Matematika IV – 9. týden
Systémy polynomiálních rovnic (dokončení), Booleovské algebry

Jan Slovák

Masarykova univerzita
Fakulta informatiky

15. 4. – 19. 4. 2013

Obsah přednášky

Plán přednášky

Theorem (Dělení se zbytkem)

Nechť $<$ *je monomiální a* $F = (f_1, \ldots, f_s)$ *s-tice polynomů v* $\mathbb{K}[x_1, \ldots, x_n]$. *Pak každý* $f \in \mathbb{K}[x_1, \ldots, x_n]$ *lze vyjádřit jako*

$$f = a_1 f_1 + \cdots + a_s f_s + r \quad \text{kde } a_i, r \in \mathbb{K}[x_1, \ldots, x_n] \quad \text{pro } i = 1, 2, \ldots, s$$

a navíc $r = 0$ *nebo* r *je lineární kombinací monomů, z nichž žádný není dělitelný kterýmkoli z* $LT\, f_1, \ldots, LT\, f_s$ *a pokud* $a_i f_i \neq 0$ *pak* multideg $f \geq$ multideg $a_i f_i$ *pro každé* i.
Polynom r *nazýváme* zbytkem po dělení f/F.

Věta neříká nic o jednoznačnosti výsledku. Následující algoritmus dává jedno možné řešení. Nadále budeme výsledkem dělení se zbytkem chápat právě tento výstup pevně zvoleného algoritmu.

1. $a_1 := 0, \ldots, a_s := 0, r := 0, p := f$
2. `while` $p \neq 0$
   1. $i := 1$
   2. $d := \mathit{false}$
   3. `while` $i \leq s \wedge \text{not } d$
      1. `if` $LT\, f_i | LT\, p$
         $a_i := a_i + LT\, p / LT\, f_i$
         $p := p - (LT\, p / LT\, f_i) \cdot f_i$
         $d := \mathit{true}$
      2. `else` $i := i + 1$
   4. `if` not d
      1. $r := r + LT\, p$
      2. $p := p - LT\, p$

V $\mathbb{K}[x_1, \ldots, x_n]$ platí pouze implikace

$$f = a_1 f_1 + \cdots + a_s f_s + 0 \implies f \in \langle f_1, \ldots, f_s \rangle$$

Obrácení obecně neplatí, uvažujme $f = xy^2 - x$, $f_1 = xy + 1$, $f_2 = y^2 - 1$. Potom algoritmus dělení dá

$$f = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

ale přitom evidentně $f = x(y^2 - 1)$, a tedy $f \in \langle f_1, f_2 \rangle$.

Definition

Ideál $I \subseteq k[x_1, \ldots, x_n]$ nazýváme *monomiální*, existuje-li množina $A \subseteq \mathbb{N}^n$ taková, že I se sestává právě ze všech polynomů tvaru $\sum_{\alpha \in A} h_\alpha x^\alpha$, kde $h_\alpha \in k[x_1, \ldots, x_n]$. Potom píšeme $I = \langle x^\alpha,\ \alpha \in A \rangle$.

Zřejmě pro monomiální ideál I platí

$$x^\beta \in I \iff \exists \alpha \in A \colon x^\alpha | x^\beta$$

Lemma

Nechť $I \subseteq k[x_1, \ldots, x_n]$ je monomiální ideál, $f \in k[x_1, \ldots, x_n]$ polynom. Pak následující tvrzení jsou ekvivalentní

1. $f \in I$
2. *Každý člen polynomu f je prvkem I.*
3. *Polynom f je lineární kombinací monomů z I s koeficienty z k.*

Lemma

Nechť $I \subseteq k[x_1, \ldots, x_n]$ je monomiální ideál, $f \in k[x_1, \ldots, x_n]$ polynom. Pak následující tvrzení jsou ekvivalentní

1. $f \in I$
2. *Každý člen polynomu f je prvkem I.*
3. *Polynom f je lineární kombinací monomů z I s koeficienty z k.*

Corollary

Dva monomiální ideály splývají právě tehdy, když obsahují stejné monomy.

Lemma

Nechť $I \subseteq k[x_1, \ldots, x_n]$ je monomiální ideál, $f \in k[x_1, \ldots, x_n]$ polynom. Pak následující tvrzení jsou ekvivalentní

1. $f \in I$
2. *Každý člen polynomu f je prvkem I.*
3. *Polynom f je lineární kombinací monomů z I s koeficienty z k.*

Corollary

Dva monomiální ideály splývají právě tehdy, když obsahují stejné monomy.

Theorem (Dicksonovo lemma)

Každý monomiální ideál $I = \langle x^\alpha,\ \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$ lze psát ve tvaru $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, kde $\alpha_1, \ldots, \alpha_s \in A$.

Je-li $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ nenulový, označme

$$LT\, I := \{ax^\alpha,\ \exists f \in I:\ LT\, f = ax^\alpha\}$$

Zřejmě $\langle LT\, I \rangle$ je monomiální, a tedy podle Dicksonova lemmatu lze psát $\langle LT\, I \rangle = \langle LT\, g_1, \ldots, LT\, g_s \rangle$ pro nějaká vhodná $g_1, \ldots, g_s \in I$.

Theorem (Hilbertova věta)

Každý ideál $I \in \mathbb{K}[x_1, \ldots, x_n]$ je konečně generovaný.

Důkaz.

Pokud by $I = \{0\}$, je tvrzení triviální. Uvažujme tedy $I \supset \{0\}$. Podle Dicksonova lematu a předchozí poznámky existují taková $g_1, \ldots, g_s \in I$, že $\langle LT\, I\rangle = \langle LT\, g_1, \ldots, LT\, g_s\rangle$ Zřejmě $\langle g_1, \ldots, g_s\rangle \subseteq I$. Vezměme libovolné $f \in I$ a proveďme dělení se zbytkem s-ticí $g_1, \ldots, g_s$. Dostáváme

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

kde žádný člen r není dělitelný $LT\, g_1, \ldots, LT\, g_s$.
Protože $r = f - a_1 g_1 - \cdots - a_s g_s$, platí $r \in I$, a tedy $LT\, r \in LT\, I$. Zřejmě tedy $LT\, r \in \langle LT\, I\rangle$. Připusťme, že $r \neq 0$. Protože $\langle LT\, I\rangle$ je monomiální, musí být $LT\, r$ dělitelný některým z jeho generátorů, tj. $LT\, g_1, \ldots, LT\, g_s$. To je ovšem spor s výsledkem algoritmu dělení. Proto $r = 0$ a I je tedy generovaný $g_1, \ldots, g_s$. □

Definition

Konečná báze $g_1, \ldots, g_s$ ideálu $I \subseteq k[x_1, \ldots, x_n]$ se nazývá *Gröbnerova*, jestliže platí $\langle LT\, I \rangle = \langle LT\, g_1, \ldots, LT\, g_s \rangle$.

Báze použitá v důkazu Hilbertovy věty byla Gröbnerova.

Corollary

Každý ideál $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ má Gröbnerovu bázi. Naopak každá množina polynomů $g_1, \ldots, g_s \in I$ splňující $\langle LT\, I \rangle = \langle LT\, g_1, \ldots, LT\, g_s \rangle$ je Gröbnerovou bází ideálu I.

Jednoduchý případ s uspořádáním $<_{\text{lex}}$:
Označme generátory $f_i = \sum_j a_{i,j}x_j + a_{i,0}$. Uvažujme matici $A = (a_{i,j})$, kde $i = 1, \ldots, s$ a $j = 0, \ldots, n$ a aplikujme na ni Gausovu eliminaci. Získáme $B = (b_{i,j})$ ve schodovitém tvaru, z ní navíc vypustíme nulové řádky. Máme novou bázi $g_1, \ldots, g_t$, kde $t \leq s$.
Vzhledem k provedeným úpravám je každé f_i vyjádřitelné jako lineární kombinace $g_1, \ldots, g_t$, a tedy

$$\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$$

získaná $g_1, \ldots, g_t$ je Gröbnerova báze:

Bez újmy na obecnosti předpokládejme, že proměnné jsou značeny tak, že $LM\, g_i = x_i$ pro $i = 1, \ldots, t$. Libovolný $f \in I$ lze psát

$$f = h_1 f_1 + \cdots + h_s f_s = h'_1 g_1 + \cdots + h'_t g_t$$

Chceme, aby $LT\, f \in \langle LT\, g_1, \ldots, LT\, g_t \rangle$, tj. $LT\, f$ má být dělitelný některým z $x_1, \ldots, x_t$. Předpokládejme, že f je pouze v proměnných $x_{t+1}, \ldots, x_n$. Pak ale $h'_1 = 0$, protože x_1 je vzhledem ke schodovitosti B pouze v g_1. Analogickým postupem získáme $h'_2 = \cdots = h'_t = 0$, a tedy $f = 0$.

Theorem

Nechť $G = \{g_1, \ldots, g_t\}$ *je Gröbnerova báze ideálu* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *a* f *je polynom v* $\mathbb{K}[x_1, \ldots, x_n]$. *Pak existuje právě jedno* $r = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ *s těmito vlastnostmi*

1. *Žádný člen* r *není dělitelný žádným z* $LT\, g_1, \ldots, LT\, g_t$, *tj.* $\forall \alpha \forall i \colon LT\, g_i \not| \, a_\alpha x^\alpha$.
2. $\exists g \in I \colon f = g + r$

Theorem

Nechť $G = \{g_1, \ldots, g_t\}$ je Gröbnerova báze ideálu $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ a f je polynom v $\mathbb{K}[x_1, \ldots, x_n]$. Pak existuje právě jedno $r = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ s těmito vlastnostmi

1. *Žádný člen r není dělitelný žádným z $LT\, g_1, \ldots, LT\, g_t$, tj. $\forall \alpha \forall i \colon LT\, g_i \not| \, a_\alpha x^\alpha$.*
2. *$\exists g \in I \colon f = g + r$*

Corollary

Nechť $G = \{g_1, \ldots, g_t\}$ je Gröbnerova báze ideálu $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ a f je polynom v $\mathbb{K}[x_1, \ldots, x_n]$. Pak platí

$$f \in I \iff \text{zbytek po dělení } f/G \text{ je nulový}$$

Definition

Pro $\alpha = \text{multideg}\, f$ a $\beta = \text{multideg}\, g$ uvažme

$$\gamma := (\gamma_1, \ldots, \gamma_n) \quad \text{kde } \gamma_i = \max\{\alpha_i, \beta_i\}$$

Monom x^γ nazýváme *nejmenším společným násobkem (least common multiple)* monomů $LM\, f$ a $LM\, g$ a zavádíme označení $LCM(LM\, f, LM\, g) := x^\gamma$. Výraz

$$S(f, g) := \frac{x^\gamma}{LT\, f} \cdot f - \frac{x^\gamma}{LT\, g} \cdot g$$

nazýváme S-polynomem (nebo také *syzygy*, neboli spřežení) polynomů f, g.

Definition

Pro $\alpha = \text{multideg}\, f$ a $\beta = \text{multideg}\, g$ uvažme

$$\gamma := (\gamma_1, \ldots, \gamma_n) \quad \text{kde } \gamma_i = \max\{\alpha_i, \beta_i\}$$

Monom x^γ nazýváme *nejmenším společným násobkem (least common multiple)* monomů $LM\, f$ a $LM\, g$ a zavádíme označení $LCM(LM\, f, LM\, g) := x^\gamma$. Výraz

$$S(f,g) := \frac{x^\gamma}{LT\, f} \cdot f - \frac{x^\gamma}{LT\, g} \cdot g$$

nazýváme S-polynomem (nebo také *syzygy*, neboli spřežení) polynomů f, g.

Jedná se o nástroj k eliminaci vedoucích členů, Gaussova eliminace je speciálním případem tohoto postupu pro stupeň 1. Narozdíl od ní ale může dojít ke zvýšení stupně, i když původní vedoucí členy odstraní.

Theorem

Nechť $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ je ideál. Pak jeho báze $G = \{g_j, \ldots, g_t\}$ je Gröbnerova právě tehdy, když pro každé $i \neq j$ je zbytek po dělení $S(g_i, g_j)/G$ nulový.

Důkaz.

Nebudeme na přednášce uvádět – hodně technické (ale napíšu časem do textů). □

Věta poskytuje účinný prostředek pro zjištění, zda nějaká báze je Gröbnerova. Uvažujme například $I = \langle x + y, y - z \rangle$. Jediný S-polynom, který připadá v úvahu je

$$S(x + y, y - z) = \frac{xy}{x}(x + y) - \frac{xy}{y}(y - z) = xz + y^2$$

Dělením získáme $xz + y^2 = z(x + y) + y(y - z)$, a tedy daná báze je Gröbnerova.

Naivní algoritmus pro Gröbnerovy báze

1. $G := F$, $G' := \emptyset$
2. `while` $G \neq G'$
   1. $G' := G$
   2. $\forall p, q \in G' : p \neq q$ `do`
      1. $s := \overline{S(p,q)}^{G'}$
      2. `if` $s \neq 0$
         $G := G \cup \{s\}$

Naivní algoritmus pro Gröbnerovy báze

1. $G := F$, $G' := \emptyset$
2. `while` $G \neq G'$
   1. $G' := G$
   2. $\forall p, q \in G' : p \neq q$ `do`
      1. $s := \overline{S(p,q)}^{G'}$
      2. `if` $s \neq 0$
         $G := G \cup \{s\}$

Tento algoritmus ovšem není zdaleka ideální. Lze vymyslet velmi jednoduše vypadající vstupy, pro něž vrací divoké výsledky. Dále výstupní báze se přímo odvíjí od vstupní, a tedy pro tentýž ideál zadaný různými bázemi dá také různé výsledky.

Lemma

Nechť G je Gröbnerova báze ideálu I a $p \in G$ takový, že $LT\, p \in \langle LT(G - \{p\})\rangle$. Pak $G - \{p\}$ je také Gröbnerova báze I.

Důkaz.

Z definice Gröbnerovy báze platí $\langle LT\, I\rangle = \langle LT\, G\rangle$. Protože $LT\, p \in \langle LT(G - \{p\})\rangle$, platí $\langle LT(G - \{p\})\rangle = \langle LT\, G\rangle$. Odsud již plyne tvrzení. □

Definition

Minimální Gröbnerovou bází ideálu I je taková Gröbnerova báze G, že pro všechna $p \in G$ platí $LC\, p = 1$ a zároveň $LT\, p \notin \langle LT(G - \{p\})\rangle$

Například mějme $k[x, y]$ a $<_{\text{grlex}}$,
$I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Zmíněný algoritmus dá

$$(f_1, \ldots, f_5) = (x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x)$$

Přitom platí $LT\, f_1 = x^3 = -x\, LT\, f_3$ a $LT\, f_2 = -\frac{1}{2}x\, LT\, f_4$ a tedy f_1 a f_2 jsou zbytečné.
Všimněme si: pro každé a je $\{x^2 + axy, xy, y^2 - 1/2x\}$ minimální Gröbnerovou bází uvedeného ideálu.

Definition

Polynom $g \in G$ nazveme *redukovaný* pro bázi G pokud žádný z jeho monomů neleží v $\langle LT(G - \{g\})\rangle$. *Redukovanou Gröbnerovou bází* ideálu I potom nazveme takovou Gröbnerovu bázi G, že pro všechna $p \in G$ platí $LC\, p = 1$ a zároveň p je redukovaný pro G.

Zjevně je každá redukovaná Gröbnerova báze je minimální a navíc platí:

Lemma

Je-li polynom g redukovaný pro nějakou minimální Gröbnerovu bázi G ideálu I, pak je také redukovaný pro každou minimální Gröbnerovu bázi G' téhož ideálu, která jej obsahuje.

Důkaz.

Tvrzení dokážeme sporem. Uvažme $G = \{g_1, \ldots, g_s\}$, $G' = \{g'_1, \ldots, g'_t\}$ a $g = \cdots + m + \cdots$ kde $m \in \langle LT(G' - \{g\})\rangle$ (tj. g není redukovaný pro G'). Potom $m = a_1\, LT\, g'_1 + \cdots + a_t\, LT\, g'_t$ pro nějaké vhodné polynomy $a_1, \ldots, a_t$. Protože G i G' jsou Gröbnerovy báze téhož ideálu, platí $\langle LT\, G\rangle = \langle LT\, G'\rangle$, a tedy každé $LT\, g'_i$ lze vyjádřit jako kombinaci $LT\, g_1, \ldots, LT\, g_s$. Odtud už plyne $m \in \langle LT\, G\rangle$ a protože je G' minimální, je $m \in \langle LT(G \setminus \{g\})\rangle$, což je spor s předpokládanou redukovaností g pro G. □

Theorem

Nechť $I \subseteq k[x_1, \ldots, x_n]$ je nenulový. Pak pro každé monomiální uspořádání existuje právě jedna redukovaná Gröbnerova báze ideálu I. Navíc každou Gröbnerovu bázi lze algoritmicky redukovat.

Budeme považovat okruh $\mathbb{K}[x_{p+1}, \ldots, x_n]$ za podokruh $\mathbb{K}[x_1, \ldots, x_n]$. Jedná se o polynomy, v nichž se nevyskytují proměnné $x_1, \ldots, x_p$. Je to skutečně podokruh, ale už ne ideál.

Definition

Nechť $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$. Pro $p = 1, \ldots, n$ definujeme

$$I_p := I \cap \mathbb{K}[x_{p+1}, \ldots, x_n]$$

Tuto množinu nazveme *p-tým eliminačním ideálem.*

Budeme považovat okruh $\mathbb{K}[x_{p+1}, \ldots, x_n]$ za podokruh $\mathbb{K}[x_1, \ldots, x_n]$. Jedná se o polynomy, v nichž se nevyskytují proměnné $x_1, \ldots, x_p$. Je to skutečně podokruh, ale už ne ideál.

Definition

Nechť $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$. Pro $p = 1, \ldots, n$ definujeme

$$I_p := I \cap \mathbb{K}[x_{p+1}, \ldots, x_n]$$

Tuto množinu nazveme *p-tým eliminačním ideálem.*

Samozřejmě I_p je ideálem pouze v $k[x_{p+1}, \ldots, x_n]$.

Na úrovni polynomiálních rovnic I_p obsahuje všechny rovnice, které jsou důsledky systému $f_1 = 0, \ldots, f_s = 0$ a v kterých vystupují pouze proměnné $x_{p+1}, \ldots, x_n$.

Na úrovni polynomiálních rovnic I_p obsahuje všechny rovnice, které jsou důsledky systému $f_1 = 0, \ldots, f_s = 0$ a v kterých vystupují pouze proměnné $x_{p+1}, \ldots, x_n$.

Theorem (Eliminační věta)

Nechť $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ je ideál, $G = \{g_1, \ldots, g_m\}$ jeho Gröbnerova báze vzhledem k $<_{lex}$. Proměnné nechť jsou uspořádány $x_1 >_{lex} x_2 >_{lex} \cdots$. Potom pro každé $p = 0, \ldots, n$ je $G_p := G \cap \mathbb{K}[x_{p+1}, \ldots, x_n]$ Gröbnerovou bází ideálu I_p.

Plán přednášky

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 $\cap$.

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:

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

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

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

existuje 0 tak, že $A \vee 0 = A$ (4)

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

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

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

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

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

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

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.

Definition

Množině K spolu s dvěmi 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 **doplněk** k prvku A.

Definition

Množině K spolu s dvěmi 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 **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 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* 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 $A, B, \cdots \in K$ 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.

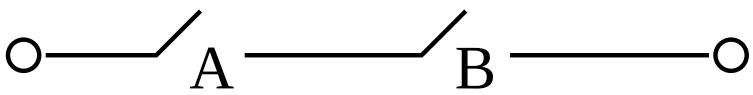
Naši symboliku interpretujeme tak, že z prvků $A, B, \cdots \in K$ tvoříme „slova“ pomocí operací $\vee$, $\wedge$, $'$ a závorek vyjasňujících v jakém pořadí a na jaké argumenty jsou operace aplikovány.
Samotné axiomy a jejich důsledky pak říkají, že velice často různá slova dávají stejnou hodnotu výsledku v K.
V případě množiny všech podmnožin $K = 2^M$ je to zřejmé – prostě jde o rovnost podmnožin.

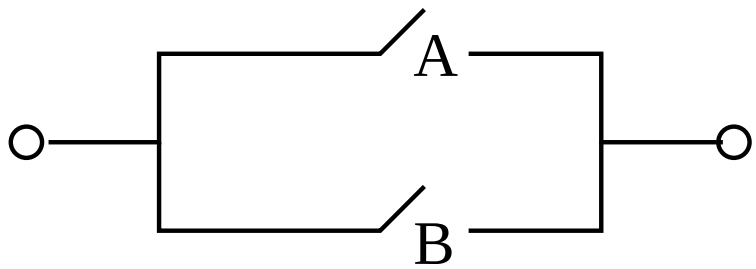
Nyní budeme pracovat opět se slovy jako výše, interpretujeme je ale jako tvrzení složené z elementárních výroků $A, B, \ldots$ a logických operací AND (binární operace $\wedge$), OR (binární operace $\vee$) a negace NOT (unární operace $'$). Taková slova nazýváme **výroky** a přiřazujeme jim pravdivostní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

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 $(A \wedge B) \vee (A' \wedge B')$. 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.

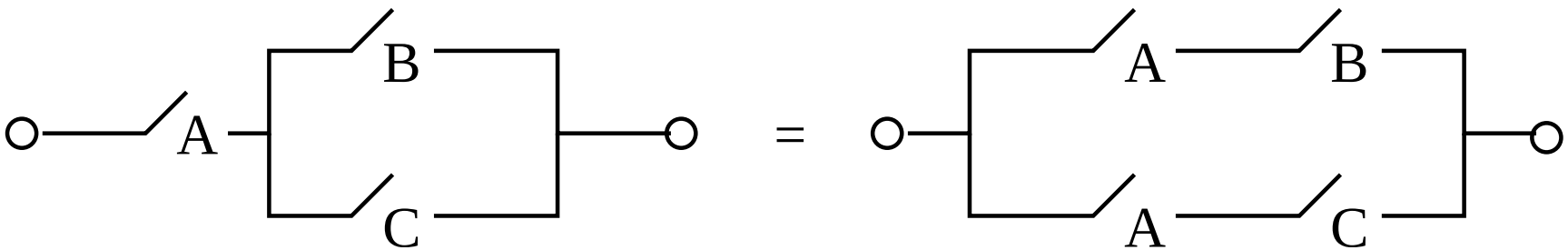
Přepínač je pro nás černá skříňka, která má jen dva stavy, buď je zapnut (a signál prochází) nebo naopak vypnut (a signál neprochází).
Jeden nebo více přepínačů zapojujeme do sítě sériově nebo paralelně. Sériové zapojení je popsáno pomocí binární operace $\wedge$, paralelní je naopak $\vee$. Unární operace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





Každé konečné slovo vytvořené pomocí přepínačů $A, B, \ldots$ 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.

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.



Dalším přirozeným příkladem Booleovské algebry je systém dělitelů přirozeného čísla nebo polynomu.
Zvolme pevně takové číslo $p \in \mathbb{N}$ nebo polynom $p \in \mathbb{K}[x_1, \ldots, x_s]$ 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. $1 \in \mathbb{K} \subset \mathbb{K}[x_1, \ldots, x_s]$. 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).

Plán přednášky

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“).

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).

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.

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.

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.

Plán přednášky

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 $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ lze zadat pomocí základních logických operací.

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 $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ 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).

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 $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ 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 $\vee$.

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 $A_1, \ldots, A_n$ 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 $A_i^{\sigma_i} = A_i'$.

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 $Y, X_1, \ldots, X_\ell$ 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 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 $f : K \to L$ 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)!

Theorem

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

Definition

Homomorfismem posetů $(K, \leq_K)$ a $(L, \leq_L)$ rozumíme takové zobrazení $f : K \to L$, že z $A \leq_K B$ vždy vyplývá také $f(A) \leq_L f(B)$. Hovoříme přitom také o **izotonních zobrazeních**.

Snadno se ověří, že bijektivnost f již zaručí, že f^{-1} je opět homomorfismem.

Z definice uspořádání na Booleových algebrách nebo svazech 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, půjde tedy vždy o izotonní zobrazení.

Mnoho praktických úloh spočívá v diskusi pevných bodů zobrazení $f : K \to K$ na nějaké množině K, tj. prvků $x \in K$ s vlastností $f(x) = x$. Naše úvahy o infimech a supremech umožňují překvapivě snadno odvodit velice silná tvrzení tohoto typu. Dokážeme si jednu takovou klasickou větu, kterou odvodili Knaster a Tarski (ve speciálním případě Booleovské algebry podmnožin dané množiny již koncem dvacátých let 20. století, obecné tvrzení pak publikoval Tarski v r. 1955):

Theorem (Tarského věta)

Uvažujme libovolný úplný svaz $(K, \wedge, \vee)$ a libovolné isotonní zobrazení $f : K \to K$. Pak f má pevný bod a množina všech pevných bodů f je (s uspořádáním zděděným z K) opět úplný svaz.

V literatuře lze najít mnoho variant vět o pevných bodech v různých souvislostech. Jednou z velmi užitečných je tzv. **Kleeneho věta**, jejíž tvrzení můžeme vyčíst z právě dokázané věty následujícím způsobem.
Jestliže (ve značení Tarského věty) uvážíme spočetnou podmnožinu v K tvořenou tzv. **Kleeneho řetězcem**

$$0 \leq f(0) \leq f(f(0)) \leq \ldots,$$

pak supremum z této podmnožiny zjevně nemůže být větší, než kterýkoliv pevný bod zobrazení f. Skutečně, pokud je y pevný bod zobrazení f pak ze vztahu $0 \leq y$ dostaneme $f(0) \leq f(y) = y$ atd. Pokud má f navíc vlastnost, že „dostatečně“ zachovává suprema, můžeme dovodit že $f(z)$ bude opět supremem téhož řetězce a tedy pevný bod. Musí to proto být nejmenší pevný bod. Toto tvrzení se nazývá **Kleeneho věta o pevném bodě** a má četná použití v teorii rekurzí, při diskusi zastavení algoritmů atd.