Výroková a predikátová logika

Petr Štěpánek

Logika prvního řádu

- je nejpoužívanější a nejlépe prozkoumaná
- v různé míře je součástí řady dalších logik
- je výhodné začít výkladem této logiky

Otázky

Je to pravda ?

sémantika

Dá se to dokázat ?

axiomy, odvozovací pravidla
(formální systém)

Vyjadřovací prostředek

Jazyk prvního řádu

Jazyk obsahuje

(i) Proměnné $x, y, z, x_1, x_2, \ldots, y', y'', \ldots$ neomezeně mnoho.

(ii) Funkční symboly $f, g, h, \ldots, f_1, f_2, \ldots$ každý má svou četnost (počet argumentů) $n \geq 0$.

(iii)Predikátové symboly $p, q, r, \ldots, p_1, p_2, \ldots$ každý má svou četnost $n > 0$.

(iv) Symboly pro logické spojky $\neg$ negace , $\vee$ disjunkce, & konjunkce, -> implikace, <-> ekvivalence .

(v) Symboly pro kvantifikátory $\forall$ univerzální $\exists$ existenční.

Postup výkladu

Nebudeme pracovat se všemi logickými symboly najednou.

- Nejprve logické spojky, těmi se zabývá *Výroková logika.*
- Potom kvantifikátory, to je *predikátová logika (bez rovnosti).*
- Nakonec přidáme predikát rovnosti tak vznikne *predikátová logika s rovností.*

Výroková logika

Motivace.

Jak už jejich název napovídá, logické spojky spojují různá tvrzení. V symbolickém jazyce jim říkáme formule.

Tím tvoří složitější tvrzení, také formule, která odpovídají souvětím v přirozeném jazyce.

Jazyk výrokové logiky je velmi jednoduchý, nemůžeme očekávat, že jím bude možné vyjádřit všechna tvrzení.

Proto musíme počítat s tím, že formule, které logické spojky spojují, budou obsahovat složitější tvrzení, tedy formule které nelze vyjádřit jen spojkami.

Ve formulích výrokové logiky takovým tvrzením vyhradíme místa, sloty, do kterých je bude možné vkládat.

Protože formule vložené do slotů nebudeme ve výrokové logice rozebírat, postačí nám jednotlivé sloty nějak označit.

K tomu použijeme nové symboly, které budeme nazývat *výrokové proměnné.*

Můžeme předpokládat, že výrokovým proměnným se jako hodnoty přiřazují nějaké formule predikátové logiky, včetně těch, které v kontextu výrokové logiky nelze rozebírat.

Jazyk prvního řádu pro potřeby výrokové logiky můžeme zjednodušit. Vyjdeme z neprázdné množiny P, která může být konečná i nekonečná. Její prvky nazýváme *prvotní formule* nebo *výrokové proměnné.*

Jazyk výrokové logiky obsahuje

(i) výrokové proměnné, tedy prvky množiny P.

(ii) logické spojky $\neg$, $\vee$, & , –> , <–>

(iii) pomocné symboly (závorky) (,) , [,] , { , } ...

Formule

Je-li dán jazyk výrokové logiky pak následující výrazy jsou formule.

(i) každá výroková proměnná $p \in P$ je formule.

(ii) jsou-li výrazy A, B formule, pak výrazy

$$\neg A\ ,\ \ (A \vee B)\ ,\ (A\ \&\ B)\ ,\ (A \text{ –> } B)\ ,\ (A \text{ <–> } B)$$

jsou také formule.

(iii) každá formule vznikne konečným užitím pravidel (i) a (ii).

Příklad (formule)

Je-li $P = \{ p, q, r, s \}$ množina výrokových proměnných, pak

p, q, r, s	jsou formule podle (i)
$(p \vee q)$ $(p \,\&\, q)$	jsou formule podle (ii)
$((p \vee q) \rightarrow (p \,\&\, q))$	je formule podle (ii)

Snadno se nahlédne, že výrazy

$$ppr \qquad (\rightarrow p) \qquad (\rightarrow \rightarrow$$

nejsou formule.

Co je možné dosadit za výrokové proměnné (příklady)

Reálná čísla

$p_1 \equiv a^2 \geq 0$

$p_2 = a \in \mathsf{R}$ {a je reálné číslo}

$p_3 = a^2 < 0$

$p_4 = (\forall x)(\exists y)(x + y = 0)$

Formule

p_1 $p_2 \rightarrow p_1$

$(\neg p_3 \ \& \ p_4)$

Vložením uvedených formulí na místa výrokových proměnných získáme formule jazyka predikátové logiky. O těch budeme podrobněji mluvit později.

V uvedených příkladech jde o formule, které nelze jen pomocí spojek rozebírat. Pro potřeby výkladu výrokové logiky postačí používat namísto nich výrokové proměnné.

Je to kratší a logické spojky, které používáme více vynikou.

Nejprve se budeme zabývat sémantikou výrokové logiky.

Ta dává odpověď na první otázku

Je to pravda ?

Přesněji, je tato formule pravdivá ?

Sémantika výrokové logiky

Formule výrokové logiky jsou konstruovány nad množinou P výrokových proměnných (prvotních formulí), které ve výrokové logice neanalyzujeme. Jejich pravdivost tedy musí být dána z vnějšku.

Množina pravdivostních hodnot $\{1,0\}$ $\{true, false\}$

(i) *Pravdivostní ohodnocení* (valuace) výrokových proměnných z P je zobrazení, které každé výrokové proměnné z P přiřadí pravdivostní hodnotu 1 nebo 0.

Je-li dáno pravdivostní ohodnocení v výrokových proměnných, pak lze každé výrokové formuli A jednoznačně přiřadit pravdivostní hodnotu $\underline{v}(A)$ následujícím způsobem

$\underline{v}(A) = v(p)$ *je-li* A výroková proměnná p

$\underline{v}(\neg A) = 0$ *je-li* $\underline{v}(A) = 1$

$= 1$ *je-li* $\underline{v}(A) = 0$

$\underline{v}(A \,\&\, B) = 1$ *je-li* $\underline{v}(A) = \underline{v}(B) = 1$

$= 0$ *jinak*

$\underline{v}(A \vee B) = 0$ *je-li* $\underline{v}(A) = \underline{v}(B) = 0$

$= 1$ *jinak*

$\underline{v}(A \rightarrow B) = 0$ *je-li* $\underline{v}(A) = 1$ *a* $\underline{v}(B) = 0$

$= 1$ *jinak*

$\underline{v}(A \leftrightarrow B) = 1$ *je-li* $\underline{v}(A) = \underline{v}(B)$

$= 0$ *jinak*

Výrokové spojky: sémantika

A	*B*	¬ *A*	*A* & *B*	*A* V *B*	*A* -> *B*	*A* <-> *B*
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Pravdivost formule (pravdivostní hodnota, model)

Říkáme, že $v(A)$ je *pravdivostní hodnota* formule A při ohodnocení v.
Z praktických důvodů píšeme jen v místo $\underline{v}(A)$.

Říkáme, že *formule* A *je pravdivá* při ohodnocení v , je-li $v(A) = 1$, jinak je A *nepravdivá.*

Je-li formule A pravdivá při ohodnocení v, říkáme, že v je *model* A a píšeme $v \models A$.

Je-li v pravdivostní ohodnocení, A formule, nechť R je množina všech výrokových proměnných ve formuli A.

Snadno se nahlédne, že pravdivostní hodnota formule A při ohodnocení v závisí jenom na pravdivostních hodnotách, které v přiřazuje výrokovým proměnným z R.

Tautologie, splnitelné množiny formulí

Nechť A je formule, T je množina formulí.

(i) Říkáme, že A je *tautologie*, jestliže je pravdivá při každém ohodnocení. Píšeme $\models A$.

(ii) Říkáme, že množina formulí T je *splnitelná* jestliže existuje pravdivostní ohodnocení v takové, že každá formule A z T je pravdivá při ohodnocení v. V takovém případě říkáme, že v je *model* T.

(iii) Říkáme, že A je (tautologickým) důsledkem množiny T a píšeme $T \models A$, jestliže formule A je pravdivá v každém modelu množiny formulí T .

Poznámka.

V definici důsledku množiny formulí T je zahrnut i případ, kdy množina T není splnitelná. V takovém případě T nemá žádný model a formule A je formálně splněna v každém modelu množiny T.

Formální argument probíhá následujícím způsobem:

množina modelů T je prázdná, tedy formule A je pravdivá v každém prvku prázdné množiny a tedy v každém modelu T.

Tento argument platí pro libovolnou formuli A, tedy důsledkem nesplnitelné množiny formulí je každá formule. Později ukážeme, že nesplnitelná množina formulí je sporná.

Příklady

Definice pravdivosti dává možnost rozhodnout o každé formuli, zda je či není tautologií. S tím spojený algoritmus je výpočtově exponenciálně složitý.

$A \vee \neg A$	Zákon vyloučeného třetího
$\neg (A \,\&\, \neg A)$	Vyloučení kontradikce
$\neg (A \,\&\, B) \iff (\neg A \vee \neg B)$	de Morganova pravidla
$\neg (A \vee B) \iff (\neg A \,\&\, \neg B)$	
$\neg\neg A \iff A$	Zákon dvojité negace

Snadno se zjistí, že pro libovolné ohodnocení v a libovolné formule $A, B,$ je-li v modelem A a $A \rightarrow B$ potom v je modelem B.

Odtud také plyne, že pro libovolnou množinu formulí T a formuli $A,$ plyne

$T \models A$ a $T \models A \rightarrow B$ implikuje $T \models B$

To je sémantické zdůvodnění odvozovacího pravidla *modus ponens:* Jsou-li formule A a $A \rightarrow B$ pravdivé při nějakém ohodnocení v, potom také formule B je pravdivá při ohodnocení v. Tedy

$$v(A) = v(A \rightarrow B) = 1 \quad \text{potom} \quad v(B) = 1$$

Říkáme, že pravidlo modus ponens je korektní.

Častokrát se odvozovací pravidlo modus ponens zapisuje ve tvaru

$$\frac{A \qquad A \rightarrow B}{B}$$

Totéže platí i pro sémantický důsledek: jsou-li formule A a $A \rightarrow B$ pravdivé při ohodnocení v, při kterém jsou pravdivé všechny formule z množiny T, potom je i formule B pravdivá při ohodnocení v.
Tedy:

$T \models A$ a $T \models A \rightarrow B$ implikuje $T \models B$.

a

$$\frac{T \models A \qquad T \models A \rightarrow B}{T \models B}$$

Odpověď na druhou otázku

Dá se to dokázat ?

přesněji, je možné danou formuli A dokázat ?

dává *formální systém výrokové logiky*, který teprve musíme vytvořit.

Formální systém výrokové logiky

- Jazyk / Redukce jazyka
- Axiomy / schemata axiomů
- Odvozovací pravidlo
- Důkazy
- Důkazy z předpokladů
- Věta o dedukci

Redukce jazyka

Chceme-li úsporně volit axiomy, je výhodné redukovat počet spojek na spojky základní, v našem případě na negaci a implikaci $\neg$, –> a ostatní spojky z nich odvodit. Uvedená volba základních spojek není jediná možná, můžeme zvolit třeba $\neg$, & nebo $\neg$, $\vee$ nehodí se $\vee$, <-> nebo -> , <-> nebo ->, $\vee$ a další.

Potom

$(A \vee B)$ je zkratka za formuli $(\neg A \rightarrow B)$

$(A \,\&\, B)$ je zkratka za formuli $\neg (A \rightarrow \neg B)$

$(A \leftrightarrow B)$ je zkratka za formuli $(A \rightarrow B) \,\&\, (B \rightarrow A)$

Axiomy

Jsou-li výrazy $A,\ B,\ C$ formule, pak každá formule následujících tvarů je axiom výrokové logiky.

$A1$ $\quad (A \to (B \to A))$

$A2$ $\quad (A \to (B \to C)) \to [(A \to B) \to (A \to C)]$

$A3$ $\quad (\neg B \to \neg\, A) \to (A \to B)$

Protože pro každou volbu formulí A, B, C vznikne nový axiom - jedna instance výrazů $A1$, $A2$, $A3$ říkáme , že $A1$, $A2$, $A3$ jsou *schemata axiomů.*

Z jazyka výrokové logiky lze vytvořit nekonečně mnoho formulí, proto každé schema axiomů zastupuje nekonečně mnoho axiomů , které nazýváme jeho *instancemi* .

Formální systém výrokové logiky má tedy tři schemata axiomů.

Je-li množina výrokových proměnných spočetná, je spočetná množina všech formulí a množina všech axiomů.

Odvozovací pravidlo modus ponens (MP) je jediným odvozovacím pravidlem výrokové logiky.

Z formulí *A* a *A –>B* odvoď formuli *B*.

Pravidlo *modus ponens* se často zapisuje ve tvaru

$$\frac{A \qquad A \;\text{->}\; B}{A}$$

Formule *A1, A2* a *A3* , které určují schemata axiomů jsou tautologie a každý axiom z nich odvozený je také tautologie.

Odvozovací pravidlo modus ponens (MP) je korektní, z formulí pravdivých při nějakém ohodnocení odvozuje pravdivé formule, speciálně z tautologií odvozuje tautologie.

Definice. (Důkaz, dokazatelnost)

(i) Je-li A formule, říkáme, že konečná posloupnost formulí $A_1, A_2, \ldots, A_n$ je *důkazem formule* A, jestliže

a) A_n formule A

b) a pro každé i, $1 \leq i \leq n$ je formule A_i buď axiom nebo je odvozena pravidlem modus z předchozích formulí v důkazu A_j, A_k, kde $j, k < i$.

(ii) Existuje-li důkaz formule A, říkáme, že A je *dokazatelná* ve výrokové logice nebo, že A je větou výrokové logiky a píšeme $\vdash A$.

Jednoduché věty výrokové logiky

$$A \rightarrow A \qquad \text{(v1)}$$

Sestrojíme posloupnost formulí, která bude důkazem formule (v1).

$\vdash A \rightarrow ((A \rightarrow A) \rightarrow A)$ instance $A1$

$\vdash (A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow [(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)]$ instance $A2$

$\vdash (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$ modus ponens

$\vdash A \rightarrow (A \rightarrow A))$ instance $A1$

$\vdash A \rightarrow A$ modus ponens

Definice. (Důkaz z předpokladů)

Nechť T je množina formulí, nechť A je formule. (i) Říkáme, že posloupnost formulí

$$A_1, A_2, \ldots, A_n$$

je *důkaz formule A z (množiny předpokladů) T*, jestliže

(i) A_n je formule A,

(ii) a pro každé i, $1 \leq i \leq n$ je každá fomule A_i axiom nebo prvek T nebo je odvozena z předchozích formulí A_j, A_k, $j, k < i$ pravidlem modus ponens.

(ii) Existuje-li důkaz formule A z předpokladů T, říkáme, že *A je dokazatelná z T* a píšeme

Věta o dedukci

Nechť T je množina formulí a nechť A, B jsou formule, potom

$$T \vdash A \rightarrow B \text{ právě když } T \cup \{A\} \vdash B$$

Poznámky. Místo $T \cup \{A\}$ na pravé straně píšeme T, A. Pravá strana ekvivalence odpovídá tomu, jak se obvykle implikace dokazují.

Věta o dedukci, je větou o existenci důkazů. Existuje-li důkaz tvrzení na levé straně ekvivalence, pak také existuje důkaz tvrzení na pravé straně a naopak.

Důkaz.

=> nechť

$$A_1 , A_2 , \dots , A_{n-1} , \quad A \rightarrow B$$

je důkaz formule $A \rightarrow B$ z předpokladů z množiny T .

Potom

$$A, A_1 , A_2 , \dots , A_{n-1} , \; A_n \equiv A \rightarrow B , B$$

je důkaz formule B z předpokladů z množiny T , A .

Tedy $T, A \vdash B$

<= (myšlenka)

Je-li

$$B_1, B_2, \ldots, B_{m-1}, B_m \equiv B$$

důkaz formule B, z předpokladů z množiny T, A, pro každé $1 \leq i \leq m$ dokážeme

$$T \vdash A \rightarrow B_i$$

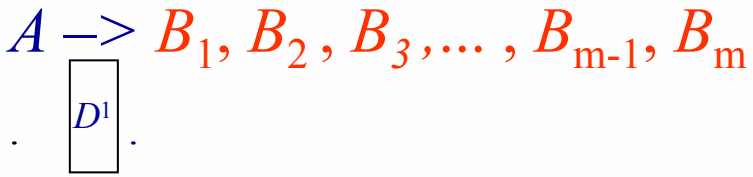
nakonec

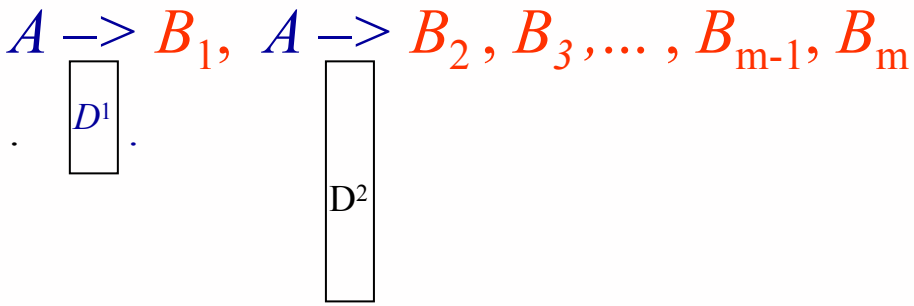
$$T \vdash A \rightarrow B_m \equiv B$$

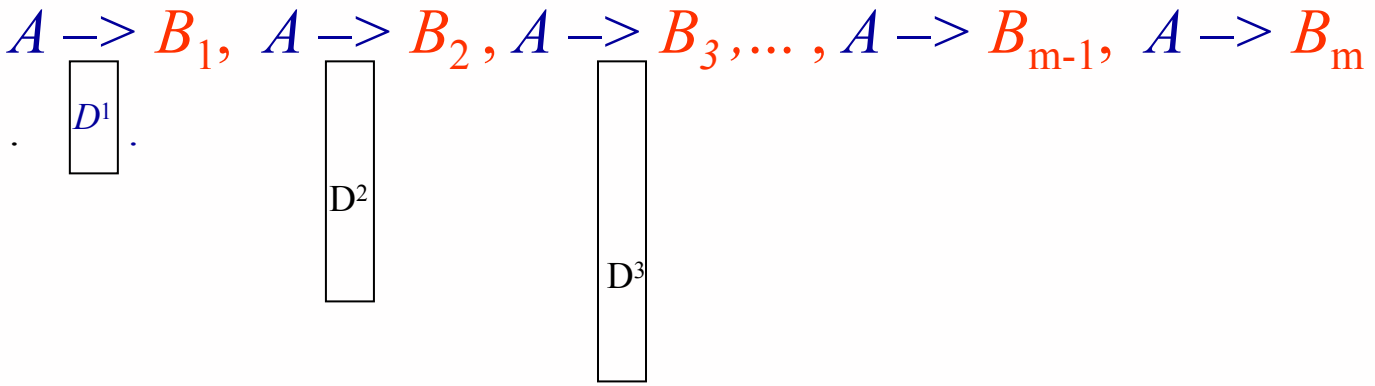
dává požadovaný výsledek

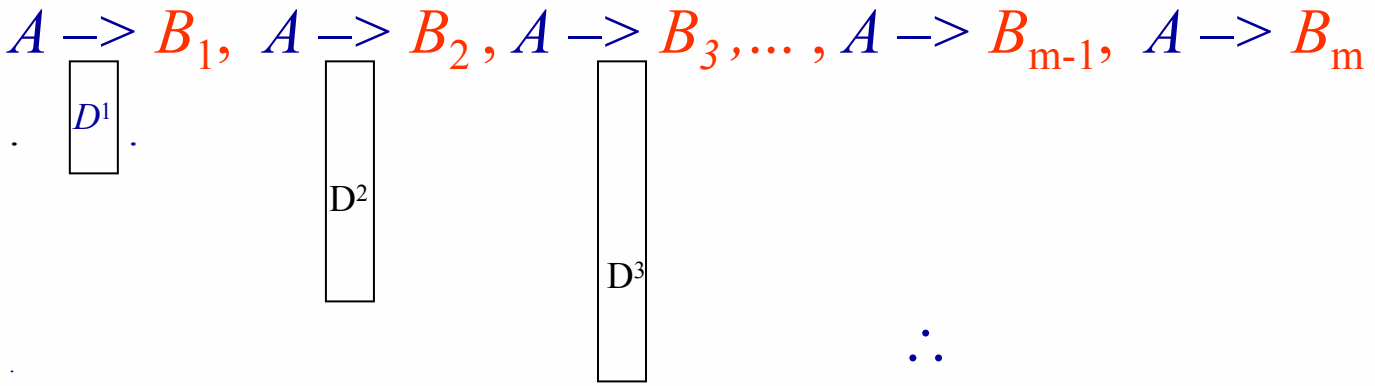
$$T \vdash A \rightarrow B$$

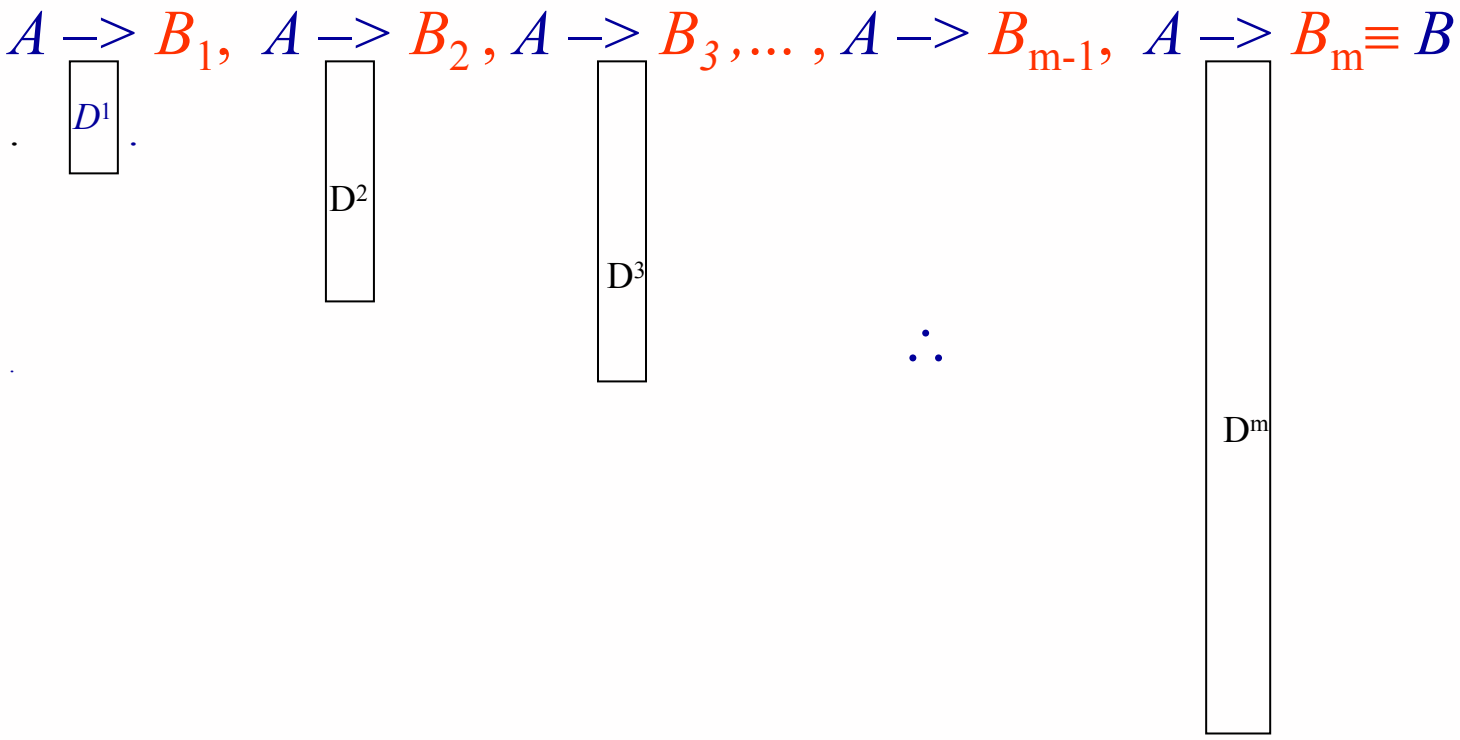
Postupujeme indukcí, jak je znázorněno na dalších snímcích.


A –> B1, B2 , B3 ,… , Bm-1, Bm
D1


A –> B1, A –> B2 , B3 ,… , Bm-1, Bm
D1
D2


A –> B1, A –> B2 , A –> B3 ,... , A –> Bm-1, A –> Bm
D1
D2
D3


A –> B1, A –> B2 , A –> B3 ,... , A –> Bm-1, A –> Bm
D1
D2
D3
∴



Spojením všech důkazů $D^1, D^2, \ldots, D^m$ dostaneme důkaz

$$T \vdash A \rightarrow B$$

<= formálně.

Nechť $T \cup \{A\} \vdash B$ a nechť $B_1, B_2, \ldots, B_m \equiv B$ je důkaz B z předpokladů T, A. Omezenou indukcí pro j, $1 \leq j \leq m$ dokážeme $T \vdash A \rightarrow B_j$.
Tím pro $j = m$ důkaz bude hotov.

Předpokládáme, že pro všechny formule B_k, $k < j$ již bylo dokázáno $T \vdash A \rightarrow B_k$. Rozebereme čtyři případy:

1) B_j je axiom výrokové logiky, potom $B_j \rightarrow (A \rightarrow B_j)$ je instancí schematu $A1$ a $T \vdash A \rightarrow B$ odvodíme pomocí pravidla modus ponens.

2) B_j je předpoklad z T. Postupujeme stejně jako v předešlém případě.

3) B_j je formule A, potom $A \rightarrow B_j$ je věta (v1).

4) B_j je odvozena z formulí B_i, B_k $i, k < j$ pravidlem modus ponens. Bez újmy na obecnosti můžeme předpokládat, že B_i je tvaru $B_k \rightarrow B_j$

Podle indukčního předpokladu

$$T \vdash A \rightarrow B_k$$

$$T \vdash A \rightarrow (B_k \rightarrow B_j) \qquad (1)$$

Ze schematu A*2* plyne

$$T \vdash (A \rightarrow (B_k \rightarrow B_j)) \rightarrow [(A \rightarrow B_k) \rightarrow (A \rightarrow B_j)]$$

Odkud dvojím použitím pravidla modus ponens z předpokladů (1) dostáváme

$$T \vdash A \rightarrow B_j$$

pro každé j , $1 \leq j \leq m$. Pro $j = m$ je $B_m \equiv B$ a věta je dokázána.

“něco jako Speedup (zrychlení)“

$$\vdash A \rightarrow A \qquad \text{(v1)}$$

$$A \vdash A$$

Pomocí Věty o dedukci „dostáváme“ důkaz (v1) v jednom kroku místo původních pěti.

Tato ukázka zrychlení (speedup*u*) důkazu není korektní , protože jsme větu (v1) použili v důkazu Věty o dedukci .

Příklady použití

Skládání implikací

$$\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)] \qquad (1)$$

$$(A \rightarrow B) \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)$$

$$(A \rightarrow B), (B \rightarrow C) \vdash A \rightarrow C$$

$$(A \rightarrow B), (B \rightarrow C), A \vdash C \qquad (2)$$

K důkazu (1) stačí dvojím použitím pravidla modus ponens z předpokladů daných v (2) dokázat C.

$$\frac{A \qquad A \rightarrow B}{B} \qquad\qquad \frac{B \qquad B \rightarrow C}{C}$$

Záměna antecedentů.

$$\vdash ((A \rightarrow (B \rightarrow C)) \rightarrow ((B \rightarrow (A \rightarrow C)) \qquad (3)$$

$$((A \rightarrow (B \rightarrow C)) \vdash (B \rightarrow (A \rightarrow C)$$

$$((A \rightarrow (B \rightarrow C)) , B \vdash (A \rightarrow C)$$

$$((A \rightarrow (B \rightarrow C)) , B , A \vdash C \qquad (4)$$

K důkazu (3) stačí dvojím použitím pravidla modus ponens z předpokladů daných v (4) dokázat C. (Obrácená implikace k (3) se dokáže stejným způsobem, jenom zaměnime jména formulí).

$$\frac{A \qquad (A \rightarrow (B \rightarrow C))}{(B \rightarrow C)} \qquad \frac{B \qquad (B \rightarrow C))}{C}$$

V uvedených příkladech se důkazy opíraly jen o Větu o dedukci a pravidlo modus ponens.

Další pomocné věty.

$$\vdash \neg A \rightarrow (A \rightarrow C) \qquad \text{(v2)}$$

Jinými slovy

$$\vdash \neg A \rightarrow (A \rightarrow \mathit{Cokoliv}) \qquad \text{(v2)}$$

$\vdash \neg A \rightarrow (A \rightarrow C)$ (v2)

$\vdash \neg A \rightarrow (\neg B \rightarrow \neg A)$	*schema A1*
$\neg A \vdash \neg B \rightarrow \neg A$	*Věta o dedukci* (VD)
$\neg A \vdash A \rightarrow B$	*A3 , MP*
$\vdash \neg A \rightarrow (A \rightarrow B)$	VD

Tím je věta (v2) dokázána.

$\vdash \neg\neg A \rightarrow A$ (v3)

$\vdash \neg\neg A \rightarrow (\neg A \rightarrow \neg\neg\neg A)$ (v2)

$\neg\neg A \vdash \neg A \rightarrow \neg\neg\neg A$ VD

$\neg\neg A \vdash \neg\neg A \rightarrow A$ A3 , MP

$\neg\neg A \vdash A$ VD

$\vdash \neg\neg A \rightarrow A$ VD

Formuli (v3) lze zapsat ve tvaru

$$\neg A \vee A$$

a to je zákon vyloučeného třetího (tertium non datur).
Naše logika je tedy klasická, ne intuicionistická.

$\vdash A \rightarrow \neg\neg A$ (v4)

$\vdash \neg\neg\neg A \rightarrow \neg A$ (v3)

$\vdash A \rightarrow \neg\neg A$ A3 , MP

$\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$ (v5)

$\neg\neg A , A \rightarrow B \vdash A$ (v3) , MP

(tedy $\neg\neg A , \neg\neg A \rightarrow A \vdash A$, odkud)

$\neg\neg A , A \rightarrow B \vdash \neg\neg B$ MP

(víme $\vdash B \rightarrow \neg\neg B$) podle (v4)

$A \rightarrow B \vdash \neg\neg A \rightarrow \neg\neg B$ VD

$A \rightarrow B \vdash \neg B \rightarrow \neg A$ A3 , MP

$\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$ VD

$\vdash A \rightarrow (\neg B \rightarrow \neg (A \rightarrow \neg B))$ (v6)

$A , A \rightarrow \neg B \vdash \neg B$	MP
$A \vdash (A \rightarrow \neg B) \rightarrow \neg B$	VD
$A \vdash \neg B \rightarrow \neg (A \rightarrow \neg B)$	(v5), MP
$\vdash A \rightarrow (\neg B \rightarrow \neg (A \rightarrow \neg B))$	VD

$\vdash (\neg A \rightarrow A) \rightarrow A$ (v7)

$\vdash \neg A \ (\neg A \rightarrow \neg(\neg A \rightarrow A))$ (v6)

$\neg A \vdash \neg A \rightarrow \neg(\neg A \rightarrow A))$ VD

$\neg A \vdash \neg(\neg A \rightarrow A))$ VD

$\vdash \neg A \rightarrow \neg(\neg A \rightarrow A))$ VD

$\vdash (\neg A \rightarrow A) \rightarrow A$ A3 , MP

Cvičení.

Dokažte

a) $\vdash (A \rightarrow \neg B) \rightarrow (B \rightarrow \neg A)$

b) $\vdash (\neg A \rightarrow B) \rightarrow (\neg B \rightarrow A)$

Cvičení A

Množinu všech formulí dokazatelných z T označíme $Con(T)$, tedy

$$Con(T) = \{A \mid T \vdash A\}$$

Nechť T a S jsou množiny formulí. Dokažte:

a) $T \subseteq Con(T)$

b) *je-li* $T \subseteq S$ *potom* $Con(T) \subseteq Con(S)$

c) $Con(Con(T)) = Con(T)$

d) *je-li* T *bezesporná , potom také* $Con(T)$ *je bezesporná.*

Bezespornost množiny předpokladů

Říkáme, že *množina T výrokových formulí je sporná*, jestliže je z ní možno dokázat každou formuli.

Jinak říkáme, že *množina T je bezesporná*.

V analogii k predikátové logice budeme někdy množinu výrokových formulí T nazývat teorií.

Věta

Pro každou formuli A platí

$T \vdash A$ právě když $T \cup \{\neg A\}$ je sporná množina.

Důkaz. (=>) Je-li formule A dokazatelná z T,

tedy je-li

$T \vdash A$ (1)

podle věty (v2) platí

$\vdash \neg A \rightarrow (A \rightarrow B)$ kde B je libovolná formule,

záměnou předpokladů v implikaci (v2) dostaneme

$$\vdash A \rightarrow (\neg A \rightarrow B) \qquad (2)$$

$$T \vdash (\neg A \rightarrow B) \qquad (1), (2), \text{MP}$$

$$T, \neg A \vdash B) \qquad \text{VD}$$

odkud pravidlem modus ponens pomocí (1) odvodíme

$$T, \neg \text{A} \vdash B$$

kde B je libovolná formule, to znamená, že $T \cup \{\neg A\}$ je sporná množina formulí.

Zbývá odvodit obrácenou implikaci.

(<=) Je-li množina $T \cup \{\neg A\}$ sporná, potom z ní lze odvodit libovolnou formuli, například formuli A .

Dostáváme

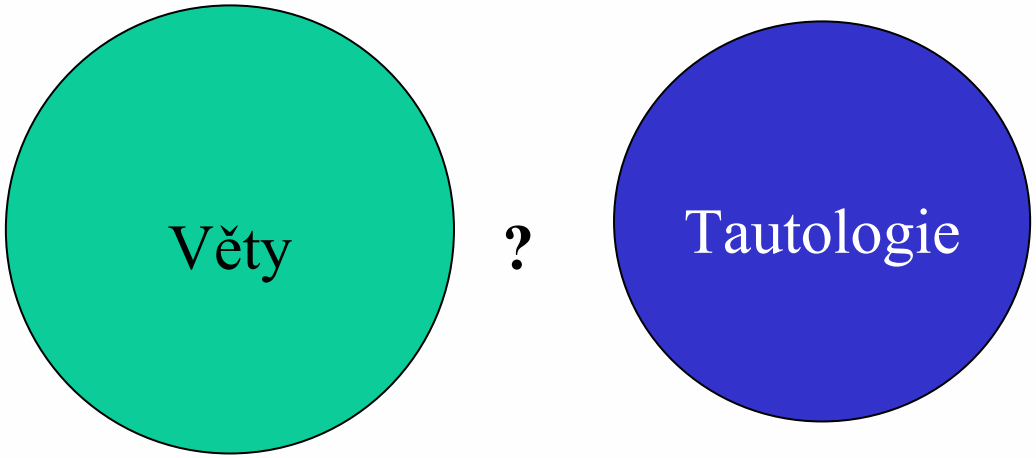
$T , \neg A \vdash A$	odtud Větou od dedukci
$T \vdash \neg A \rightarrow A$	(3) podle (v7) platí
$\vdash (\neg A \rightarrow A) \rightarrow A$	
$T \vdash A$	(3) , MP

Tím je věta dokázána.

Dokázali jsme několik pomocných vět výrokové logiky.

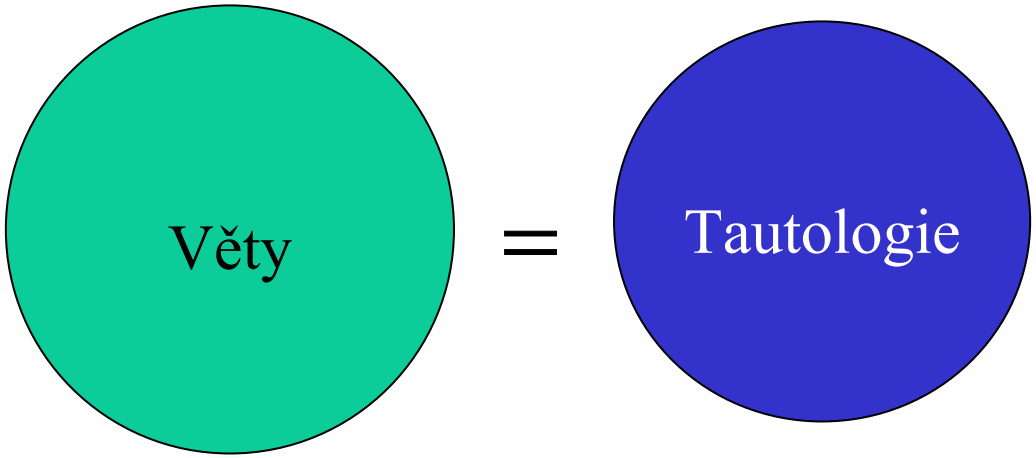
Nyní se budeme zabývat vztahem vět odvoditelných ve formálním systému výrokové logiky a formulemi sémanticky pravdivými, tedy tautologiemi.

Naším cílem je dokázat *Větu o úplnosti*, která dává dohromady oba pojmy: *pojem věty a pojem tautologie.*



Formální systém Sémantika

Věta o úplnosti:



Formální systém Sémantika

Věta o úplnosti

Bezespornost a maximalita

Nechť T je množina formulí

(i) Říkáme, že T je sporná, (nekonzistentní), jestliže libovolná formule A je dokazatelná z předpokladů T, jinak je T bezesporná (konzistentní).

(ii) T je maximální bezesporná množina , jestliže je bezesporná a neexistuje bezesporná množina T' , která je různá od T a obsahuje T.

Větu o úplnosti dokážeme jako důsledek silnějšího tvrzení

Věty o bezespornosti a splnitelnosti.

Cvičení B

Nechť T je množina formulí výrokové logiky a nechť A ,B jsou libovolné formule

a) množina T je sporná, právě když T |- A & ¬ A pro nějakou formuli A .

V dalším předpokládejme, že T maximální bezesporná množina, potom

b) T |- A platí, právě když formule A je prvkem T ,

c) pro libovolnou formuli A , právě jedna z fomulí

A , ¬ A je prvkem T ,

d) *konjunkce* $A \,\&\, B$ *je prvkem* T,

právě když

formule A *a* B *leží v* T,

e) *disjunkce* $A \vee B$ *je prvkem* T,

právě když

A *nebo* B *je prvkem* T.

Věta (Lindenbaum)

Každnou bezespornou množinu formulí T lze rozšířit do maximální bezesporné množiny S , $T \subseteq S$.

Důkaz.

Uspořádejme všechny formule jazyka do posloupnosti

$$A_1, A_2, \ldots, A_n, \ldots \qquad (1)$$

na uspořádání formulí nezáleží, důležité je, aby posloupnost byla prostá.

Vytvoříme neklesající posloupnost bezesporných množin

$$T = T_0 \subseteq T_1 \subseteq T_2 \subseteq \ \ldots \ \subseteq \ T_n \subseteq \ \ldots$$

následujícím postupem.

Je-li $T \cup \{ A_1 \}$ bezesporná množina položíme

$$T_1 = T \cup \{A_1\} ,$$

je-li sporná, pak

$$T_1 = T$$

V i -tém kroku testujeme zda množina $T_i \cup \{A_i\}$ je bezesporná. V kladném případě položíme

$$T_{i+1} = T_i \cup \{A_i\}$$

je-li sporná, položíme

$$T_{i+1} = T_i .$$

Nechť S je sjednocení všech množin T_n .

Nejprve ukážeme, že S je bezesporná množina.

Předpokládejme naopak, že S není bezesporná. Potom existuje důkaz sporu, z předpokladů S

$$B_1, B_2, \ldots, B_n$$

(například důkaz formule $p \,\&\, \neg p$) .

Nechť

$$C_1, C_2, \ldots, C_m \qquad (1)$$

jsou všechny formule z S, které se vyskytují v uvedeném důkazu. Z předpokladů (1) lze tedy dokázat spor.

Pak pro nějakýdostatečně velký index k jsou všechny formule z (1) jsou prvkem množiny T_k , která je podle konstrukce bezesporná - spor .

Zbývá dokázat, že S je maximální bezesporná množina.
Předpokládejme, že S' je bezesporná množina a $S \subseteq S'$.

Pro každou formuli A_n z posloupnosti formulí (1) ,
která je prvkem S' je množina

$$T_{n+1} = T_n \cup \{A_n\} \subseteq S$$

bezesporná, a tedy A_n je prvkem S .

Ukázali jsme, že $S = S'$, a tedy S je maximální.

Věta o bezespornosti a splnitelnosti

Je-li T množina formulí výrokové logiky, potom

T je bezesporná, právě když je splnitelná.

Důkaz.

a) Předpokládejme, že T je splnitelná a v je model T, tedy $v \models T$.

Ukážeme, že každá formule dokazatelná z předpokladů T, je pravdivá při ohodnocení v. Postupujeme indukcí.

Nechť $A_1, A_2, \ldots, A_n$ je důkaz formule A_n z předpokladů T.

Pro libovolné m, $m \leq n$ platí

Je-li A_m axiom výrokové logiky, nebo prvek T, platí

$$v \models A_m .$$

Je-li A_m odvozena z formulí $A_i\, A_i \rightarrow A_m$ pravidlem modus ponens, pak z indukčního předpokladu a korektnosti pravidla modus ponens dostáváme $\nu \models A_m$.

Tedy každá formule dokazatelná z předpokladů T je pravdivá při ohodnocení v.

Protože $p \,\&\, \neg\, p$ pro výrokovou proměnnou p není pravdivá při ohodnocení v, není tato formule dokazatelná z T a T je bezesporná množina.

b) Nyní předpokládejme, že T je bezesporná. Podle Lindenbaumovy věty, lze T rozšířit do maximální bezesporné nadmnožiny S.

Nechť v je pravdivostní ohodnocení, které je modelem T, tedy ohodnocení definované vztahem

$$v(p) = 1 \quad \textit{právě když} \quad p \in \mathrm{S}$$

je také modelem T.

Pro libovolnou formuli A dokážeme

$$A \in S \quad \textit{právě když} \quad \nu \models A \qquad (1)$$

Postupujeme indukcí podle složitosti formule A.

Přímo z definice plyne (1) pro výrokové proměnné.

Ze cvičení c) plyne, že platí-li (1) pro B, pak platí i pro $\neg B$.

Ze cvičení e) plyne, že platí-li (1) pro $\neg B$ a C, pak platí i pro $B \to C$.

Tím je (1) dokázáno pro libovolnou formuli A .

Tedy ν je modelem S a podle Lindenbaumovy věty je $T \subseteq S$, to znamená, že ν je také modelem T.

Množina T je tedy splnitelná.

c) *pro libovolnou formuli* A , *právě jedna z fomulí* A , $\neg A$ *je prvkem* T ,

e) *disjunkce* $A \vee B$ *je prvkem* T ,

právě když

A *nebo* B *je prvkem* T .

Důsledek. **Věta o úplnosti.**

Je-li T množina formulí, A formule, potom platí

(*i*) $T \vdash A$ *právě když* $T \models A$

(*ii*) $\vdash A$ *právě když* $\models A$

Z (ii) plyne, že

A je větou výrokové logiky *právě když* A je tautologie.

Důkaz. (*i*) Víme, že

$$T \vdash A \quad \textit{právě když} \quad T \cup \{\neg A\} \text{ je sporná}$$

$$\textit{právě když} \quad T \cup \{\neg A\} \text{ je nesplnitelná}$$

$$\textit{právě když} \quad T \models A$$

(*ii*) Tvrzení je speciálním případem (*i*) pro $T = 0$.

Důsledek.

Výroková logika je bezesporná.

Důkaz. Z Věty o úplnosti plyne, že ve výrokové logice jsou dokazatelné právě tautologie.

Pro kteroukoli výrokovou proměnnou p, formule

$$p \,\&\, \neg\, p$$

není tautologie, a proto není větou výrokové logiky.

Podle definice je tedy výroková logika bezesporná.

Věta o kompaktnosti.

Množina formulí T je splnitelná, právě když je splnitelná každá konečná podmnožina množiny T.

Důsledek.

Je-li $T \models A$,

pak existuje konečná podmnožina $T' \subseteq T$,

taková, že $T' \models A$.

Důkaz. Věty o kompaktnosti.

a*)* (->) *Je-li množina formulí* T *splnitelná, pak je splnitelná i každá její část.*

b) (<-) Předpokládejme, že T není splnitelná. Podle věty o splnitelnosti je množina T sporná. Tedy $T \vdash p \,\&\, \neg p$ pro nějakou výrokovou proměnnou.
Ale důkaz sporu využívá jen konečnou podmnožinu T' množiny T. Tedy T' je sporná a proto není ani splnitelná.

Ukázali jsme, že pokud množina T není splnitelná, pak existuje její konečná podmnožina, která také není splnitelná.

Důkaz. Důsledku věty o kompaktnosti.

Předpokládejme $T \models A$.

Z věty o úplnosti dostáváme

$$T' \vdash A \qquad (1)$$

pro nějakou konečnou podmnožinu T' množiny T sestávající z formulí, které se použijí v důkazu na pravé straně tvrzení (1).

Použijeme-li větu o úplnosti a dostáváme $T' \models A$.

Normální tvary výrokových formulí

Ke každé formuli dovoluje výroková logika sestrojit ekvivalentní formuli v určitém standardním tvaru. Jsou to tvary výrokových formulí, které lze použít jako vstup do počítače.

Potřebujeme

- Vědět něco o dokazování formulí s odvozenými spojkami.
- Větu o ekvivalenci (kterou jsme mohli dokázat již dříve).
- Normální tvary výrokových formulí. (Jsou dva).

Lemma.

(i) $A \,\&\, B \vdash A$ a $A \,\&\, B \vdash B$

podle Věty o dedukci dostáváme

$\vdash (A \,\&\, B) \to A$ a $\vdash (A \,\&\, B) \to A$

(ii) $A, B \vdash A \,\&\, B$

a podle Věty o dedukci

$\vdash (A \to (B \to (A \,\&\, B)))$

Důkaz.

(i) Výraz $A \,\&\, B$ je zkratkou pro formuli $\neg (A \rightarrow \neg B)$.

Podle (v2) platí

$$\vdash \neg A \rightarrow (A \rightarrow \neg B)$$

odkud $\vdash \neg (A \rightarrow \neg B) \rightarrow A$ (v3), (v5),MP

tedy $\vdash (A \,\&\, B) \rightarrow A$

Zbytek plyne z věty o dedukci.

Důkaz druhého tvrzení v (i)

|- $\neg B \rightarrow (A \rightarrow \neg B)$ instance axiomu (A1)

|- $\neg (A \rightarrow \neg B) \rightarrow B$ (v5), MP

|- $(A \,\&\, B) \rightarrow B$

Důkaz (ii) z (v6) dostáváme

$$\vdash A \to (\neg\neg B \to \neg (A \to \neg B))$$

z věty o dedukci plyne

$$A, \neg\neg B \vdash A \,\&\, B \qquad \text{(v3)}$$

tedy

$$A,B \vdash A \,\&\, B$$

z věty o dedukci

$$\vdash A \to (B \to (A \,\&\, B))$$

Důsledek.

Uvědomíme-li si, že ekvivalence $A \leftrightarrow B$ je zkratkou za formuli

$$(A \rightarrow B) \,\&\, (B \rightarrow A)$$

dostáváme

(i) $A \leftrightarrow B \vdash A \rightarrow B$

(ii) $A \leftrightarrow B \vdash B \rightarrow A$

(iii) $A \rightarrow B \,\&\, A \rightarrow B \vdash A \leftrightarrow B$

(iv) Pro libovolnou množinu formulí T a libovolné formule A, B z $T \vdash A \leftrightarrow B$ plyne

$T \vdash A$ právě když $T \vdash B$.

Důsledek.

(i) $\vdash A \leftrightarrow (A \,\&\, A)$ (idempotence)

(ii) $\vdash (A \,\&\, B) \leftrightarrow (B \,\&\, A)$ (komutativnost)

(iii) $\vdash ((A \,\&\, B) \,\&\, C) \leftrightarrow (A \,\&\, (B \,\&\, C))$ (asociativnost)

(iv) $\vdash (A_1 \rightarrow \ldots (A_n \rightarrow B)) \leftrightarrow ((A_1 \,\&\, \ldots \,\&\, A_n) \rightarrow B)$

Věta o ekvivalenci.

Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $A_1, A_2, \ldots, A_n$ formulemi $A_1', A_2', \ldots, A'_n$.

Je-li

$$\vdash A_1 \leftrightarrow A_1' \quad \vdash A_2 \leftrightarrow A_2' \quad \ldots \vdash A_n \leftrightarrow A_n'$$

potom

$$\vdash A \leftrightarrow A'$$

Důkaz.

Indukcí podle složitosti formule A.

a) A je výroková proměnná nebo některá z formulí A_j $j \leq n$,

potom A' je formule A .

b) A je formule $\neg B$ potom z indukčního předpokladu pro B dostáváme

$$|- B <-> B'$$

a podle předchozího důsledku (i)

$$|- B -> B'$$

a z (v5) také $|- A' -> A$.

Opačná implikace se dokazuje podobně.

c) A je $B \rightarrow C$ a z indukčního předpokladu je

$$\vdash B \leftrightarrow B' \text{ a } \vdash C \leftrightarrow C' .$$

Potom také

$$\vdash B' \rightarrow B \quad \text{a} \quad \vdash C \rightarrow C'$$

následující formule je tautologie (skládání implikací)

$$\vdash (B' \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow ((C \rightarrow C') \rightarrow (B' \rightarrow C')))$$

$$\vdash (B \rightarrow C) \rightarrow (B' \rightarrow C') \qquad \text{2x MP}$$

Opačná implikace se dokáže záměnou čárkovaných a nečárkovaných formulí.

de Morganova pravidla.

(i) $\vdash \neg (A \,\&\, B) \leftrightarrow (\neg A \vee \neg B)$

(ii) $\vdash \neg (A \vee B) \leftrightarrow (\neg A \,\&\, \neg B)$

Důkaz.

Z (v3), (v4) a zavedení ekvivalence plyne $\vdash A \leftrightarrow \neg\neg A$

Užitím věty o ekvivalenci dostáváme

$$\vdash \neg (A \,\&\, B) \leftrightarrow \neg\neg (A \rightarrow \neg B)$$

$$\leftrightarrow (\neg\neg A \rightarrow \neg B)$$

$$\leftrightarrow (\neg A \vee \neg B)$$

Tvrzení (ii) se dokazuje obdobně.

Důsledek.

(i) $\vdash A \rightarrow (A \vee B) \quad \vdash B \rightarrow (A \vee B)$ (monotonnost)

(ii) $\vdash A \leftrightarrow (A \vee A)$ (idempotence)

(iii) $\vdash (A \vee B) \leftrightarrow (B \vee A)$ (komutativnost)

(iv) $\vdash ((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$ (asociativnost)

Důkaz.

(i) Podle zavedení disjunkce je $\vdash (A \vee B) <-> (\neg A \to B)$ proto formule $A \to (A \vee B)$ je obdobou (v2) a $B \to (A \vee B)$ je instancí schematu (A1).

(ii) - (iv) Použitím de Morganových pravidel lze tato tvrzení převést na již dokázaná tvrzení o konjunkci.

Lemma o důkazu rozborem případů.

Je-li T množina formulí a A, B, C jsou formule, potom

$T, (A \vee B) \vdash C$ *právě když* $T, A \vdash C$ a $T, B \vdash C$

Důkaz.

=> Je-li $T, (A \vee B) \vdash C$ z monotonnosti disjunkce a Věty o dedukci dostáváme $T, A \vdash (A \vee B)$ a $T, B \vdash (A \vee B)$

odkud plyne $T, A \vdash C$ a $T, B \vdash C$.

<= Je-li naopak $T, A \vdash C$ a $T, B \vdash C$ podle věty o dedukci a (v5) dostáváme

$T, \neg C \vdash \neg A$ a $T, \neg C \vdash \neg B$

tedy $T, \neg C \vdash \neg A \,\&\, \neg B$ konjunkce

$T, \neg C \vdash \neg (A \vee B)$ de Morganovo pravidlo

$T \vdash \neg C \rightarrow \neg (A \vee B)$ VD

$T, (A \vee B) \vdash C$ (A3), VD

Distributivnost konjunkce a disjunkce

(i) $\vdash (A \vee (B \,\&\, C)) \;<\!-\!>\; ((A \vee B) \,\&\, (A \vee C))$

(ii) $\vdash (A \,\&\, (B \vee C)) \;<\!-\!>\; ((A \,\&\, B) \vee (A \,\&\, B))$

Důkaz.

(i) => Použijeme důkaz rozborem případů. Platí

$A \vdash (A \vee B)$ $A \vdash (A \vee C)$ (monotonnost)

Tedy $A \vdash ((A \vee B) \ \& \ (A \vee C))$ (konjunkce)

Podobně

$B \ \& \ C \vdash B$ $B \ \& \ C \vdash C$ (konjunkce)

$B \ \& \ C \vdash A \vee B$ $B \ \& \ C \vdash A \vee C$ (monotonnost)

$B \ \& \ C \vdash (A \vee B) \ \& \ (A \vee C)$ (konjunkce)

podle věty o důkazu rozborem případů

$\vdash (A \vee (B \ \& \ C)) \rightarrow ((A \vee B) \ \& \ (A \vee C))$

(i) <= Platí

$(A \vee B) \,\&\, (A \vee C)) \vdash (A \vee B)\,,\,(A \vee C)$ (konjunkce)

Přitom $A \vee B$ je zkratka za implikaci $\neg A \rightarrow B$ (1)

Tedy

$\neg A\,,\; A \vee B \vdash B$ a $\neg A\,,\; A \vee C \vdash C$

$(A \vee B) \,\&\, (A \vee C) \vdash \neg A \rightarrow (B \,\&\, C)$

VD konjunkce

$\vdash ((A \vee B) \,\&\, (A \vee C)) \rightarrow (A \vee (B \,\&\, C))$

(1) , VD

Tvrzení (ii) se dokazuje podobně.

Normální tvary výrokových formulí

Syntax

- *Výrokové proměnné*
- *Literály* výrokové proměnné a jejich negace
- *Klauzule* disjunkce literálů
- *Formule v konjunktivním tvaru* (CNF) konjukce klauzulí
- *Formule v disjunktivním tvaru* (DNF) disjunkce konjunkcí literálů

Příklady

Nechť $p_1 , p_2 , \ldots , p_n$ jsou výrokové proměnné.

$a)$ $(p_1 \vee \neg p_3 , \vee p_5) \ \& \ p_1 \ \& \ (p_2 \vee p_7)$ je CNF

$b)$ $(p_2 \ \& \ \neg p_3 \ \& \ \neg p_{10}) \ (\neg p_2 \ \& \ \neg p_1)$ je DNF

Věta o normálních tvarech.

Ke každé formuli A lze sestrojit formule A_k, A_d v konjunktivním a disjunktivním tvaru, tak že

$$\vdash A \leftrightarrow A_k \quad \text{a} \quad \vdash A \leftrightarrow A_d$$

Sestrojení formulí A_k a A_d budeme ilustrovat příkladem.

Příklad.

Mějme formuli A tvaru

$$A \equiv p \text{ -> } (q \text{ <-> } s)$$

$$\neg p \vee ((q \text{ -> } s) \,\&\, (s \text{ -> } q))$$

$$\neg p \vee ((\neg q \vee s) \,\&\, (\neg s \vee q))$$

$$(\neg p \vee \neg q \vee s) \,\&\, (\neg p \vee \neg s \vee q) \qquad \text{(CNF)}$$

$$\neg p \vee (\neg q \,\&\, \neg s)\ \ (\neg q \,\&\, q)\ (s \,\&\neg\, s)\ (s \,\&\, q) \qquad \text{(DNF)}$$

Je mnoho metod jak transformovat formule do normalních tvarů. Jsou syntaktické, sémantické nebo kombinují syntaktický a sémantický postup.

V uvedeném příkladu jsme postupovali syntakticky v následujících krocích:

• implikaci a ekvivalenci vyjádřit pomocí ostatních spojek

• stlačit negaci k výrokovým proměnným pomocí de Morganových pravidel při vynechání dvojtých negací

• pomocí distributivity konjunkce a disjunkce vyjádřit normální tvary CNF a DNF.

Po sémantické analýze DNF lze vynechat (sporné) konjunkce $(\neg q \,\&\, q)$ a $(s \,\&\, \neg s)$.