Matematická logika

přednáška třetí

Miroslav Kolařík

Zpracováno dle textu R. Bělohlávka:
Matematická logika – poznámky k přednáškám, 2004.

a dle učebního textu R. Bělohlávka a V. Vychodila:
Diskrétní matematika pro informatiky I a II, Olomouc 2006.

Obsah

Obsah

Booleovská funkce s n argumenty (**n-ární booleovská funkce**) je libovolné zobrazení, které každé uspořádané n-tici hodnot 0 nebo 1 přiřadí hodnotu 0 nebo 1. Každou booleovskou funkci f s n argumenty lze zapsat v tabulce podobně jako u tabulkové metody. Předpokládejme, že argumenty funkce f označíme $x_1, \ldots, x_n$, pak píšeme také $f(x_1, \ldots, x_n)$.

Příklad

Všechny booleovské funkce jedné proměnné:

x_1	f_1	f_2	f_3	f_4
0	0	0	1	1
1	0	1	0	1

Vidíme, že f_3 je pravdivostní funkce spojky negace, tj. $f_3(0) = 1$ a $f_3(1) = 0$.

Příklad

Všechny booleovské funkce dvou proměnných:

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
1	1	1	1	1	1	1	1	1	1
1	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0
0	0	1	0	1	0	1	0	1	0

x_1	x_2	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	0	0	0	0	0	0	0	0
1	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0
0	0	1	0	1	0	1	0	1	0

Vidíme, že f_2 je pravdivostní funkce spojky disjunkce, f_5 je pravdivostní funkce spojky implikace, f_7 je pravdivostní funkce spojky ekvivalence a f_8 je pravdivostní funkce spojky konjunkce.

Pravdivostní funkce spojek $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ jsou booleovské funkce dvou argumentů, pravdivostní funkce spojky $\neg$ je booleovská funkce jednoho argumentu.

Tvrzení: Existuje $2^{(2^n)}$ booleovských funkcí s n argumenty.

Je jasné, že každá formule φ obsahující výrokové symboly $p_1, \ldots, p_n$ indukuje booleovskou funkci n argumentů. Je to právě funkce, jejíž tabulku získáme vytvořením tabulky pro formuli φ. Zajímavé ale je, že platí také opačné tvrzení: Ke každé booleovské funkci f s n argumenty existuje formule φ_f taková, že tato formule indukuje právě funkci f. Platí dokonce, že formule φ_f může obsahovat pouze spojky $\neg$, $\wedge$, $\vee$.

Definice

Nechť V je množina výrokových symbolů. Pak

- **literál** nad V je libovolný výrokový symbol z V nebo jeho negace
- **úplná elementární konjunkce** nad V je libovolná konjunkce literálů, ve které se každý výrokový symbol z V vyskytuje právě v jednom literálu
- **úplná elementární disjunkce** nad V je libovolná disjunkce literálů, ve které se každý výrokový symbol z V vyskytuje právě v jednom literálu
- **úplná konjunktivní normální forma** nad V je konjukce úplných elementárních disjunkcí nad V
- **úplná disjunktivní normální forma** nad V je disjunkce úplných elementárních konjunkcí nad V.

Poznámka: Tabulkovou metodou se lze snadno přesvědčit, že formule $p \wedge (q \wedge r)$ a $(p \wedge q) \wedge r$ jsou sémanticky ekvivalentní, tedy u formulí ve tvaru konjunkce nezáleží na uzávorkování. To samé platí pokud bychom nahradili konjunkci disjunkcí. Píšeme tedy stručně $p_1 \wedge \dots \wedge p_n$ místo $p_1 \wedge (p_2 \wedge (\dots (p_{n-1} \wedge p_n) \dots))$, atp. Analogicky pro disjunkci.

Věta

Ke každé formuli VL, která není tautologií (kontradikcí) existuje s ní sémanticky ekvivalentní formule, která je ve tvaru úplné konjunktivní normální formy (úplné disjunktivní normální formy).

Konstrukce ÚDNF pro formuli φ s výr. symboly $p_1, \ldots, p_n$:

1) pro $\varphi(p_1, \ldots, p_n)$ uvažme tabulku pravdivostních hodnot
2) pro řádky s hodnotou 1 (ve sloupci φ) sestrojme ÚEK z p_i (pro 1) a $\neg p_i$ (pro 0)
3) výsledná ÚDNF je disjunkcí takových ÚEK.

Pro ÚKNF postupujeme duálně:

Konstrukce ÚKNF pro formuli φ s výr. symboly $p_1, \ldots, p_n$:

1) pro $\varphi(p_1, \ldots, p_n)$ uvažme tabulku pravdivostních hodnot
2) pro řádky s hodnotou 0 (ve sloupci φ) sestrojme ÚED z p_i (pro 0) a $\neg p_i$ (pro 1)
3) výsledná ÚKNF je konjunkcí takových ÚED.

Příklady: Viz přednáška a cvičení.

Příklad

Sestrojte ÚDNF a ÚKNF k formuli φ: $(p \Leftrightarrow q) \wedge (q \Rightarrow r)$

p	q	r	$p \Leftrightarrow q$	$q \Rightarrow r$	φ	ÚEK	ÚED
1	1	1	1	1	1	$p \wedge q \wedge r$	
1	1	0	1	0	0		$\neg p \vee \neg q \vee r$
1	0	1	0	1	0		$\neg p \vee q \vee \neg r$
1	0	0	0	1	0		$\neg p \vee q \vee r$
0	1	1	0	1	0		$p \vee \neg q \vee \neg r$
0	1	0	0	0	0		$p \vee \neg q \vee r$
0	0	1	1	1	1	$\neg p \wedge \neg q \wedge r$	
0	0	0	1	1	1	$\neg p \wedge \neg q \wedge \neg r$	

Tedy ÚDNF je $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$,
ÚKNF je $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r)$.

Obsah

Množina booleovských funkcí $\{f_1, \ldots, f_k\}$ je **funkčně úplná**, pokud každou booleovskou funkci $f : \{0,1\}^n \rightarrow \{0,1\}$ lze vyjádřit jako složení některých funkcí z $\{f_1, \ldots, f_k\}$.

Řekneme, že množina výrokových spojek je **úplná** (tvoří **úplný systém spojek**), jestliže je funkčně úplná množina jim odpovídajících booleovských funkcí.

Každý úplný minimální systém spojek VL nazveme **bází**.

Tvrzení

$\{\neg, \curlyvee, \curlywedge\}$ tvoří úplný systém spojek VL.

Důkaz: Platnost plyne z tvrzení o ÚDNF (ÚKNF).

Z de Morganových zákonů je zřejmé, že systém $\{\neg, \curlyvee, \curlywedge\}$ není bází. Jednoduše se dá ukázat, že existují dvouprvkové báze $\{\neg, \curlyvee\}$, $\{\neg, \curlywedge\}$, $\{\neg, \rightarrow\}$.

Otázka: Existují jednoprvkové báze VL?

Speciální význam mají **Piercova** (**Nicodova**) **spojka** (význam: "ani ..., ani ..."; označujeme ji symbolem $\Downarrow$) a **Shefferova spojka** (význam: "pokud ..., pak neplatí ..."; označujeme ji symbolem $\Uparrow$), které samy o sobě tvoří úplný systém spojek. Obě spojky jsou interpretovány následujícími pravdivostními funkcemi:

$\downarrow$	0	1
0	1	0
1	0	0

$\uparrow$	0	1
0	1	1
1	1	0

Tvrzení: Existují pouze dvě jednoprvkové báze; tvoří je spojky Sheffer $\{\uparrow\}$ a Nicod $\{\downarrow\}$ (též tzv. Piercova spojka). (Tedy pomocí Sheffera (resp. Nicoda) lze nahradit všechny ostatní spojky VL.)

K důkazu: Pomocí $\Uparrow$ (resp. $\Downarrow$) lze vyjádřit $\neg, \wedge, \vee$:
Zřejmě

$$(a \Uparrow b) \Leftrightarrow \neg(a \wedge b).$$

Odtud:

1) $\neg a \Leftrightarrow \neg(a \wedge a) \Leftrightarrow (a \Uparrow a)$;
2) $(a \wedge b) \Leftrightarrow \neg\neg(a \wedge b) \Leftrightarrow \neg(a \Uparrow b) \Leftrightarrow ((a \Uparrow b) \Uparrow (a \Uparrow b))$;
3) $(a \vee b) \Leftrightarrow \neg\neg(a \vee b) \Leftrightarrow \neg(\neg a \wedge \neg b) \Leftrightarrow (\neg a \Uparrow \neg b) \Leftrightarrow ((a \Uparrow a) \Uparrow (b \Uparrow b))$.

Podobně pro $\Downarrow$.

Obsah

Motivace: Tabelace je neúnosná při velkém množství výrokových symbolů. Nabízí se tedy otázka, zda-li není možné o sémantickém vyplývání rozhodnout jinak než tabelací ...

Odvozovací pravidlo modus ponens

Nejprve si zavedeme nový pojem vyplývání, který nebude založen na pojmu pravdivostní ohodnocení, ale pouze na manipulaci s formulemi na úrovni jejich tvaru. Základní pojem, na kterém je tento typ vyplývání založen je **odvozovací pravidlo** – předpis pomocí nějž ze vstupních formulí odvozujeme další formule. Odvozovací pravidla formalizují elementární úsudky. Nám bude ve VL postačovat pouze jediné odvozovací pravidlo, tzv. **pravidlo odloučení** neboli **modus ponens** (MP), které lze schématicky vyjádřit

$$\text{MP:} \qquad \frac{\varphi, \varphi \Rightarrow \psi}{\psi}$$

a jehož význam je: "z formulí φ a $\varphi \Rightarrow \psi$ odvodíme formuli ψ". Formulím $\varphi, \varphi \Rightarrow \psi$ někdy říkáme **předpoklady**.

Například formule $\neg q$ vzniká použitím modus ponens z formulí $p \Rightarrow r$ a $(p \Rightarrow r) \Rightarrow \neg q$.

Axiomy VL

Při odvozování formulí budeme dále používat **axiomy**, což jsou formule, které automaticky přijímáme jako "platné". Axiomy popisují vlastnosti logických spojek a jejich vzájemný vztah. Axiomy VL si definujeme pomocí tří **axiomových schémat**:

(A1) $\varphi \Rightarrow (\psi \Rightarrow \varphi)$,

(A2) $(\varphi \Rightarrow (\psi \Rightarrow \chi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \chi))$,

(A3) $(\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$.

Jakákoli formule, která je ve tvaru jednoho ze schémat (A1) – (A3) se nazývá **axiom** VL.

Axiomová schémata jsou "předpisy", kterými definujeme všechny axiomy. Ačkoli budeme používat pouze tři axiomová schémata, axiomů jako takových je nekonečně mnoho. Např. formule $(\neg(p \Rightarrow q) \Rightarrow \neg\neg p) \Rightarrow (\neg p \Rightarrow (p \Rightarrow q))$ je axiom, který je instancí schéma (A3). Dále např. $p \Rightarrow (q \Rightarrow r)$ není axiom.

Množinu axiomů a odvozovacích pravidel, která používáme, souhrnně nazýváme **axiomatický systém**.

Důkaz

Pod pojmem "důkaz" je intuitivně myšlen záznam odvozování, provedený tak, že za sebe napíšeme tvrzení, ke kterým se postupně dobíráme tak, že začneme předpoklady a pokračujeme tvrzeními, která z předchozích tvrzení plynou pomocí elementárních úsudkových kroků.

Nyní zavedeme přesný pojem důkazu v našem axiomatickém systému – neformální pojem důkazu tak převedeme z úrovně intuice na přesnou formální úroveň.

Důkaz, syntaktické vyplývání

Definice

Důkaz formule φ z množiny formulí T je lib. posloupnost formulí $\varphi_1, \ldots, \varphi_n$ taková, že $\varphi_n = \varphi$ a každá φ_i ($i = 1, \ldots, n$)

- je axiomem,
- nebo náleží do T,
- nebo vzniká z předchozích formulí důkazu pomocí odvozovacího pravidla MP, tedy existují indexy $j, k < i$ tak, že φ_k je formule ve tvaru $\varphi_j \Rightarrow \varphi_i$.

Formule φ je dokazatelná z T (zapisujeme $T \vdash \varphi$), pokud existuje důkaz formule φ z T. Pokud $\vdash \varphi$, pak říkáme, že φ je dokazatelná (z prázdného systému předpokladů).

Dokazatelnosti budeme také říkat **syntaktické vyplývání**, abychom tím zdůraznili, že jde o protějšek sémantického vyplývání. Fakt $T \vdash \varphi$ lze tedy číst "φ syntakticky plyne z T", případně "φ je syntaktickým důsledkem T".

Zřejmě každý axiom je dokazatelný, neboť $\vdash \varphi$ platí pro každý axiom φ, protože jednoprvková posloupnost φ je důkazem φ z prázdného systému předpokladů.

Poznámka: Máme dva pojmy vyplývání formule z množiny formulí: sémantické vyplývání ($T \models \varphi$) a syntaktické vyplývání ($T \vdash \varphi$). Jak spolu souvisí uvidíme později (věta o úplnosti). Speciálně máme dva pojmy platnosti formule: $\models \varphi$ označuje platnost φ v sémantickém smyslu (pravdivost), $\vdash \varphi$ označuje platnost φ v syntaktickém smyslu (dokazatelnost).

Tvrzení

Pro každou množinu formulí T a formule φ, ψ platí, že z $T \vdash \varphi \Rightarrow \psi$ a $T \vdash \varphi$ plyne $T \vdash \psi$.

Důkaz: Máme tedy dokázat, že jsou-li z T dokazatelné formule $\varphi \Rightarrow \psi$ a φ, pak je z T dokazatelná i formule ψ. Jsou-li však z T dokazatelné formule $\varphi \Rightarrow \psi$ a φ, znamená to, že existuje důkaz $\chi_1, \ldots, \chi_n$ formule $\varphi \Rightarrow \psi$ z T (tj. χ_n je formulí $\varphi \Rightarrow \psi$) a že existuje důkaz $\theta_1, \ldots, \theta_m$ formule φ z T (tj. θ_m je formulí φ). Nyní však stačí vzít posloupnost $\chi_1, \ldots, \chi_n, \theta_1, \ldots, \theta_m, \psi$ – ta je již důkazem ψ z T. Abychom se o tom přesvědčili, stačí ověřit podmínky z definice pojmu důkaz (pro každou formuli uvažované posloupnosti). Zřejmě každá formule χ_i je buď axiomem nebo je formulí z T nebo plyne z nějakých předchozích χ_k, χ_l pomocí MP. Podobně uvažujeme pro libovolnou formuli θ_j. Dále, formule ψ plyne z formulí χ_n (což je $\varphi \Rightarrow \psi$) a θ_m (což je φ) pomocí MP. Vidíme tedy, že posloupnost $\chi_1, \ldots, \chi_n, \theta_1, \ldots, \theta_m, \psi$ je důkazem ψ z T, tj. $T \vdash \psi$.

Věta

Pro každou formuli φ platí $\vdash \varphi \Rightarrow \varphi$ (tj. formule $\varphi \Rightarrow \varphi$ je dokazatelná v našem axiomatickém systému).

Důkaz: Máme ukázat, že existuje důkaz (z prázdné množiny předpokladů), jehož posledním prvkem je $\varphi \Rightarrow \varphi$. Důkazem formule $\varphi \Rightarrow \varphi$ je například posloupnost formulí

1. $\varphi \Rightarrow ((\varphi \Rightarrow \varphi) \Rightarrow \varphi)$
2. $(\varphi \Rightarrow ((\varphi \Rightarrow \varphi) \Rightarrow \varphi)) \Rightarrow ((\varphi \Rightarrow (\varphi \Rightarrow \varphi)) \Rightarrow (\varphi \Rightarrow \varphi))$
3. $(\varphi \Rightarrow (\varphi \Rightarrow \varphi)) \Rightarrow (\varphi \Rightarrow \varphi)$
4. $\varphi \Rightarrow (\varphi \Rightarrow \varphi)$
5. $\varphi \Rightarrow \varphi$

Fakt, že $\vdash \varphi \Rightarrow \varphi$ budeme dále používat.

Lemma – monotonie dokazatelnosti

Nechť T a S jsou množiny formulí a φ, ψ jsou formule. Pak platí: pokud $T \vdash \varphi$ a pro každou $\psi \in T$ máme $S \vdash \psi$, pak $S \vdash \varphi$.

Důkaz: Předpokládejme, že platí $T \vdash \varphi$. To jest existuje důkaz $\chi_1, \dots, \chi_n$ z T, kde $\chi_n = \varphi$. Uvažujme posloupnost $\vartheta_1, \dots \vartheta_m$, kterou vytvoříme z posloupnosti $\chi_1, \dots, \chi_n$ tak, že každý člen χ_i, pro který máme $\chi_i \in T$, nahradíme některým jeho důkazem ze systému S (důkaz vždy existuje, jelikož $S \vdash \chi_i$), jinými slovy, formuli χ_i "vyjmeme" z posloupnosti $\chi_1, \dots, \chi_n$ a na její místo "vložíme důkaz" formule χ_i z S, což je opět konečná posloupnost formulí. Vzniklá posloupnost $\vartheta_1, \dots \vartheta_m$ je evidentně důkazem z S a ϑ_m je formule φ. Dostáváme tedy $S \vdash \varphi$.

Věta o dedukci (VoD)

Pro každou množinu formulí T a formule φ, ψ platí: $T \vdash \varphi \Rightarrow \psi$, právě když $T, \varphi \vdash \psi$.

Důkaz:
"$\Rightarrow$" Předpokládáme-li $T \vdash \varphi \Rightarrow \psi$, je tím spíše $T, \varphi \vdash \varphi \Rightarrow \psi$. Použitím MP okamžitě dostáváme $T, \varphi \vdash \psi$.
"$\Leftarrow$" Nechť $T, \varphi \vdash \psi$, tj. existuje důkaz $\psi_1, \ldots, \psi_n$ formule ψ z T, φ (ψ_n je ψ). Indukcí dokážeme, že $T \vdash \varphi \Rightarrow \psi_i$ platí pro $i = 1, \ldots, n$, z čehož dostaneme požadovaný vztah jako speciální případ pro $i = n$. Vezměmě tedy $i \in \{1, \ldots, n\}$ a předpokládejme, že pro každé $j < i$ platí $T \vdash \varphi \Rightarrow \psi_j$ (indukční předpoklad). Dokážeme, že $T \vdash \varphi \Rightarrow \psi_i$. Podle definice důkazu mohou nastat pouze následující tři případy:

(A) ψ_i je axiom nebo formule z T. Pak je posloupnost formulí
$\psi_i \Rightarrow (\varphi \Rightarrow \psi_i)$,
ψ_i,
$\varphi \Rightarrow \psi_i$
důkazem formule $\varphi \Rightarrow \psi_i$ z T.

(B) ψ_i je formulí φ. Pak $T \vdash \varphi \Rightarrow \psi_i$ plyne z předchozí Věty.

(C) ψ_i plyne z předchozích formulí $\psi_j, \psi_k = \psi_j \Rightarrow \psi_i$ ($j, k < i$) pomocí MP. Dle indukčního předpokladu existuje důkaz $\alpha, \ldots, \varphi \Rightarrow \psi_j$ z T a důkaz $\beta, \ldots, \varphi \Rightarrow (\psi_j \Rightarrow \psi_i)$ z T.
Přidáme-li k posloupnosti
$\alpha, \ldots, \varphi \Rightarrow \psi_j, \beta, \ldots, \varphi \Rightarrow (\psi_j \Rightarrow \psi_i)$ formule
$(\varphi \Rightarrow (\psi_j \Rightarrow \psi_i)) \Rightarrow ((\varphi \Rightarrow \psi_j) \Rightarrow (\varphi \Rightarrow \psi_i))$,
$(\varphi \Rightarrow \psi_j) \Rightarrow (\varphi \Rightarrow \psi_i)$,
$\varphi \Rightarrow \psi_i$,
dostaneme důkaz formule $\varphi \Rightarrow \psi_i$ z T.

Důkaz je hotov.

Věta o dedukci umožňuje mimo jiné zkracovat důkazy.

Příklad

Ukažme, že jestliže $T \vdash \varphi \Rightarrow \psi$ a $T \vdash \psi \Rightarrow \chi$, pak $T \vdash \varphi \Rightarrow \chi$ (tzv. **princip tranzitivity implikace**). Skutečně, máme $T, \varphi \vdash \psi$ (dle VoD aplikované na $T \vdash \varphi \Rightarrow \psi$), dále $T, \varphi \vdash \chi$ (použitím MP a monotonie dokazatelnosti) a konečně $T \vdash \varphi \Rightarrow \chi$ (VoD použitá na $T, \varphi \vdash \chi$).

Věta

Pro formule φ, ψ platí

($a_\vdash$) $\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \psi)$,

($b_\vdash$) $\vdash \neg\neg\varphi \Rightarrow \varphi$,

($c_\vdash$) $\vdash \varphi \Rightarrow \neg\neg\varphi$,

($d_\vdash$) $\vdash (\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$,

($e_\vdash$) $\vdash \varphi \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$.

Důkaz: ($a_\vdash$), ($b_\vdash$), ($c_\vdash$) viz cvičení, ($d_\vdash$), ($e_\vdash$) viz přednáška.

Poznámka: Vztahy ($a_\vdash$) – ($e_\vdash$) mají dobrý intuitivní význam. Vztah ($a_\vdash$) vyjadřuje, že pokud je φ neplatná, pak z vlastnosti φ plyne lib. formule. Vztahy ($b_\vdash$) a ($c_\vdash$) popisují vlastnosti dvojí negace – popisují právě to, co na sémantické úrovni vyjadřuje fakt, že φ a $\neg\neg\varphi$ jsou sémanticky ekvivalentní. Vztah ($d_\vdash$) je duálním vztahem k axiomovému schématu (A3) a spolu s (A3) popisuje to, co na sémantické úrovni vyjadřuje fakt, že $\varphi \Rightarrow \psi$ a $\neg\psi \Rightarrow \neg\varphi$ jsou sémanticky ekvivalentní. Vztah ($e_\vdash$) je modifikací vztahu: "z platnosti φ a z platnosti ψ plyne platnost $\varphi \wedge \psi$".