí

$$|E(M') \cap E(L)| > |E(M) \cap E(L)|,$$

což je ve sporu s výběrem kostry M. Tento spor ukazuje, že kostra L je minimální. □

Jaká je časová složitost hladového algoritmu? Ukážeme, že při vhodné implementaci jím lze minimální kostru najít v čase $O(mn)$, kde m je počet hran a n počet vrcholů vstupního grafu G. (Složitost je v tomto případě vyjádřena jako funkce dvou proměnných, ne jenom počtu vrcholů n.)

Počet kroků algoritmu je $n-1$, protože v každém kroku přidáme jednu z hran kostry L. V každém kroku musíme pro každou z $O(m)$ zbývajících hran zjistit, zda jejím přidáním vznikne kružnice. To by při nešikovné implementaci vyžadovalo čas $O(n)$, takže celková složitost této implementace by byla $O(mn^2)$. Lze však ušetřit pomocí následujícího vylepšení, známého jako *Kruskalův algoritmus*.

Seřadíme vrcholy do posloupnosti $v_1, \ldots, v_n$. Pro každý vrchol v_j budeme udržovat číslo $m(v_j)$, které udává minimum z indexů všech vrcholů, které leží ve stejné komponentě jako v_j. V rámci přípravné fáze algoritmu pro každé j položíme

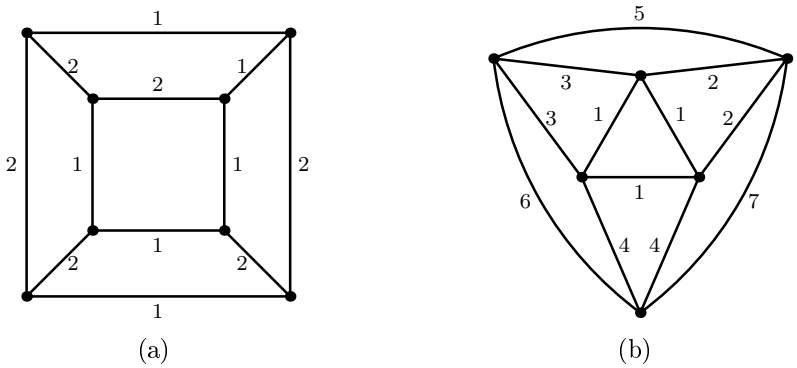
$m(v_j) := j$. Po každém provedeném kroku algoritmu přepočítáme hodnoty $m(v_j)$ (přidáním hrany se spojí dvě komponenty faktoru L_i, takže v jedné z nich je třeba hodnoty upravit). Ke zjištění, zda přidáním hrany v_jv_k vznikne kružnice, nyní stačí porovnat hodnoty $m(v_j)$ a $m(v_k)$: kružnice vznikne právě tehdy, když jsou shodné.

Analyzujme složitost vylepšené verze algoritmu. Přípravná fáze zabere $O(n)$ operací na inicializaci hodnot $m(v_j)$. Následuje $O(n)$ kroků algoritmu. V rámci každého z nich je třeba pro každou z $O(m)$ hran provést konstantní počet[3] operací (porovnání hodnot $m(v_j)$). Z hran, které lze přidat, vybereme tu s minimální vahou, a *poté* v čase $O(n)$ přepočítáme hodnoty $m(v_j)$. Dostáváme tedy celkový odhad $O(mn)$.

Cvičení

► **12.5** Je pravda, že je-li T minimální kostra ohodnoceného neorientovaného grafu G a $u, v \in V(G)$, pak cesta z u do v v kostře T je minimální cestou z u do v v G? Dokažte nebo najděte protipříklad.

► **12.6** Pomocí hladového algoritmu najděte minimální kostry grafů na obrázku 12.5.



Obrázek 12.5: Najděte minimální kostry.

12.5 Problém obchodního cestujícího

Všechny úlohy, které jsme zatím v kapitole 12 zkoumali, byly řešitelné efektivními algoritmy. Nyní stručně popíšeme problému, u kterého se situace zdá být odlišná. Jedná se o tzv. *úlohu obchodního cestujícího*.

[3]Konstantní zde znamená 'nezávislý na m a n'. Konstantní veličinu lze v rámci používaného formalismu značit symbolem $O(1)$.

Obchodní cestující má za úkol objet všechna města v daném kraji, a to po nejkratší možné trase (měřeno počtem ujetých kilometrů). Každé město musí navštívit právě jednou a má skončit ve výchozím bodě.

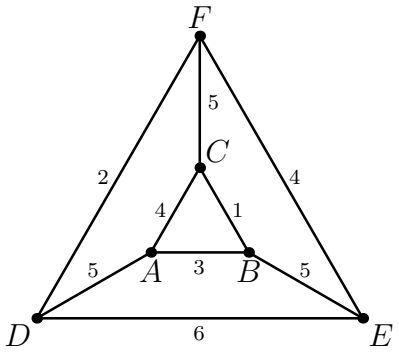
Reformulace problému v jazyce teorie grafů je nasnadě: zadáním je ohodnocený neorientovaný graf, jehož vrcholy odpovídají městům, hrany dvojicím měst s přímým silničním spojením, a váha každé hrany je vzdálenost příslušné dvojice měst. Hledaným řešením je hamiltonovská kružnice s nejmenší možnou vahou (*optimální* hamiltonovská kružnice).

Pro grafy malé velikosti lze řešení poměrně rychle najít 'hrubou silou' jako v následujícím příkladu.

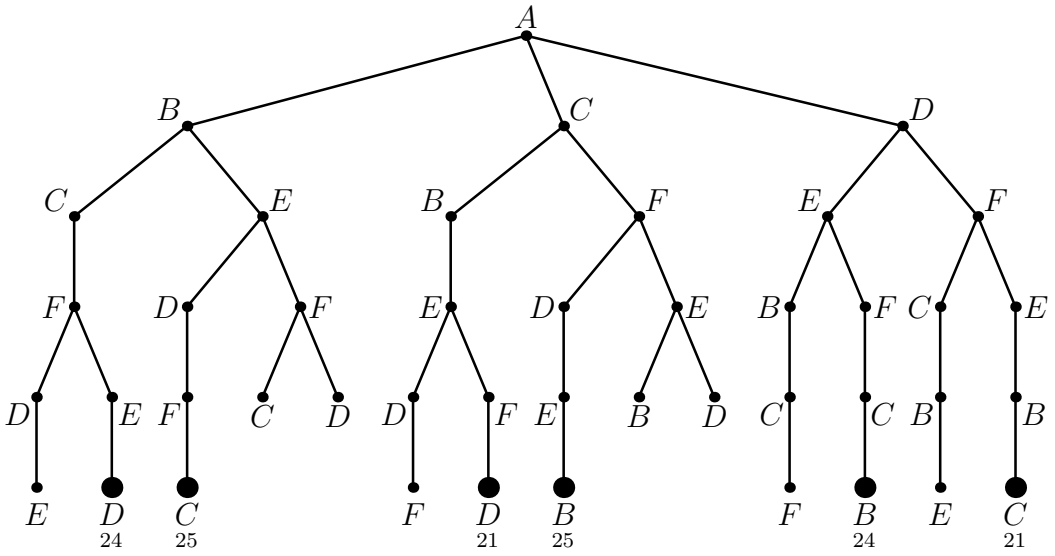
Nechť G je ohodnocený graf na obr. 12.6. Budeme procházet všechny hamiltonovské kružnice v grafu G a hledat mezi nimi optimální řešení. Začneme-li ve vrcholu A, můžeme pokračovat do libovolného z jeho 3 sousedů. Z každého souseda pak lze přejít do dvou dosud nenavštívených vrcholů atd. Nemá-li již aktuální vrchol x žádného nenavštíveného souseda, jsou dvě možnosti. Buďto je možné přejít z x do A a uzavřít tím hamiltonovskou kružnici (pak je nutné porovnat její váhu se stávajícím minimem a případně jej aktualizovat), nebo to možné není a daná větev prohledávání skončila neúspěchem. V každém případě se vrátíme k poslední učiněné volbě a zvolíme další z variant. Jsou-li všechny možnosti probrány, algoritmus končí.

Postup lze přehledně znázornit kořenovým stromem na obr. 12.7 (tzv. *rozhodovací strom*). Kořenu je přiřazen výchozí vrchol A, potomci každého vrcholu odpovídají variantám dalšího prohledávání. Zvýrazněné listy tohoto stromu představují hamiltonovské kružnice (čísla u listů jsou váhy těchto kružnic), ostatní listy představují cesty, které se na hamiltonovské kružnice nedají rozšířit. Úloha má dvě řešení o váze 21.

I na tomto malém příkladu je vidět, že se rozhodovací strom našeho algoritmu může rychle rozrůst. Časová složitost je zhruba dána funkcí $n!$ (roste tedy ještě mnohem rychleji než 2^n). Např. u úplného grafu totiž probíráme všech $(n-1)!$ hamiltonovských kružnic (viz cvičení 12.7).



Obrázek 12.6: Zadání úlohy obchodního cestujícího.



Obrázek 12.7: Rozhodovací strom pro úlohu obchodního cestujícího.

Pro úlohu obchodního cestujícího není znám žádný efektivní algoritmus. Stejně jako problém rozpoznávání hamiltonovských grafů, o kterém jsme hovořili v oddílu 6.6, patří i tato úloha k tzv. NP-úplným problémům.

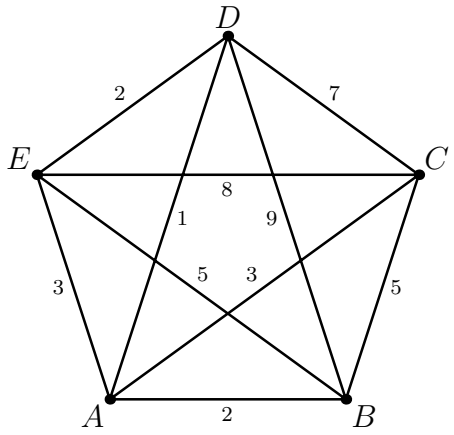
Cvičení

▶ **12.7** Ukažte, že úplný graf na n vrcholech má $(n-1)!$ hamiltonovských kružnic.

▶ **12.8** Pomocí rozhodovacího stromu najděte řešení úlohy obchodního cestujícího pro ohodnocený graf na obr. 12.8.

12.6 Toky v sítích

V této kapitole jsme uvedli jen několik aplikací ohodnocených grafů. Oblastí velmi bohatou na tyto aplikace je také teorie toků v sítích, která se zabývá následující situací. *Síť* je orientovaný graf obsahující dva význačné vrcholy z (zdroj) a s (stok). Každá hrana má určenou *propustnost* (budeme-li si hrany představovat jako potrubí, jde o množství kapaliny, které může hranou za jednotkový čas protéct). *Tok* v této síti je ohodnocení hran s vlastností, že součet ohodnocení hran vstupujících do libovolného vrcholu $x \notin \{z, s\}$ je shodný se součtem ohodnocení hran, které z x vystupují (z x tedy odtéká tolik kapaliny, kolik do něj přiteklo). Cílem je najít *maximální tok*, tj. tok, pro který ze zdroje vytéká maximální množství kapaliny. Existuje věta (tzv. věta o maximálním toku), která toto množství



Obrázek 12.8: Graf ke cvičení 12.8.

jistým elegantním způsobem charakterizuje. Pro nalezení maximálního toku jsou k dispozici efektivní algoritmy. Podrobnější informace k tomuto tématu lze získat mj. v přednáškách [8].

Výsledky cvičení

Kapitola 1

1.1.

$$X \cup Y = \{z : x \in X \text{ nebo } z \in Y\},$$
$$X \cap Y = \{z : x \in X \text{ a } z \in Y\},$$
$$X - Y = \{z : x \in X \text{ a } z \notin Y\}.$$

1.3. A má 2^n podmnožin, z toho 2^{n-1} sudých.

1.4. (a)

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$
$$\binom{6}{3} = 20, \binom{10}{6} = 210, \binom{10}{0} = 1, \binom{0}{0} = 1.$$

1.5. (a) 2^n. (b) 0.

1.8. V obou případech tvrzení platí.

1.9. $L(R) = P(R) = \{3, 4\}$.

1.10.

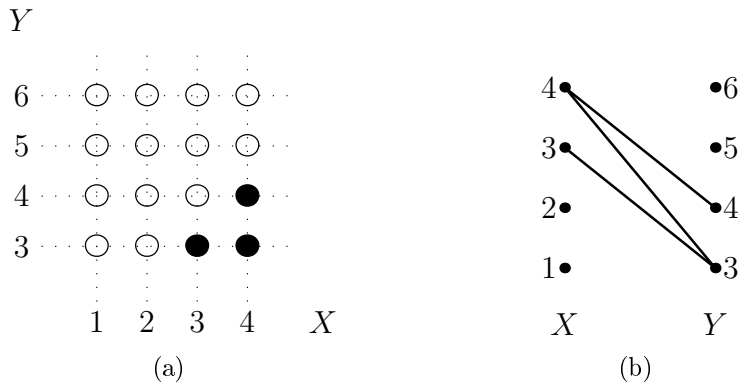
$$R \cup T = \{(1,a),(1,b),(1,c),(2,b),(3,a),(3,b),(4,a),(4,b),(4,c),(4,d)\},$$
$$R \cap T = \{(1,c),(3,a)\},$$
$$R - T = \{(1,a),(2,b),(3,b),(4,b),(4,c),(4,d)\},$$
$$R \triangle T = \{(1,a),(1,b),(2,b),(3,b),(4,a),(4,b),(4,c),(4,d)\}.$$

1.11. 2^{mn}.

1.12. R implikuje S, právě když $R \subset S$.

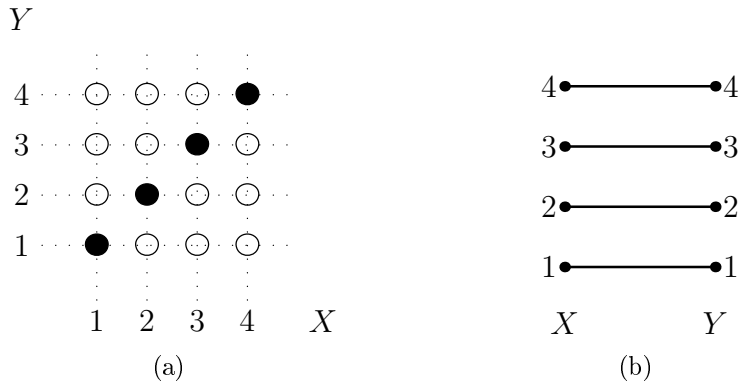
1.13. Obr. 1.1a: např. prvky $L(R)$ odpovídají sloupcům obsahujícím alespoň jeden vyznačený prvek. Na obr. 1.1b odpovídají bodům z množiny X, ze kterých vede alespoň jedna spojnice.

1.14. Viz obr. 12.9.



Obrázek 12.9: Řešení cvičení 1.14.

1.15. Např. pro $X = \{1, 2, 3, 4\}$ viz obr. 12.10.



Obrázek 12.10: Řešení cvičení 1.15.

1.16. Obě složení jsou rovna R.

1.17. (a) Například relace $R = \{(1, 2), (1, 3), (2, 3)\}$ na množině $\{1, 2, 3\}$. (b) Relace E_X na libovolné množině X.

1.18. Jedno je zrcadlovým obrazem druhého podle diagonály.

1.19. Například: (a) prázdná relace na neprázdné množině, (b) relace

$$R = \{(1,1),(1,2),(2,1),(2,2)\}$$

na $X = \{1,2\}$.

1.20. Ne, např. pro $R = \{(1,1),(1,2),(2,2)\}$ a $S = \{(1,2),(2,1)\}$ na $X = \{1,2\}$.

1.21. Vztah (b) v platnosti nezůstane, viz např. relace $R = \{(2,2)\}$, $S = \{(2,1)\}$ a $T = \{(1,1),(1,2),(2,1),(2,2)\}$ na $X = \{1,2\}$.

1.24. (a) m^n. (b) $m(m-1)\dots(m-n+1) = \binom{m}{n} \cdot n!$. (c) $n!$ pokud $m = n$, jinak 0.

1.25. (a) Například $f(n) = 2n$. (b) Například $f(0) = 0$, $f(n) = n-1$ pro $n \geq 1$.

1.26. (a) Je-li $f \circ g$ na, pak g je na, f ne nutně. (b) Je-li $f \circ g$ prostá, pak f je prostá, g ne nutně.

1.27. 'Analogický fakt' je $f \circ p = g \circ p \Rightarrow f = g$.

1.31. Například: (a) $n \mapsto n/2$. (b) $n \mapsto 2n$ pro $n > 0$ a $n \mapsto -2n+1$ pro $n \leq 0$.

1.33. Slabě antisymetrická zobrazení jsou charakterizována např. podmínkou

$$\text{pokud } f(f(x)) = x, \text{ pak } f(x) = x.$$

1.35. Uvádíme zkratky vlastností daných relací (R = reflexívní, A = slabě antisymetrická atd.): (a) RAT, (b) AT, (c) RS, (d) RST, (e) S, (f) RAT, (g) RT, (h) SAT (platí totiž $S = \{(0,0)\}$!), (i) T, (j) RT, (k) nic, (l) RST.

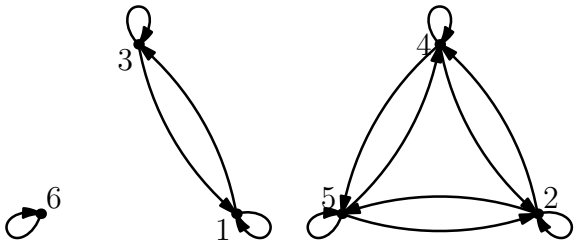
1.36. Ne, viz například prázdná relace.

1.37. Jde právě o podmnožiny identické relace.

1.38. Matice reflexívní relace má na diagonále samé jedničky, matice symetrické relace je symetrická.

1.41. Ano.

1.42. Relace $\sim$ není ekvivalence, protože $p \sim -p$, ale není $-p \sim p$.



Obrázek 12.11: Řešení cvičení 1.48.

1.44. (a) Ne, viz relace $R = \{(1,2),(2,1)\} \cup \Delta$ a $S = \{(2,3),(3,2)\} \cup \Delta$ na množině $\{1,2,3\}$, kde $\Delta = \{(1,1),(2,2),(3,3)\}$. (b) Ne, není reflexívní. (c) Ne, viz cvičení 1.45.

1.46. (a) Ano, přímky rovnoběžné s $y = x$. (b) Ano, přímky rovnoběžné s $y = kx$. (c) Ano, soustředné elipsy.

1.47. Ekvivalence $\approx$ má $n+1$ tříd, ekvivalence $\simeq$ nekonečně mnoho.

1.48. Viz obr. 12.11.

1.49. Matice M je v 'blokovém tvaru', pokud

$$M = \begin{bmatrix} B_1 & 0 & \dots & 0 \\ 0 & B_2 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & B_k \end{bmatrix},$$

kde 'bloky' B_i jsou čtvercové matice složené ze samých jedniček, jejichž diagonály leží na diagonále matice M. V matici $M(R)$ v blokovém tvaru bloky odpovídají třídám ekvivalence R.

Kapitola 2

2.1. Grupa na množině $\{0,a,b,c\}$ s operací $\star$:

$\star$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0.

2.3. Nejmenší příklad tvoří grupa ze cvičení 2.1 spolu s grupou určenou tabulkou

$\star$	0	a	b	c
0	0	a	b	c
a	a	b	c	0
b	b	c	0	a
c	c	0	a	b,

což je v podstatě grupa $\mathbf{Z}_4$, definovaná v oddílu 2.2.

2.4. Když se x a y v i-té souřadnici shodují.

2.5. 25.

2.6. Množina řešení je

$$\{(4t+2, 2, t+1, t) : t \in \mathbf{Z}_5\}.$$

2.7. Těleso $\mathbf{Z}_2$:

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	1
1	1

Těleso $\mathbf{Z}_7$:

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

2.12. Nechť z je reprezentant třídy a. Pokud p dělí z, pak $a = 0$ a inverzní prvek neexistuje. Jinak $(z, p) = 1$, protože p je prvočíslo, a stačí najít koeficient x v rovnosti $zx + py = (z, p)$. Třída $[x]_p$ je inverzní ke třídě a.

2.15. Jde o kritéria: (a) x je dělitelné 3 (resp. 9), právě když má součet cifer dělitelný 3 (resp. 9). (b) Číslo x je dělitelné 8, právě když má poslední trojčíslí dělitelné 8. (c) Číslo x je dělitelné 11, právě když je rozdíl součtu cifer na lichých pozicích a součtu cifer na sudých pozicích dělitelný 11.

Kapitola 3

3.1. (a) ne, (b) ano, neporovnatelné dvojice jsou $\{1,2\}$ a $\{4,5\}$.

3.2. Nechť X je abeceda (množina symbolů) s lineárním uspořádáním $\leq$. Pro slova $a = a_1 \ldots a_m$ a $b = b_1 \ldots b_n$ (kde symboly a_i, b_j jsou z X) položíme $a \preceq b$, právě když existuje $k \leq \min(m,n)$ s vlastnostmi:

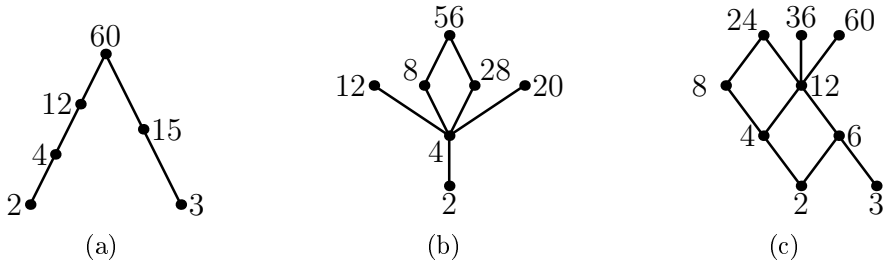
(1) pro každé $j \leq k$ je $a_j \leq b_j$, a dále

(2) buď $k < \min(m,n)$ a $a_{k+1} \leq b_{k+1}$, nebo $k = m$.

Relace $\preceq$ je tzv. *lexikografické uspořádání* na množině slov nad abecedou X.

3.3. Je to prázdná relace.

3.4. Viz obr. 12.12. V příkladu (a) existuje jen největší prvek (60), v příkladu (b) největší (56) i nejmenší (2), v příkladu (c) ani jeden.



Obrázek 12.12: Řešení cvičení 3.4.

3.5. (b) Například množina reálných čísel se standardním uspořádáním (viz cvičení 3.3).

3.6. Například množina všech celých čísel se standardním uspořádáním a s přidaným prvkem $*$, který je menší než 0 a neporovnatelný se všemi zápornými čísly. Prvek $*$ je jediný minimální prvek, ale nejmenší prvek neexistuje.

3.7. (a) Ne, protože $(d,a) \notin R$. (b) Ano, minimální prvky jsou b, e, maximální a, d.

3.8. Například množina $\{1,\ldots,7\}$ s uspořádáním

$$R = \{(i,j) : i \leq 2, j \geq 3\} \cup \{(i,i) : i = 1,\ldots,7\}.$$

3.9. Existují, infimum odpovídá největšímu společnému děliteli, supremum nejmenšímu společnému násobku.

3.12. Jediný minimální prvek je prázdné uspořádání, maximální prvky jsou lineární uspořádání.

3.14. Dokážeme jen neplatnost vztahu (3.1) ve svazu M_5. Nechť x, y, z jsou všechny tři prvky svazu M_5 různé od 0, 1, přičemž $y \leq z$. Potom $z \wedge (x \vee y) = z \wedge 1 = z$, zatímco $(z \wedge x) \vee (z \wedge y) = 0 \vee x = x$, takže distributivita neplatí. U svazu N_5 je rovněž třeba uvážit tři prvky různé od 0, 1.

3.15. Vlastnost neplatí např. pro prvky svazu N_5 různé od $0, 1$.

3.16. Ano.

3.17. Nejmenší prvek je 1, největší 0. Svaz je distributivní: podle cvičení 3.9 infimum čísel a, b odpovídá nejmenšímu společnému děliteli $\mathrm{nsd}(a, b)$, supremum nejmenšímu společnému násobku $\mathrm{nsn}(a, b)$. Protože platí

$$a \cdot b = \mathrm{nsd}(a, b) \cdot \mathrm{nsn}(a, b),$$

podle cvičení 3.15 snadno dostáváme distributivitu daného svazu.

3.18. (b) Ne, například pro $X = \{1, 2, 3, 5, 30\}$ jde o svaz N_5.

3.19.

případ	minimální	maximální	nejmenší	největší	svaz	distributivní
(a)	2	4, 42	2	—	ne	—
(b)	2,3,7	42	—	42	ne	—
(c)	1	30	1	30	ano	ne
(d)	1	36	1	36	ne	—
(e)	1	60	1	60	ano	ne
(f)	1	30	1	30	ano	ano

3.20. Jsou to množiny $\{1, 2, 3, 12\}$, $\{1, 2, 3, 4, 12\}$, $\{1, 4, 6, 12\}$, $\{1, 3, 4, 6, 12\}$.

3.25. Ano.

Kapitola 4

4.1.

případ	svaz	distributivní	komplementární	Booleova algebra
(a)	ne	—	—	—
(b)	ano	ne	ano	ne
(c)	ano	ano	ano	ano
(d)	ano	ano	ne	ne

4.2. Uspořádaná množina $D(n)$ je Booleova algebra, právě když n není dělitelné druhou mocninou žádného prvočísla. (Pokud totiž p^2 dělí n, pak p nemá komplement.)

4.5. Zkratky: R = reflexívní, S = symetrická, A = slabě antisymetrická, T = tranzitivní

případ	R	S	A	T	ekvivalence	uspořádání
(a)	ne	ne	ano	ano	ne	ne
(b)	ne	ano	ne	ne	ne	ne
(c)	ne	ano	ne	ne	ne	ne

4.6. Např. prvek a nemá inverzní prvek vzhledem k násobení.

4.7. Uvedeme pouze tabulku operace + (v obvyklém zápisu, takže např. množinu $\{b, c\}$ označujeme bc).

$+$	0	a	b	c	ab	ac	bc	1
0	0	a	b	c	ab	ac	bc	1
a	a	a	ab	ac	ab	ac	bc	1
b	b	ab	b	bc	ab	1	bc	1
c	c	ac	bc	c	1	ac	bc	1
ab	ab	ab	ab	1	ab	1	1	1
ac	ac	ac	1	ac	1	ac	1	1
bc	bc	1	bc	bc	1	1	bc	1
1	1	1	1	1	1	1	1	1

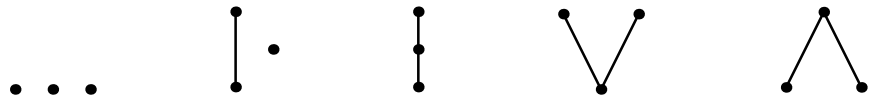
4.10. Atomy jsou: (a) množiny $\{a\}, \{b\}, \{c\}$, (b) jednoprvkové podmnožiny množiny X, (c) prvky 2, 3 a 5.

4.11. Atomy jsou jednoprvkové podmnožiny množiny přirozených čísel.

4.12. (d) Spojení, průsek a komplement lze popsat následovně:

$$[A] \wedge [B] = [A \cap B],$$
$$[A] \vee [B] = [A \cup B],$$
$$\overline{[A]} = [\mathbf{N} - A].$$

4.18. (a) Hasseovy diagramy těchto uspořádaných množin jsou na obr. 12.13. (c) Např. následující uspořádání S, T: uspořádání S je standardní uspořádání přirozených čísel, uspořádání T se s ním shoduje na množině $\{1, 2, \ldots\}$, ale číslo 0 je v něm větší než všechna ostatní čísla.



Obrázek 12.13: Pět neisomorfních tříprvkových uspořádaných množin.

4.19. Množinou atomů direktního součinu $\mathcal{A}_1 \times \mathcal{A}_2$ je kartézský součin $\mathrm{At}(\mathcal{A}_1) \times \mathrm{At}(\mathcal{A}_2)$.

4.20. Hodnoty získáme, pokud v tabulce 4.2 provedeme následující nahrazení:

$$0 \to 00, \qquad a \to 10, \qquad b \to 01, \qquad 1 \to 11.$$

4.21. Výsledkem jsou tyto pravdivostní tabulky:

x	y	$x \to y$	$y + x\bar{y}$
0	0	1	0
0	1	1	1
1	0	0	1
1	1	1	1

4.22. Je to booleovský polynom rovný polynomu x_2.

4.23. Supremum funkcí f, g je funkce, jejíž hodnota v každé n-tici $(a_1, \ldots, a_n) \in \mathcal{B}_2^n$ je supremem hodnot $f(a_1, \ldots, a_n)$ a $g(a_1, \ldots, a_n)$. Podobně infimum a komplement.

4.24. $|F_2| = 16$, $|F_n| = 2^{2^n}$.

4.25. Platí

$$\begin{aligned} \bar{x} &= x \,|\, x, \\ x + y &= \bar{x} \,|\, \bar{y} = (x \,|\, x) \,|\, (y \,|\, y), \\ x \cdot y &= \overline{x \,|\, y} = (x \,|\, y) \,|\, (x \,|\, y). \end{aligned}$$

4.26. (a) Ani v jednom, (b) jen v součinovém, (c) v obou, (d) v obou.

4.27.

$$\begin{aligned} f(x,y,z) &= \bar{x}y\bar{z} + x\bar{y}\bar{z} + x\bar{y}z + xyz \\ &= (x+y+z)(x+y+\bar{z})(x+\bar{y}+\bar{z})(\bar{x}+\bar{y}+z), \\ g(x,y,z) &= \bar{x}\bar{y}\bar{z} + \bar{x}y\bar{z} + \bar{x}yz + x\bar{y}z + xyz \\ &= (x+y+\bar{z})(\bar{x}+y+z)(\bar{x}+\bar{y}+z). \end{aligned}$$

4.28. Například $x\bar{y}\bar{z}$ a $x\bar{y}\bar{z} + x\bar{x}$.

4.29. Věta neplatí, konstantní 1 má vyjádření v úplném součtovém, ale nikoli v úplném součinovém tvaru.

4.30.

$$\begin{aligned} x \to (y \to x) &= xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z} \\ &\quad \text{(vyjádření v úplném součinovém tvaru neexistuje)}, \\ x \oplus (y \to z) &= xy\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z} \\ &= (x+\bar{y}+z)(\bar{x}+y+z)(\bar{x}+y+\bar{z})(\bar{x}+\bar{y}+\bar{z}), \\ \overline{y(x+\bar{y}z)} &= x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z} \\ &= (x+y+z)(x+y+\bar{z})(\bar{x}+\bar{y}+z), \\ ((\bar{x}y) \oplus z)((xz) \to y) &= xyz + \bar{x}y\bar{z} + \bar{x}\bar{y}z \\ &= (x+y+z)(x+\bar{y}+\bar{z})(\bar{x}+y+z)(\bar{x}+y+\bar{z})(\bar{x}+\bar{y}+z). \end{aligned}$$

4.31.

$$\begin{aligned} x \to ((y+\bar{x}z) \oplus \bar{z}) &= xyz + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z} \\ &= (\bar{x}+\bar{y}+z)(\bar{x}+y+\bar{z}), \\ ((x\bar{y}) \oplus (y\bar{z})) \oplus (z\bar{x}) &= xy\bar{z} + x\bar{y}z + xy\bar{z} + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}z \\ &= (x+y+z)(\bar{x}+\bar{y}+\bar{z}). \end{aligned}$$

4.32. 2^n.

Kapitola 5

5.3. Jeden z isomorfismů například přiřazuje vrcholům $1, 2, \ldots, 6$ po řadě vrcholy b, e, f, c, a, d.

5.4. Po řadě $\binom{n}{2}$, 0, $n-1$ a n.

5.6. Všechny vrcholy grafu K_n mají stupeň $n-1$, v grafu D_n jsou všechny stupně 0. V grafu P_n jsou pro $n \geq 2$ dva vrcholy stupně 1, ostatní mají stupeň 2. Graf P_1 má jeden vrchol stupně 0. Všechny stupně v grafu C_n jsou 2.

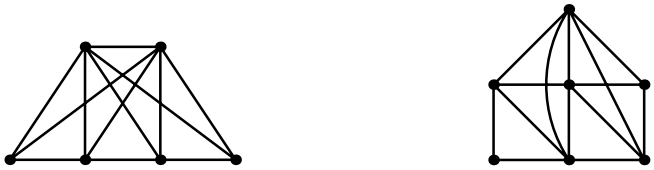
5.7. (a) Pro $p \geq q$ je skóre $(p, p, \ldots, p, q, q, \ldots, q)$, přičemž p se opakuje q-krát a q se opakuje p-krát. (b) $(k, k, \ldots, k)$, kde k se opakuje 2^k-krát.

5.8. Například kružnice C_6 a disjunktní sjednocení dvou kružnic C_3.

5.9. Pro žádné. Graf s n vrcholy nemůže mít vrchol stupně n.

5.10. (a) Viz obr. 12.14a. (b) Viz obr. 12.14b. (c) Neexistuje (součet stupňů je lichý).

5.11. (b) Jde o následující charakterizaci: k-regulární graf na n vrcholech existuje právě tehdy, když $k-1$ dělí n.



(a) (b)

Obrázek 12.14: Příklady řešení cvičení 5.10.

Kapitola 6

6.2. Např. každé prosté zobrazení množiny X do množiny Y je homomorfismus diskrétního grafu s množinou vrcholů X do diskrétního grafu s množinou vrcholů Y a má požadované vlastnosti.

6.5. (a) 3, (b) 4.

6.11. Tah je hranový monomorfismus z cesty P_k do grafu G, uzavřený tah je hranový monomorfismus z kružnice C_k do G.

6.12. Např. $(1, 2, 3, 1, 4, 2, 5, 3, 6, 4, 5, 6, 1)$.

Kapitola 7

7.1. Počet různých stromů je 16, počet neisomorfních 2.

7.2. (a) 1, (b) n, (c) $n^2 + 2n$.

7.3. 3^n.

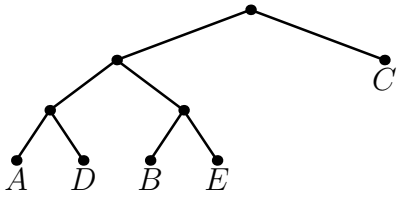
7.4. (a) $n \cdot 2^{n-1}$, (b) $2^{n-1}(n+2)$.

7.7. Průměrná vážená hloubka je 2.36.

7.8. ELEGIE: 10101001000111, LILIE: 010001101000111. Huffmanův kód se 'vyplatí' u prvního slova (má délku 14, zatímco při zakódování každého symbolu trojicí bitů bychom potřebovali 18 bitů. U druhého slova je délka v obou případech stejná.

7.9. LIGA.

7.10. Huffmanův strom je na obr. 12.15. Jeho průměrná vážená hloubka je 2.6.



Obrázek 12.15: Huffmanův strom ve cvičení 7.10.

Kapitola 8

8.2. Například sjednocení orientovaného cyklu na vrcholech a, b, c, d a orientované cesty na vrcholech d, e, f.

8.6. Například $(5, 2, 3, 1, 6, 4)$ nebo $(5, 2, 1, 3, 6, 4)$.

8.7. Například graf G, jehož množinou vrcholů je množina všech celých čísel, a hrany jsou všechny dvojice $(k, k+1)$, kde $k \in \mathbf{Z}$.

8.8. (a) R je reflexívní, právě když u každého vrcholu je smyčka. (b) R je symetrická, právě když ke každé hraně mezi různými vrcholy existuje protichůdná hrana. (c) R je antisymetrická, právě když graf G neobsahuje žádnou dvojici protichůdných hran.

8.11. V obou případech jde o orientovaný graf se dvěma vrcholy spojenými jednou hranou.

Kapitola 9

9.1. (a)

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 \end{bmatrix},$$

(b)

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 & -1 & 0 & 0 \end{bmatrix}.$$

9.2. Liší se jen pořadím řádků a sloupců.

9.3. Ano. Vektory $v_1, \ldots, v_n \in \mathbf{R}^n$ jsou lineárně závislé, právě když matice s řádky $v_1, \ldots, v_n$ má nulový determinant.

9.4. Hodnost je $2k$, hledané množiny obsahují pro každou komponentu právě dva řádky odpovídající jejich vrcholům.

9.5. Počet faktorů je 2^m.

9.6. Je jich 8 (viz také cvičení 7.2c).

9.7. (a) 12. (b) 21. (c) 75. (d) 384.

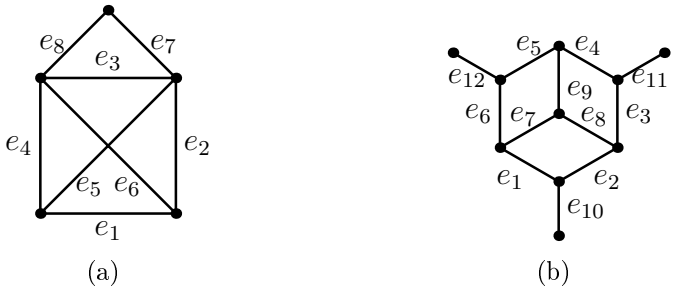
Kapitola 10

10.2. Například sjednocení dvou trojúhelníků se společným vrcholem. Faktor obsahující všechny hrany je sudý, ale není to kružnice.

10.3. Při očíslování hran jako na obr. 12.16 dostaneme matice, které se od následujících liší jen pořadím řádků:

(a)
$$\begin{bmatrix}
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix},$$

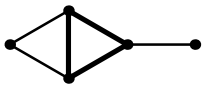
(b)
$$\begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.$$



Obrázek 12.16: Označení hran grafů z cvičení 10.3.

10.4. Např. hvězda vrcholu stupně 3 v grafu na obr. 7.1a není řez.

10.5. Opačná implikace neplatí, např. tučně označená množina hran A na obrázku 12.17 není řezem.



Obrázek 12.17: Příklad k cvičení 10.5.

10.8. Řešení je na obr. 12.18 a 12.19.

Kapitola 11

11.1. Na diagonále jsou stupně vrcholů, jinde 0.

11.2. Pět: $v_2v_1v_2v_1v_2$, $v_2v_3v_2v_1v_2$, $v_2v_1v_2v_3v_2$, $v_2v_3v_2v_3v_2$, $v_2v_3v_3v_3v_2$.

11.3. Jde o vztah

$$F_1 = F_2 = 1,$$
$$F_{i+2} = F_i + F_{i+1},$$

kde $i \geq 1$.

11.5. Pro sudé n je

$$D(C_n) = \begin{bmatrix} 0 & 1 & 2 & \dots & \frac{n}{2}-1 & \frac{n}{2} & \frac{n}{2}-1 & \dots & 2 & 1 \\ 1 & 0 & 1 & \dots & \frac{n}{2}-2 & \frac{n}{2}-1 & \frac{n}{2} & \dots & 3 & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{n}{2} & \frac{n}{2}-1 & \frac{n}{2}-2 & \dots & 1 & 0 & 1 & \dots & \frac{n}{2}-2 & \frac{n}{2}-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 2 & 3 & \dots & \frac{n}{2} & \frac{n}{2}-1 & \frac{n}{2}-2 & \dots & 1 & 0 \end{bmatrix}$$

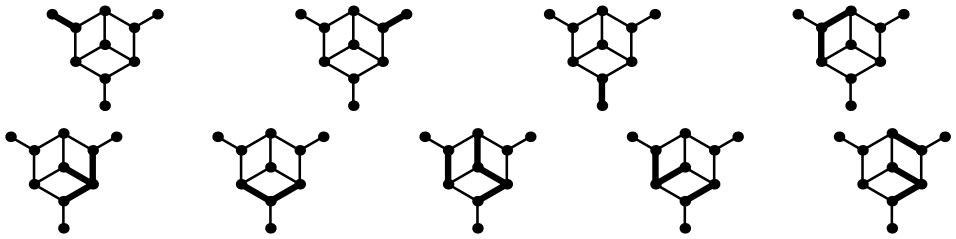
(pro liché n jsou nutné malé změny). Dále je

$$D(\vec{C_n}) = \begin{bmatrix} 0 & 1 & 2 & \dots & n-2 & n-1 \\ n-1 & 0 & 1 & \dots & n-3 & n-2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 2 & 3 & \dots & n-1 & 0 \end{bmatrix}.$$

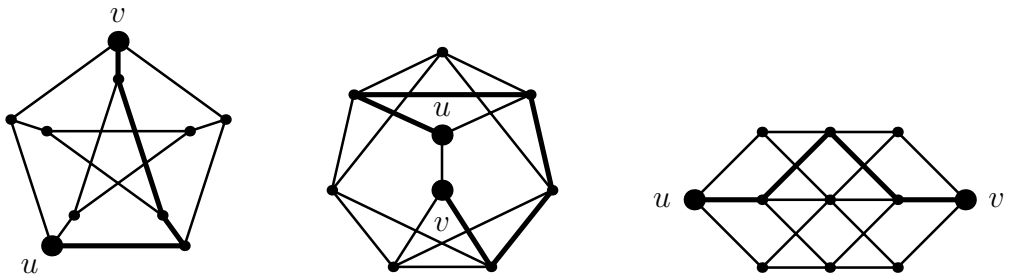
11.7. Graf je silně souvislý, právě když jeho distanční matice neobsahuje položky ∞.

12.1. Čtvercové symetrické nezáporné reálné matice.

Obrázek 12.18: Fundamentální soustava kružnic ve cvičení 10.8 (tučně).



Obrázek 12.19: Fundamentální soustava řezů ve cvičení 10.8 (tučně).



Obrázek 12.20: (Některé) minimální cesty v příkladu 12.2.

12.2. Příklady řešení jsou na obr. 12.20. Váhy minimálních cest jsou: (a) 22, (b) 21, (c) 21.

12.3. Označme vrcholy zleva doprava $u, x_1, x_2, \ldots, x_6, v$. Potom minimální cesta je: (a) (u, x_3, x_2, x_5, v), váha 29, (b) $(u, x_2, x_1, x_4, x_3, x_6, v)$, váha 28.

12.4. Matice vážených vzdáleností jsou:

$$\text{(a)}\ \begin{bmatrix} 0 & 3 & 1 & 3 \\ 1 & 0 & 2 & 3 \\ 3 & 2 & 0 & 2 \\ 8 & 7 & 6 & 0 \end{bmatrix}, \qquad \text{(b)}\ \begin{bmatrix} 0 & 8 & 1 & 5 & 7 \\ 9 & 0 & 5 & 3 & 3 \\ 4 & 7 & 0 & 4 & 10 \\ 6 & 5 & 2 & 0 & 8 \\ 6 & 6 & 3 & 1 & 0 \end{bmatrix},$$

$$\text{(c)}\ \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}, \qquad \text{(d)}\ \begin{bmatrix} 0 & 2 & 3 & 6 & 6 \\ 6 & 0 & 1 & 4 & 5 \\ 8 & 2 & 0 & 3 & 4 \\ 9 & 3 & 4 & 0 & 1 \\ 8 & 5 & 6 & 2 & 0 \end{bmatrix}.$$

Kapitola 12

12.5. Tvrzení neplatí, stačí uvážit trojúhelník s hranami ohodnocenými 2, 2, 3, přičemž u a v jsou koncové vrcholy hrany o váze 3.

12.6. Minimální kostry mají váhu (a) 8, (b) 11. Jejich příklady jsou na obrázku 12.21.

(a) (b)

Obrázek 12.21: Minimální kostry v cvičení 12.6.

12.8. Optimální kružnice je (A, D, E, B, C, A) a má váhu 16.

Literatura

[1] J. Holenda a Z. Ryjáček, *Lineární algebra II.* Skripta, Západočeská univerzita v Plzni, 1997.

[2] L. Kučera, *Kombinatorické algoritmy.* SNTL, Praha, 1983.

[3] L. Lovász, *Combinatorial Problems and Exercises.* Akadémiai Kiadó, Budapest, 1979.

[4] J. Matoušek a J. Nešetřil, *Kapitoly z diskrétní matematiky.* Matfyzpress, Praha, 1996.

[5] L. Procházka, *Algebra.* Academia, Praha, 1990.

[6] E.R. Scheinerman, *Mathematics: A Discrete Introduction.* Brooks/Cole, Pacific Grove, 2000.

[7] N.J.A.S. Sloane, *The On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences`.

[8] *Teorie grafů a diskrétní optimalizace I., II.* Přednášky na Západočeské univerzitě v Plzni.

Rejstřík