Matematika IV – 7. přednáška
Uspořádané množiny, svazy a Booleovy algebry

Michal Bulant

Masarykova univerzita
Fakulta informatiky

31. 3. 2008

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- R. Kučera, *e*-text **Svazy 2003** (`http://www.math.muni.cz/~kucera/texty/Svazy2003.pdf`) a příklady na procvičení (`http://www.math.muni.cz/~kucera/texty/Svazy-dopl.ps`)
- L. Procházka a kol., **Algebra**, Academia, Praha 1990.
- S. MacLane, G. Birkhoff, **Algebra**, Alfa, Bratislava 1974.
- dále *Předmětové záložky v IS MU*

Posety a svazy

Z dřívějška víme, že uspořádání na množině M je relace na M, která je

- reflexivní,
- antisymetrická,
- tranzitivní.

Přitom obecně nemusí být **úplné**, tj. nemusí pro libovolnou dvojici $x, y \in M$ platit $x \leq y$ ani $y \leq x$. Někdy proto zdůrazňujeme, že mluvíme o **částečném uspořádání** a o dvojici $(M, \leq)$ jako o **posetu** (z angl. partially ordered set).

Příklad

- Je-li dána (konečná či nekonečná) množina K, pak na množině $M = 2^K$ všech podmnožin K lze definovat takové uspořádání prostřednictvím inkluze (tj. pro $A, B \subseteq K$ definujeme $A \leq B \iff A \subseteq B$). Obdobně ale uspořádanou množinu tvoří i $(2^K, \supseteq)$.
- Uspořádanou množinu tvoří např. naše běžné číselné obory spolu s operací uspořádání – např. $(\mathbb{Z}, \leq), (\mathbb{N}, \leq), (\mathbb{Q}, \leq)$. Uspořádání na $\mathbb{N}$ je navíc tzv. **dobré** uspořádání, kdy každá neprázdná podmnožina má nejmenší prvek (ikoliv nutně největší). To umožní provádění matematické indukce (tuto vlastnost nemá ani $\mathbb{Z}$, ani $\mathbb{Q}$).
- Poznamenejme, že na $\mathbb{C}$ není žádné uspořádání, které by *přirozeně* vycházelo z uspořádání reálných čísel.
- Uspořádanou množinu tvoří rovněž množina všech kladných dělitelů daného přirozeného čísla n vzhledem k relaci dělitelnosti.(Uvažte, proč nevyhovuje množina **všech** dělitelů). Obecněji, rovněž $(\mathbb{N}, |)$ je uspořádanou množinou.

K uspořádaným množinám se vztahují pojmy:

- nejmenší a největší prvek
- maximální a minimální prvek
- horní (dolní) závora dané množiny
- supremum (infimum) dané množiny

Konečné posety se přehledně zobrazují pomocí orientovaných grafů. Prvky K jsou představovány uzly a hranou jsou spojeny právě prvky v relaci s orientací od většího k menšímu .
Hasseovský diagram posetu je zakreslení takového grafu v rovině tak, že větší prvky jsou zobrazeny vždy výš než menší (a orientace hran je tedy dána takto implicitně) – kvůli přehlednosti, přitom hrany kreslíme pouze tehdy, pokud větší prvek *pokrývá* menší.

Svazy

Definice

Svaz (angl. lattice) je poset $(K, \leq)$, ve kterém má každá dvouprvková množina $\{A, B\}$ supremum $A \vee B$ a infimum $A \wedge B$ v K.
Úplný svaz je pak takový poset, kdy má infimum a supremum každá podmnožina.

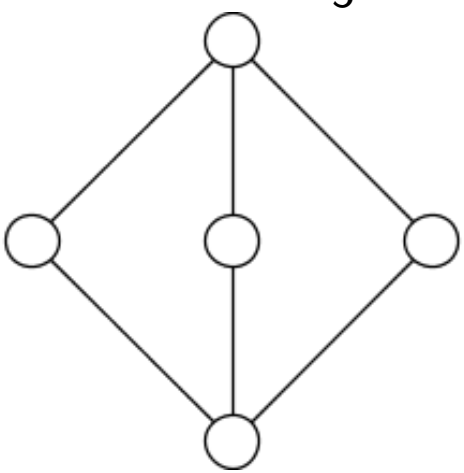
Příklad

- Libovolná úplně uspořádaná množina tvoří svaz – $(\mathbb{R}, \leq)$ apod.
- Poset D_n kladných dělitelů přirozeného čísla n tvoří svaz.
- Poset $(\mathbb{N}, |)$ není je svaz, který není úplný (ale přidáním 0 jej můžeme zúplnit).
- Množina všech (normálních) podgrup dané grupy tvoří úplný svaz.

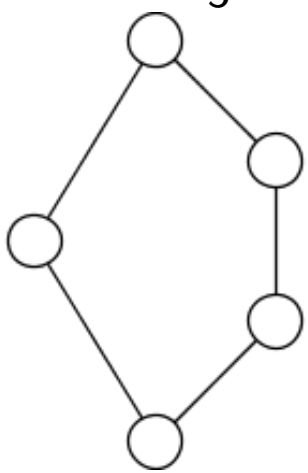
Nedistributivní svazy

Na svazu $(K, \leq)$ tedy máme definovány binární operace $\wedge$ a $\vee$ a přímo z definice je zjevná asociativita a komutativita těchto operací. Často se na svaz díváme jako na algebraickou strukturu $(K, \wedge, \vee)$, přitom lze snadno ukázat, že původní uspořádání lze *znovuobjevit* předpisem $A \leq B \iff A \vee B = B \iff A \wedge B = A$. Snadno lze ale nakreslit Hasseho diagram svazu, který není *distributivní*, tj. operace $\wedge$ a $\vee$ nedistribuují (viz definice okruhu). Lze ukázat, že každý nedistributivní svaz má podsvaz *izomorfní* s jedním z následujících svazů:

svaz M_5



svaz N_5



S každou množinou M máme také množinu $K = 2^M$ všech jejích podmnožin a na ní operace $\vee : K \times K \to K$ sjednocení množin a $\wedge : K \times K \to K$ průniku množin.
To jsou dvě binární operace, které se častěji značí $\cup$ a $\cap$.
Dále máme ke každé množině $A \in K$ také její množinu doplňkovou A', což je další unární operace. Konečně máme *největší objekt*, tj. celou množinu M, který je neutrální vůči operaci $\wedge$ a který proto budeme v této souvislosti označovat jako 1, a obdobně se chová prázdná množina $\emptyset \in K$ vůči operaci $\wedge$. Tu budeme v této souvislosti značit jako 0.

Na množině K všech podmnožin v M přitom platí pro všechny prvky A, B, C následující vlastnosti:

$$A \wedge (B \wedge C) = (A \wedge B) \wedge C, \quad A \vee (B \vee C) = (A \vee B) \vee C \tag{1}$$

$$A \wedge B = B \wedge A, \quad A \vee B = B \vee A \tag{2}$$

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C),$$
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C) \tag{3}$$

existuje 0 tak, že $A \vee 0 = A$ (4)

existuje 1 tak, že $A \wedge 1 = A$ (5)

$$A \wedge A' = 0, \quad A \vee A' = 1. \tag{6}$$

Vlastnost (1) je asociativní zákon pro obě operace, (2) je komutativita, (3) je distributivita obou operací. Poslední vlastnost (6) vystihuje vlastnosti komplementu.

Definice

Množině K spolu se dvěma binárními operacemi $\wedge$ a $\vee$ a jednou unární operací $'$ splňující vlastnosti (1)–(7) říkáme **booleovská (Booleova) algebra**. Operaci $\wedge$ budeme říkat **infimum** (případně **průnik**, anglicky často také **meet**), operaci $\vee$ budeme říkat **supremum** (případně **sjednocení**, anglicky také **join**). Prvku A' se říká **komplement** (**doplněk**) k prvku A.

Všimněme si, že axiomy booleovské algebry jsou zcela symetrické vůči záměně operací $\wedge$ a $\vee$, společně se záměnou prvků 0 a 1. Důsledkem tohoto faktu je, že jakékoliv tvrzení, které odvodíme z axiomů, má také platné **duální tvrzení**, které vznikne z prvého právě záměnou všech výskytů $\wedge$ za $\vee$ a naopak a stejně tak všech výskytů 0 a 1. Hovoříme o **principu duality**.

Stejně jako u speciálního případu booleovské algebry všech podmnožin v dané množině M je komplement k $A \in K$ určen jednoznačně (tj. máme-li dáno $(K, \wedge, \vee)$, může existovat nejvýše jedna unární operace, se kterou dostaneme booleovskou algebru). Skutečně, pokud B a $C \in K$ splňují vlastnosti A', platí

$$B = B \vee 0 = B \vee (A \wedge C) = (B \vee A) \wedge (B \vee C) = 1 \wedge (B \vee C) = B \vee C$$

a podobně také $C = C \vee B$. Je tedy nutně $B = C$.

Poznámka

Pokud ve svazu K existuje ke každému prvku komplement, říkáme, že svaz je komplementární. Takovými jsou např. svazy M_5 i N_5, u nich ovšem není komplement určen jednoznačně (jednoznačnost vynutí až distributivní zákony).

V následujícím výčtu se vlastnostem (2) říká **absorpční zákony**, vlastnosti (3) popisují **idempotentnost** operací a (4) jsou tzv. **De Morganova pravidla**.

Věta

V každé booleovské algebře $(K, \wedge, \vee, ')$ *platí pro všechny prvky v* K

1. $A \wedge 0 = 0, \quad A \vee 1 = 1$
2. $A \wedge (A \vee B) = A, \quad A \vee (A \wedge B) = A$
3. $A \wedge A = A, \quad A \vee A = A$
4. $(A \wedge B)' = A' \vee B', \quad (A \vee B)' = A' \wedge B'$
5. $(A')' = A.$

Alternativní definice booleovské algebry

Věta

Booleovská algebra je distributivní svaz s největším prvkem 1 *a nejmenším prvkem* 0 *takový, že v něm existují ke všem prvkům komplementy.*

Ověřili jsme již, že v takovém případě komplementy jsou definovány jednoznačně, takže je naše alternativní definice booleovské algebry korektní.

Příklad

Protože svaz podgrup dané grupy může mít podsvaz typu M_5, není obecně distributivní a nejde tedy obecně o booleovskou algebru.

Od booleovské algebry zpět k posetu

Libovolná booleovská algebra je posetem ve smyslu uspořádání definovaného $A \leq B$ právě tehdy, když $A \wedge B = A$ (což je totéž jako $A \vee B = B$).
Pak navíc platí:

Lemma

1. $A \wedge B \leq A$
2. $A \leq A \vee B$
3. *jestliže* $A \leq C$ *a zároveň* $B \leq C$, *pak také* $A \vee B \leq C$
4. $A \leq B$ *právě, když* $A \wedge B' = 0$
5. $0 \leq A$ *a* $A \leq 1$ *pro všechny* $A \in K$.

Všimněme si, že stejně jako v případě algebry podmnožin je v Booleovských algebrách $A \wedge B = A$ právě, když je $A \vee B = B$.
Skutečně, je-li $A \wedge B = A$, pak z absorpčních zákonů plyne $A \vee B = (A \wedge B) \vee B = B$, a naopak.

Naši symboliku interpretujeme tak, že z prvků $A, B, \cdots \in K$ tvoříme *slova* pomocí operací $\vee$, $\wedge$, $'$ a závorek vyjasňujících v jakém pořadí a na jaké argumenty jsou operace aplikovány. Samotné axiomy a jejich důsledky pak říkají, že velice často různá slova dávají stejnou hodnotu výsledku v K.

V případě množiny všech podmnožin $K = 2^M$ je to zřejmé – prostě jde o rovnost podmnožin.

Nyní budeme pracovat opět se slovy jako výše, interpretujeme je ale jako tvrzení složené z elementárních výroků $A, B, \ldots$ a logických operací AND (binární operace $\wedge$), OR (binární operace $\vee$) a negace NOT (unární operace $'$). Takové slova nazýváme **výroky** a přiřazujeme jim pravdivostní hodnotu v závislosti na pravdivostní hodnotě jednotlivých elementárních argumentů. Pravdivostní hodnotu přitom bereme jako prvek z triviální Booleovy algebry $\mathbb{Z}_2$, tedy buď 0 nebo 1.
Pravdivostní hodnota výroku je plně určena přiřazením hodnot pro nejjednoduší výroky $A \wedge B$, $A \vee B$ a A', tj. $A \wedge B$ je pravdivé pouze, když jsou oba výroky A a B pravdivé, $A \vee B$ je nepravdivé pouze, když jsou oba výroky nepravdivé a A' má opačnou hodnotu než A.

Výrok obsahující k elementárních výroků tedy představuje funkci $(\mathbb{Z}_2)^k \to \mathbb{Z}_2$ a dva výroky nazýváme logicky ekvivalentní, jestliže zadávají stejnou funkci. Snadno se nyní přímo ověří, že na množině tříd logicky ekvivalentních výroků jsme takto zadefinovali strukturu Booleovy algebry (je pouze třeba projít naše axiomy a ověřit je). Nutně tedy pro výrokovou logiku bude v tomto smyslu platné vše, co dokážeme pro obecné Booleovy algebry.

Stručně si proberme, jak vypadají obvyklé další jednoduché výroky ve výrokové logice jakožto prvky Booleovy algebry (tj. reprezentujeme vždy naším výrazem třídu výroků ekvivalentních):

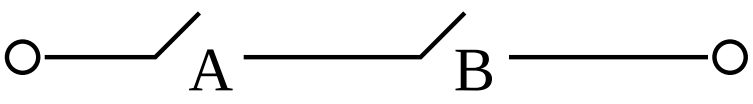
- Implikaci $A \Rightarrow B$ dostaneme jako $A' \vee B$,
- ekvivalenci $A \Leftrightarrow B$ odpovídá $(A \wedge B) \vee (A' \wedge B')$,
- vylučovací OR, neboli XOR, je dáno jako $(A \wedge B') \vee (A' \wedge B)$,
- negace *NOR* operace *OR* je vyjádřena jako $A' \wedge B'$ a
- negace NAND operace AND je dána jako $A' \vee B'$.

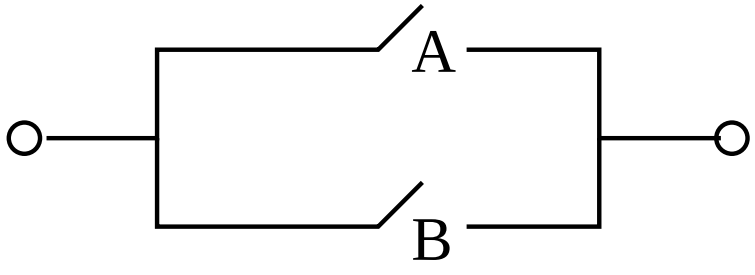
Poznámka

Všimněme si, že *XOR* odpovídá v množinové algebře symetrickému rozdílu množin.
Podobně je možné veškeré základní výrokové spojky realizovat pouze pomocí NAND (příp. NOR) – viz NAND flash paměti (např. USB disky).

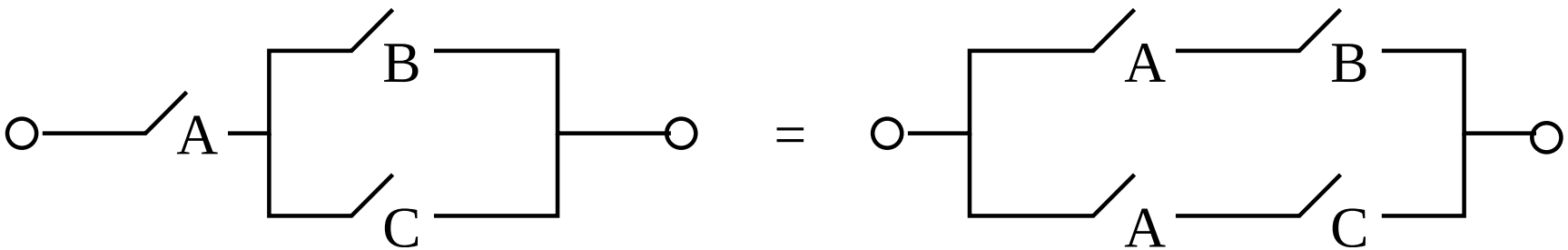
Přepínače

Přepínač je pro nás černá skříňka, která má jen dva stavy, buď je zapnut (a signál prochází) nebo naopak vypnut (a signál neprochází).
Jeden nebo více přepínačů zapojujeme do sítě sériově nebo paralelně. Sériové zapojení je popsáno pomocí binární operace $\wedge$, paralelní je naopak $\vee$. Unární operace A' zadává přepínač, který je vždy v opačné poloze než A.





Každé konečné slovo vytvořené pomocí přepínačů $A, B, \ldots$ a operací $\wedge$, $\vee$ a $'$ umíme převést na obrázek, který bude představovat systém přepínačů propojených dráty a zcela obdobně jako v minulém odstavci nám každá volba poloh jednotlivých přepínačů zadá hodnotu *zapnuto/vypnuto* pro celý systém. Opět se snadno krok po kroku ověří platnost základních axiomů Booleových algeber pro náš systém. Na obrázku je ilustrován jeden z axiomů distributivity. Propojení bez přepínače odpovídá prvku 1, koncové body bez propojení (nebo sériové zapojení A a A') dává prvek 0.



Dělitelé

Dalším přirozeným příkladem Booleovské algebry je systém kladných dělitelů přirozeného čísla.
Zvolme pevně takové číslo $n \in \mathbb{N}$. Za nosnou množinu D_p bereme množinu všech kladných dělitelů d našeho n. Pro dva takové dělitele definujeme $d \wedge e$ jako největší společný dělitel prvků d a e, $d \vee e$ je nejmenší společný násobek. Největším prvkem je $n \in D_n$ (zápis $1 = n$ je v tomto případě poněkud schizofrenní) a neutrálním prvkem vůči supremu je jednička v $\mathbb{N}$. Unární operaci $'$ dostáváme pomocí dělení: $d' = n/d$.

Lemma

Množina D_n spolu s výše uvedenými operacemi $\wedge$, $\vee$ a $'$ je Booleova algebra právě, když rozklad n neobsahuje kvadráty (tj. v jednoznačném rozkladu $n = q_1 \dots q_r$ na prvočísla jsou všechna q_i po dvou různá).

Při diskusi výrokové logiky jsme se potýkali s problémem, co vlastně jsou prvky příslušné Booleovy algebry. Formálně vzato jsme je definovali jako třídy ekvivalentních výroků. Jinak řečeno, pracovali jsme s hodnotovými funkcemi pro výroky s daným počtem argumentů. Vůbec jsme přitom neřešili obtížný problém (tzv. **equivalence checking** je NP těžký), jak rozpoznat stejné výroky v tomto smyslu. Také jsme neřešili, jestli všechny formálně možné hodnotové funkce $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ lze zadat pomocí základních logických operací.

Zcela obdobně se můžeme tázat, jak poznat, zda dva systémy přepínačů mají stejnou funkci. Obdobně jako u výroků zde pro systém s n přepínači pracujeme s funkcemi $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ a zjevně existuje právě 2^{2^n} různých takových přepínacích funkcí. Na těchto funkcích umíme přirozeným způsobem zadat strukturu Booleovy algebry (využíváme, že hodnoty, tj. $\mathbb{Z}_2$ jsou Booleovou algebrou).

Odpovíme nyní na výše uvedené otázky tak, že pro libovolný prvek obecné Booleovy algebry sestrojíme jeho tzv. **normální disjunktivní tvar**, tj. napíšeme jej pomocí vybrané skupiny nejjednodušších prvků a operace $\vee$.

Definice

Prvek $A \in K$ nazveme **atom** v Booleově algebře K, jestliže pro všechny $B \in K$ platí $A \wedge B = A$ (tj. $A \leq B$) nebo $A \wedge B = 0$.

Jinak řečeno, A je atom, když pro všechny ostatní prvky $B \leq A$ implikuje $B = 0$ nebo $B = A$.

Lemma

Booleova algebra funkcí přepínačového systému s n přepínači $A_1, \ldots, A_n$ *má* 2^n *atomů, které jsou tvaru* $A_1^{\sigma_1} \wedge \cdots \wedge A_n^{\sigma_n}$, *kde buď* $A_i^{\sigma} = A_i$ *nebo* $A_i^{\sigma_i} = A_i'$.

Věta

Každý prvek B v konečné Booleově algebře $(K, \wedge, \vee, ')$ lze zapsat jako supremum atomů

$$B = A_1 \vee \cdots \vee A_k.$$

Tato formule je navíc jednoznačná až na pořadí atomů.

Tato věta se dokazuje s pomocí tří jednoduchých tvrzení:

Věta

1. *Jestliže jsou $Y, X_1, \ldots, X_\ell$ atomy v K, pak $Y \leq X_1 \vee \cdots \vee X_\ell$ tehdy a jen tehdy, když $Y = X_i$ pro nějaké $i = 1, \ldots, \ell$.*
2. *Pro každý prvek $Y \neq 0$ v K existuje atom X, pro který je $X \leq Y$.*
3. *Jestliže jsou $X_1, \ldots, X_r$ všechny atomy v K, pak $Y = 0$ právě, když $Y \wedge X_i = 0$ pro všechny $i = 1, \ldots, r$.*

Jak jsme již viděli u mnoha matematických struktur, o objektech se dozvídáme informace pomocí tzv. homomorfismů, tj. zobrazení, které zachovávají příslušné operace. V případě Booleovských algeber definujeme podobně jako u okruhů:

Definition

Zobrazení $f : (K, \wedge, \vee, ') \to (L, \wedge, \vee, ')$ se nazývá **homomorfismus Booleovských algeber**, jestliže pro všechny A, $B \in K$ platí

1. $f(A \wedge B) = f(A) \wedge f(B)$
2. $f(A \vee B) = f(A) \vee f(B)$
3. $f(A') = f(A)'$.

Homomorfismus f je izomorfismem booleovských algeber, jestliže je f navíc bijektivní.

Snadno se ověří, že bijektivnost f již zaručí, že f^{-1} je opět homomorfismem.
Z definice uspořádání na Booleových algebrách je zřejmé, že každý homomorfismus $f : K \to L$ bude také splňovat $f(A) \leq f(B)$ pro všechny prvky $A \leq B$ v K. To je definiční vlastnost pro tzv. **izotonní zobrazení** neboli **homomorfismy posetů**.
Jakkoliv umíme rekonstruovat operace suprema a infima z uspořádání, pokud toto vzniklo z Booleovy algebry, není pravda, že by každý homomorfismus posetů byl automaticky homomorfismem příslušných algeber. Zkuste si najít příklad (stačí vkládat algebru se dvěma atomy do algebry s alespoň čtyřmi atomy)!
To, že struktura Booleových algeber je v podstatě velmi jednoduchá, ukazuje náseldující věta.

Věta

Každá konečná Booleova algebra je izomorfní Booleově algebře $M = 2^K$, kde K je množina atomů v M.