

Drsná matematika IV – 4. přednáška

Uspořádané množiny a Booleovské algebry

Jan Slovák

Masarykova univerzita
Fakulta informatiky

12. 3. 2012

Obsah přednášky

- 1 Literatura
- 2 Množinová algebra
- 3 Výroková logika
- 4 Přepínače a dělitelé
- 5 Posety a svazy
- 6 Normální tvar
- 7 Homomorfismy

Kde je dobré číst?

- vlastní poznámky, texty současného přednášejícího, GOOGLE, atd.
- Riley, K.F., Hobson, M.P., Bence, S.J. Mathematical Methods for Physics and Engineering, second edition, Cambridge University Press, Cambridge 2004, ISBN 0 521 89067 5, xxiii + 1232 pp.
- W. J. Gilbert, W. K. Nicholson, Modern algebra with applications, 2nd ed. John Wiley and Sons (Pure and applied mathematics) ISBN 0-471-41451-4
- Zvára, Štěpán: Pravděpodobnost a matematická statistika ISBN 80-86732-71-7, 4.. vydání, 232 str., Matfyzpres, Praha.

S každou množinou M máme také množinu $K = 2^M$ všech jejích podmnožin a na ní operace $\vee : K \times K \rightarrow K$ sjednocení množin a $\wedge : K \times K \rightarrow K$ 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 \vee . 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:

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

$$A \wedge B = B \wedge A, \quad A \vee B = B \vee A \quad (2)$$

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C), \quad A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C) \quad (3)$$

$$\text{existuje } 0 \text{ tak, že } A \vee 0 = A \quad (4)$$

$$\text{existuje } 1 \text{ tak, že } A \wedge 1 = A \quad (5)$$

$$A \wedge A' = 0, \quad A \vee A' = 1. \quad (6)$$

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

Definition

Množině K spolu s dvěma binárními operacemi \wedge a \vee a jednou unární operací $'$ splňující vlastnosti (1)–(7) říkáme **Booleovská 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 **doplňěk** 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 prvního 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 doplněk 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 $B = C$.

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

Theorem

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

- 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 $(A')' = A.$

Naši symboliku interpretujeme tak, že z prvků $A, B, \dots \in K$ 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.

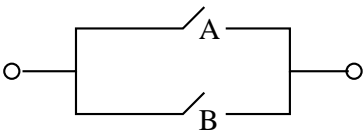
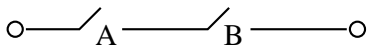
Nyní budeme pracovat opět se slovy jako výše, interpretujeme je ale jako tvrzení složené z elementárních výroků A, B, \dots a logických operací AND (binární operace \wedge), OR (binární operace \vee) a negace NOT (unární operace $'$). Taková slova nazýváme **výroky** a přiřazujeme jim pravdivostní hodnotu 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 $(\mathbb{Z}_2)^k \rightarrow \mathbb{Z}_2$ 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.

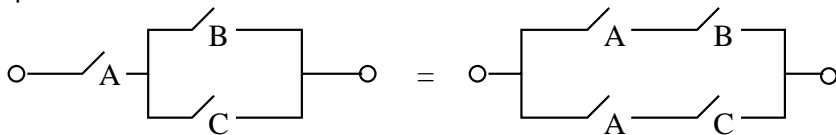
Stručně si proberme, jak vypadají obvyklé další jednoduché výroky ve výrokové logice jakožto prvky Booleovy algebry (tj. reprezentujeme vždy naším výrazem třídu výroků ekvivalentních): Implikaci $A \Rightarrow B$ dostaneme jako $A' \vee B$, ekvivalenci $A \Leftrightarrow B$ odpovídá $(A \wedge B) \vee (A' \wedge B')$. Dále 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 $A' \vee B'$. Všimněme si také, že XOR odpovídá v množinové algebře symetrickému rozdílu množin.

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, \dots 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.



Dalším přirozeným příkladem Booleovské algebry je systém dělitelů přirozeného čísla nebo polynomu.

Zvolme pevně takové číslo $p \in \mathbb{N}$ nebo polynom $p \in \mathbb{K}[x_1, \dots, x_s]$ nad oborem integrity \mathbb{K} s jednoznačným rozkladem. Za nosnou množinu D_p bereme množinu všech dělitelů q našeho p . Pro dva takové dělitele definujeme $q \wedge r$ jako největší společný dělitel prvků q a r , $q \vee r$ je nejmenší společný násobek. Dále klademe $p = 1 \in D_p$ a neutrálním prvkem vůči supremu je jednička v \mathbb{Z} , resp. $1 \in \mathbb{K} \subset \mathbb{K}[x_1, \dots, x_s]$. Unární operaci $'$ dostáváme pomocí dělení: $q' = p/q$.

Lemma

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

Vzpomeňme na definici uspořádání jakožto reflexivní, antisymetrické a tranzitivní relace \leq na množině K . Taková relace obecně neříká o každé dvojici $a, b \in K$ jestli je $a \leq b$ nebo $b \leq a$ (takové uspořádání se nazývá **úplné uspořádání** nebo dobré uspořádání). Často v našem případě obecného uspořádání hovoříme také o **částečném uspořádání** a množina (K, \leq) vybavená částečným uspořádáním se nazývá **poset** (z anglického „partial ordered set“). Takové uspořádání je zejména vždy na množině $K = 2^M$ všech podmnožin množiny M prostřednictvím inkluze podmnožin. Pomocí naší relace infima na K je můžeme definovat jako $A \subset B$ právě, když $A \wedge B = A$. Ekvivalentně, $A \subset B$ právě, když $A \vee B = B$.

Lemma

Je-li $(K, \wedge, \vee, ')$ Booleova algebra, pak relace \leq definovaná vytahem $A \leq B$ právě, když $A \wedge B = A$, je částečné uspořádání. Navíc platí

- 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.

Viděli jsme, že každá Booleova algebra zadává poset (K, \leq) . Zdaleka ne každý poset ovšem vzniká takovýmto způsobem. Např. triviální částečné uspořádání, kdy $A \leq A$ pro všechny A a všechny dvojice různých prvků jsou nesrovnatelné, samozřejmě z Booleovy algebry vzniknout nemůže, pokud je v K více než jeden prvek (viděli jsme, že největší a nejmenší prvek v Booleově algebře je totiž srovnatelný s každým prvkem). Zkusme se zamyslet, do jaké míry lze z uspořádání budovat operace \wedge a \vee .

Pracujme s pevně zvoleným posetem (K, \leq) . O prvku $C \in K$ řekneme, že je **dolní závorou** pro nějakou množinu prvků $L \subset K$, je-li $C \leq A$ pro všechny $A \in L$. Prvek $C \in K$ je **infimem množiny** $L \subset K$, jestliže je dolní závorou a pro každou jinou dolní závoru D téže množiny platí $D \leq C$.

Obdobně definujeme **horní závory** a **supremum** podmnožiny L záměnou \leq za \geq v posledním odstavci.

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. **Hasseho 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).

Definition

Svaz je poset (K, \leq) , ve kterém každá dvouprvková množina $\{A, B\}$ má supremum $A \vee B$ a infimum $A \wedge B$ v K .

Na svazu (K, \leq) tedy máme definovány binární operace \wedge a \vee a přímo z definice je zjevná asociativita a komutativita těchto operací. Snadno lze ale nakreslit Hasseho diagram svazu, který není distributivní.

Nyní můžeme snadno definovat Booleovskou algebru v jazyce svazů: 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.

Všimněme si také, při diskusi dělitelů daného čísla nebo polynomu p jsme narazili na svazy D_p , které jsou Booleovskou algebrou právě tehdy, když rozklad p neobsahuje kvadráty.

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, jak rozpoznat stejné výroky v tomto smyslu. Také jsme neřešili, jestli všechny formálně možné hodnotové funkce $(\mathbb{Z}_2)^n \rightarrow \mathbb{Z}_2$ 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 $(\mathbb{Z}_2)^n \rightarrow \mathbb{Z}_2$ 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 .

Prvek $A \in K$ nazveme **atom** v Booleově algebře K , jestliže pro všechny $B \in K$ platí $A \wedge B = A$ 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, \dots, A_n má 2^n atomů, které jsou tvaru $A_1^{\sigma_1} \wedge \dots \wedge A_n^{\sigma_n}$, kde buď $A_i^{\sigma} = A_i$ nebo $A_i^{\sigma} = A_i'$.

Theorem

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.

Pro důkaz budeme potřebovat tři jednoduchá tvrzení:

Theorem

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

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 $f : (K, \wedge, \vee, ') \rightarrow (L, \wedge, \vee, ')$ 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 izomorfismus Booleovských algeber, jestliže je f 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 $f : K \rightarrow L$ 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)!

Theorem

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