Kapitola 2

Syntaxe a sémantika výrokové logiky

Syntaxe je soubor formálních pravidel pro tvoření korektních vět sestávajících ze slov (v případě přirozených jazyků), nebo formálních výrazů sestávajících ze symbolů (např. příkazy v programovacím jazyce). Naproti tomu *sémantika* popisuje význam takových výrazů. Vztah mezi syntaxí a sémantikou se prolíná celou logikou a je klíčem k jejímu pochopení.

2.1 Syntaxe výrokové logiky

Nejprve definujeme formální 'nápisy', se kterými budeme v logice pracovat.

2.1.1 Jazyk

Jazyk výrokové logiky je určený neprázdnou množinou *výrokových proměnných* $\mathbb{P}$ (také jim říkáme *prvovýroky* nebo *atomické výroky*). Tato množina může být konečná nebo i nekonečná, obvykle ale bude spočetná[1] (pokud neřekneme jinak), a bude mít dané uspořádání. Pro výrokové proměnné budeme obvykle používat označení p_i (od slova "proposition"), ale pro lepší čitelnost, zejména je-li $\mathbb{P}$ konečná, také $p, q, r, \ldots$ Například:

$$\mathbb{P}_1 = \{p, q, r\}$$
$$\mathbb{P}_2 = \{p_0, p_1, p_2, p_3, \ldots\} = \{p_i \mid i \in \mathbb{N}\}$$

Do jazyka patří kromě výrokových proměnných také *logické symboly*: symboly pro logické spojky $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ a závorky $(,)$. Budeme ale pro jednoduchost mluvit o "jazyce $\mathbb{P}$".

Poznámka 2.1.1. Pokud budeme potřebovat formálněji vyjádřit uspořádání jazyka $\mathbb{P}$, představíme si ho jako bijekci $\iota\colon \{0, 1, \ldots, n-1\} \to \mathbb{P}$ (pro konečný, n-prvkový jazyk) resp. $\iota\colon \mathbb{N} \to \mathbb{P}$ (je-li $\mathbb{P}$ spočetně nekonečný). V našich příkladech $\iota_1(0) = p$, $\iota_1(1) = q$, $\iota_1(2) = r$, a $\iota_2(i) = p_i$ pro všechna $i \in \mathbb{N}$.[2]

[1] To je důležité v mnoha aplikacích v informatice, nespočetné množiny se do počítače nevejdou.

[2] Množina přirozených čísel $\mathbb{N}$ obsahuje nulu, viz standard ISO 80000-2:2019.

2.1.2 Výrok

Základním stavebním kamenem výrokové logiky je *výrok* neboli *výroková formule*. Je to konečný řetězec sestavený z výrokových proměnných a logických symbolů podle jistých pravidel. Prvovýroky jsou výroky, a dále můžeme vytvářet výroky z jednodušších výroků a logických symbolů: například pro logickou spojku $\wedge$ vypíšeme nejprve symbol '(', potom první výrok, symbol '$\wedge$', druhý výrok, a nakonec symbol ')'.

Definice 2.1.2 (Výrok)**.** *Výrok* (*výroková formule*) v jazyce $\mathbb{P}$ je prvek množiny $\mathrm{VF}_{\mathbb{P}}$ definované následovně: $\mathrm{VF}_{\mathbb{P}}$ je nejmenší množina splňující[3]

- pro každý prvovýrok $p \in \mathbb{P}$ platí $p \in \mathrm{VF}_{\mathbb{P}}$,
- pro každý výrok $\varphi \in \mathrm{VF}_{\mathbb{P}}$ je $(\neg\varphi)$ také prvek $\mathrm{VF}_{\mathbb{P}}$
- pro každé $\varphi, \psi \in \mathrm{VF}_{\mathbb{P}}$ jsou $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, a $(\varphi \leftrightarrow \psi)$ také prvky $\mathrm{VF}_{\mathbb{P}}$.

Výroky označujeme obvykle řeckými písmeny φ, ψ, χ (φ od slova "formule"). Abychom nemuseli vypisovat všechny čtyři binární logické spojky, používáme pro ně někdy zástupný symbol $\square$. Třetí bod definice bychom tedy mohli vyjádřit takto:

- pro každé $\varphi, \psi \in \mathrm{VF}_{\mathbb{P}}$ a $\square \in \{\wedge, \vee, \to, \leftrightarrow\}$ je $(\varphi \square \psi)$ také prvek $\mathrm{VF}_{\mathbb{P}}$.

Podvýrok (*podformule*) je podřetězec, který je sám o sobě výrokem. Uvědomte si, že všechny výroky jsou nutně konečné řetězce, vzniklé aplikací konečně mnoha kroků z definice na své podvýroky.

Příklad 2.1.3. Výrok $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \to (p \wedge q)))$ má následující podvýroky: $p, q, (\neg q), (p \vee (\neg q)), r, (p \wedge q), (r \to (p \wedge q)), \varphi$.

Výrok v jazyce $\mathbb{P}$ nemusí obsahovat všechny prvovýroky z $\mathbb{P}$ (ani nemůže pokud je $\mathbb{P}$ nekonečná množina). Bude se nám proto hodit značení $\mathrm{Var}(\varphi)$ pro množinu prvovýroků vyskytujících se ve φ.[4] V našem příkladě $\mathrm{Var}(\varphi) = \{p, q, r\}$.

Zavedeme si zkratky pro dva speciální výroky: $\top = (p \vee (\neg p))$ (*pravda*) a $\bot = (p \wedge (\neg p))$ (*spor*), kde $p \in \mathbb{P}$ je pevně zvolený (např. první prvovýrok z $\mathbb{P}$). Tedy výrok $\top$ je vždy pravdivý a výrok $\bot$ je vždy nepravdivý.

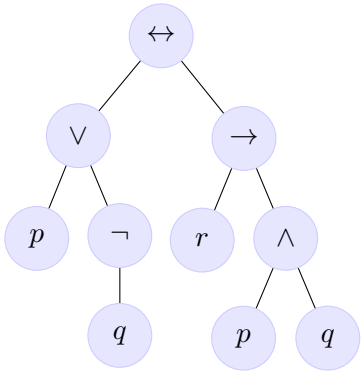
Při zápisu výroků můžeme pro lepší čitelnost některé závorky vynechat. Např. výrok φ z příkladu 2.1.3 můžeme reprezentovat nápisem $p \vee \neg q \leftrightarrow (r \to p \wedge q)$. Vynecháváme vnější závorky a používáme prioritu operátorů: $\neg$ má nejvyšší prioritu, dále $\wedge, \vee$, a konečně $\to, \leftrightarrow$ mají nejnižší prioritu. Dále nápisem $p \wedge q \wedge r \wedge s$ myslíme výrok $(p \wedge (q \wedge (r \wedge s)))$, a podobně pro $\vee$.[5][6]

[3] Takovému druhu definice říkáme *induktivní*. Lze také přirozeně vyjádřit pomocí *formální gramatiky*, viz předmět NTIN071 Automaty a gramatiky.

[4] Pokud nespecifikujeme v jakém jazyce je výrok (a pokud to není jasné z kontextu), myslíme tím, že je v jazyce $\mathrm{Var}(\varphi)$.

[5] Díky asociativitě $\wedge, \vee$ na uzávorkování nezáleží.

[6] Někdy se zavádí jemnější priority, $\wedge$ mívá vyšší prioritu než $\vee$, $\to$ vyšší než $\leftrightarrow$. A někdy se píše $p \to q \to r$ místo $(p \to (r \to q))$, byť $\to$ není asociativní a na uzávorkování záleží. Obojímu se ale raději vyhneme.



Obrázek 2.1: Strom výroku $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$

2.1.3 Strom výroku

V definici výroku jsme zvolili *infixový* zápis se závorkami čistě z důvodu čitelnosti pro člověka. Nic by nám nebránilo použít *prefixový* zápis ("polskou notaci"), tj. definovat výroky takto:

- každý prvovýrok je výrok, a
- jsou-li φ, ψ výroky, jsou také $\neg\varphi$, $\wedge\varphi\psi$, $\vee\varphi\psi$, $\rightarrow\varphi\psi$, a $\leftrightarrow\varphi\psi$ výroky.

Výrok $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$ bychom potom zapsali jako $\varphi = \leftrightarrow\vee p\neg q\rightarrow r\wedge pq$. Také bychom mohli použít *postfixový* zápis a psát $\varphi = pq\neg\vee rpq\wedge\rightarrow\leftrightarrow$. Vše podstatné o výroku ve skutečnosti obsahuje jeho stromová struktura, která zachycuje, jak je sestaven z jednodušších výroků, obdobně jako strom aritmetického výrazu.

Příklad 2.1.4. Strom výroku $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$ je znázorněný na obrázku 2.1. Všimněte si také, že podvýroky φ odpovídají podstromům. Výrok φ získáme průchodem stromem od kořene, v každém vrcholu:

- pokud je label prvovýrok, vypíšeme ho
- pokud je label negace: vypíšeme '(¬', rekurzivně zavoláme syna, vypíšeme ')',
- jinak (pro binární logické spojky): vypíšeme '(', zavoláme levého syna, vypíšeme label, zavoláme pravého syna, vypíšeme ')'.[7]

Nyní si strom výroku definujeme formálně, *indukcí podle struktury výroku*:[8]

Definice 2.1.5 (Strom výroku)**.** *Strom výroku* φ, označme $\mathrm{Tree}(\varphi)$ je zakořeněný uspořádaný strom, definovaný induktivně takto:

- Je-li φ prvovýrok p, obsahuje $\mathrm{Tree}(\varphi)$ jediný vrchol, jeho label je p.
- Je-li φ tvaru $(\neg\varphi')$, má $\mathrm{Tree}(\varphi)$ kořen s labelem $\neg$, a jeho jediný syn je kořen $\mathrm{Tree}(\varphi')$.

[7] Prefixový a postfixový zápis bychom získali podobně, ale nevypisujeme závorky a label vypíšeme hned při vstupu resp. těsně před opuštěním vrcholu.

[8] Jakmile máme definovaný strom výroku, můžeme indukci podle struktury výroku chápat jako indukci podle hloubky stromu. Zatím tím ale chápejme indukci podle počtu kroků z definice 2.1.2, kterými výrok vznikl. Alternativně postačí indukce podle délky výroku, nebo podle počtu logických spojek.

- Je-li φ tvaru $(\varphi' \square \varphi'')$ pro $\square \in \{\wedge, \vee, \to, \leftrightarrow\}$, má $\mathrm{Tree}(\varphi)$ kořen s labelem $\square$ a dvěma syny: levý syn je kořen stromu $\mathrm{Tree}(\varphi')$, pravý je kořen $\mathrm{Tree}(\varphi'')$.

Cvičení 2.1. Dokažte, že každý výrok má jednoznačně určený strom výroku, a naopak.

2.1.4 Teorie

V praktických aplikacích nevyjádříme požadované vlastnosti jediným výrokem — to by musel být velmi dlouhý a složitý a špatně by se s ním pracovalo — ale mnoha jednoduššími výroky.

Definice 2.1.6 (Teorie)**.** *Teorie* v jazyce $\mathbb{P}$ je libovolná množina výroků v $\mathbb{P}$, tedy libovolná podmnožina $T \subseteq \mathrm{VF}_{\mathbb{P}}$. Jednotlivým výrokům $\varphi \in T$ říkáme také *axiomy*.

Konečné teorie by tedy bylo možné (byť ne praktické) nahradit jediným výrokem: konjunkcí všech jejich axiomů. Připouštíme ale i nekonečné teorie, triviálním příkladem je teorie $T = \mathrm{VF}_{\mathbb{P}}$, a prázdná teorie $T = \emptyset$.[9]

2.2 Sémantika výrokové logiky

V naší logice je sémantika daná jednou ze dvou možných hodnot: *pravda*, nebo *nepravda*. (V jiných logických systémech může být sémantika zajímavější, viz příloha C.)

2.2.1 Pravdivostní hodnota

Výrokům můžeme přiřadit jednu ze dvou možných pravdivostních hodnot: *pravdivý* (*True*, 1), nebo *lživý* (*False*, 0). Prvovýroky reprezentují jednoduchá, nadále nedělitelná tvrzení (proto jim také říkáme *atomické* výroky); pravdivostní hodnotu jim musíme přiřadit tak, aby odpovídala tomu, co chceme modelovat (proto jim říkáme *výrokové proměnné*). Jakmile ale *ohodnotíme* prvovýroky, pravdivostní hodnota libovolného složeného výroku je jednoznačně určená, a snadno ji spočteme podle stromu výroku:

Příklad 2.2.1. Spočtěme pravdivostní hodnotu výroku $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \to (p \wedge q)))$ při ohodnocení (a) $p = 0$, $q = 0$, $r = 0$, (b) $p = 1$, $q = 0$, $r = 1$. Postupujeme od listů směrem ke kořeni, podobně jako bychom vyhodnocovali např. aritmetický výraz. Výrok φ *platí* při ohodnocení z (a), *neplatí* při ohodnocení z (b). Viz obrázek 2.2.1.

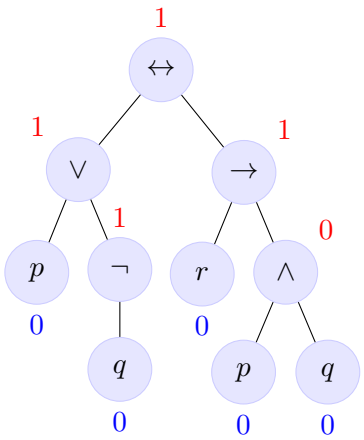
Logické spojky ve vnitřních vrcholech vyhodnocujeme podle jejich *pravdivostních tabulek*, viz tabulka 2.1.[10]

2.2.2 Výroky a booleovské funkce

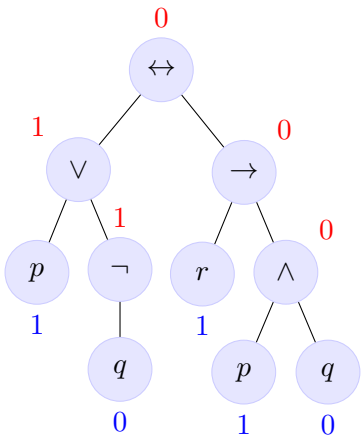
Abychom mohli formalizovat pravdivostní hodnotu výroku, podíváme se nejprve na souvislost výroků a booleovských funkcí.

Booleovská funkce je funkce $f\colon \{0,1\}^n \to \{0,1\}$, tedy vstupem je n-tice nul a jedniček, a výstupem 0 nebo 1. Každá logická spojka reprezentuje booleovskou funkci. V případě negace jde o unární funkci $f_\neg(x) = 1 - x$, ostatním logickým spojkám odpovídají binární funkce popsané v tabulce 2.2.

[9] Nekonečné teorie se hodí například pro popis vývoje nějakého systému v (diskrétním) čase $t = 0, 1, 2, \ldots$ Prázdná teorie se nehodí k ničemu, ale bylo by nešikovné formulovat věty o logice, pokud by teorie musely být



(a) $p = 0$, $q = 0$, $r = 0$



(b) $p = 1$, $q = 0$, $r = 1$

Obrázek 2.2: Pravdivostní ohodnocení výroku

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Tabulka 2.1: Pravdivostní tabulky logických spojek.

$f_\wedge(x,y)$:

	0	1
0	0	0
1	0	1

$f_\vee(x,y)$:

	0	1
0	0	1
1	1	1

$f_\to(x,y)$:

	0	1
0	1	1
1	0	1

$f_\leftrightarrow(x,y)$:

	0	1
0	1	0
1	0	1

Tabulka 2.2: Booleovské funkce logických spojek

Definice 2.2.2 (Pravdivostní funkce)**.** *Pravdivostní funkce* výroku φ v konečném jazyce $\mathbb{P}$ je funkce $f_{\varphi,\mathbb{P}}\colon \{0,1\}^{|\mathbb{P}|} \to \{0,1\}$ definovaná induktivně:

- je-li φ i-tý prvovýrok z $\mathbb{P}$, potom $f_{\varphi,\mathbb{P}}(x_0,\ldots,x_{n-1}) = x_i$,
- je-li $\varphi = (\neg\varphi')$, potom
$$f_{\varphi,\mathbb{P}}(x_0,\ldots,x_{n-1}) = f_{\neg}(f_{\varphi',\mathbb{P}}(x_0,\ldots,x_{n-1})),$$
- je-li $(\varphi' \square \varphi'')$ kde $\square \in \{\wedge,\vee,\to,\leftrightarrow\}$, potom
$$f_{\varphi,\mathbb{P}}(x_0,\ldots,x_{n-1}) = f_{\square}(f_{\varphi',\mathbb{P}}(x_0,\ldots,x_{n-1}), f_{\varphi'',\mathbb{P}}(x_0,\ldots,x_{n-1})).$$

Příklad 2.2.3. Spočtěme pravdivostní funkci výroku $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \to (p \wedge q)))$ v jazyce $\mathbb{P}' = \{p,q,r,s\}$:

$$f_{\varphi,\mathbb{P}'}(x_0,x_1,x_2,x_3) = f_{\leftrightarrow}(f_{\vee}(x_0, f_{\neg}(x_1)), f_{\to}(x_2, f_{\wedge}(x_0,x_1)))$$

Pravdivostní hodnotu výroku φ při ohodnocení $p=1$, $q=0$, $r=1$, $s=1$ spočteme takto (srovnejte s obrázkem 2.2.1(b)):

$$\begin{aligned} f_{\varphi,\mathbb{P}'}(1,0,1,1) &= f_{\leftrightarrow}(f_{\vee}(1, f_{\neg}(0)), f_{\to}(1, f_{\wedge}(1,0))) \\ &= f_{\leftrightarrow}(f_{\vee}(1,1), f_{\to}(1,0)) \\ &= f_{\leftrightarrow}(1,0) \\ &= 0 \end{aligned}$$

Pozorování 2.2.4. *Pravdivostní funkce výroku φ nad $\mathbb{P}$ závisí pouze na proměnných odpovídajících prvovýrokům z* $\mathrm{Var}(\varphi) \subseteq \mathbb{P}$.

Tedy i pokud máme výrok φ v *nekonečném* jazyce $\mathbb{P}$, můžeme se omezit na jazyk $\mathrm{Var}(\varphi)$ (který je konečný) a uvažovat pravdivostní funkci nad tímto jazykem.

2.2.3 Modely

Konkrétní pravdivostní ohodnocení výrokových proměnných představuje reprezentaci 'reálného světa' (systému) v námi zvoleném 'formálním světě', proto mu také říkáme *model*.

Definice 2.2.5 (Model jazyka)**.** *Model* jazyka $\mathbb{P}$ je libovolné pravdivostní ohodnocení $v\colon \mathbb{P} \to \{0,1\}$. *Množinu (všech) modelů jazyka* $\mathbb{P}$ označíme $\mathrm{M}_{\mathbb{P}}$:

$$\mathrm{M}_{\mathbb{P}} = \{v \mid v\colon \mathbb{P} \to \{0,1\}\} = \{0,1\}^{\mathbb{P}}$$

Modely budeme označovat písmeny v, u, w apod. (v od slova 'valuation'). Model jazyka je tedy funkce, formálně množina dvojic (vstup, výstup). Například pro jazyk $\mathbb{P} = \{p,q,r\}$ a pravdivostní ohodnocení ve kterém p je pravda, q nepravda, a r pravda máme model

$$v = \{(p,1),(q,0),(r,1)\}.$$

Pro jednoduchost ale budeme psát jen $v = (1,0,1)$. Pro jazyk $\mathbb{P} = \{p,q,r\}$ tedy máme $2^3 = 8$ modelů:

$$\mathrm{M}_{\mathbb{P}} = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

neprázdné.

[10] Připomeňme ještě jednou, že disjunkce není exkluzivní, tj. $p \vee q$ platí i pokud platí p i q, a že implikace je čistě logická, tj. $p \to q$ platí kdykoliv p neplatí.

Poznámka 2.2.6. Formálně vzato, ztotožňujeme množinu $\{0,1\}^{\mathbb{P}}$ s množinou $\{0,1\}^{|\mathbb{P}|}$ pomocí uspořádání ι jazyka $\mathbb{P}$ (viz Poznámka 2.1.1). Konkrétně, místo prvku $v = \{(p,1),(q,0),(r,1)\} \in \{0,1\}^{\mathbb{P}}$ píšeme $(1,0,1) = (v \circ \iota)(0,1,2) = (v(\iota(0)), v(\iota(1)), v(\iota(2))) \in \{0,1\}^{|\mathbb{P}|}$ (kde funkcím v, ι dovolíme působit 'po složkách').[11] Pokud by se to zdálo matoucí, představte si model v jako množinu prvovýroků, které jsou ohodnocené jako pravda, tj. $\{p,r\} \subseteq \mathbb{P}$, náš zápis $v = (1,0,1)$ je potom charakteristický vektor této množiny. Toto ztotožnění budeme nadále používat bez dalšího upozornění.

2.2.4 Platnost

Nyní můžeme definovat klíčový pojem logiky, *platnost* výroku v daném modelu. Neformálně, výrok platí v modelu (tj. při konkrétním pravdivostním ohodnocení prvovýroků), pokud jeho pravdivostní hodnota, tak jak jsme ji počítali v Příkladu 2.2.1, je rovna 1. Ve formální definici využijeme pravdivostní funkci výroku (Definice 2.2.2).[12]

Definice 2.2.7 (Platnost výroku v modelu, model výroku)**.** Mějme výrok φ v jazyce $\mathbb{P}$ a model $v \in \mathrm{M}_{\mathbb{P}}$. Pokud platí $f_{\varphi,\mathbb{P}}(v) = 1$, potom říkáme, že výrok φ *platí* v modelu v, v je *modelem* φ, a píšeme $v \models \varphi$. Množinu všech modelů výroku φ označujeme $\mathrm{M}_{\mathbb{P}}(\varphi)$.

Modelům jazyka, které nejsou modely φ, budeme někdy říkat *nemodely* φ. Tvoří doplněk množiny modelů φ. S pomocí zápisu pro inverzní relaci můžeme psát:

$$\mathrm{M}_{\mathbb{P}}(\varphi) = \{v \in \mathrm{M}_{\mathbb{P}} \mid v \models \varphi\} = f^{-1}_{\varphi,\mathbb{P}}[1]$$
$$\overline{\mathrm{M}_{\mathbb{P}}(\varphi)} = M_{\mathbb{P}} \setminus M_{\mathbb{P}}(\varphi) = \{v \in \mathrm{M}_{\mathbb{P}} \mid v \not\models \varphi\} = f^{-1}_{\varphi,\mathbb{P}}[0]$$

Je-li jazyk zřejmý z kontextu, můžeme psát jen $\mathrm{M}(\varphi)$. Musíme si ale být opravdu jistí: například v jazyce $\mathbb{P} = \{p,q\}$ máme

$$\mathrm{M}_{\{p,q\}}(p \to q) = \{(0,0),(0,1),(1,1)\},$$

zatímco v jazyce $\mathbb{P}' = \{p,q,r\}$ bychom měli

$$\mathrm{M}_{\mathbb{P}'}(p \to q) = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,1,0),(1,1,1)\}.$$

Definice 2.2.8 (Platnost teorie, model teorie)**.** Je-li T teorie v jazyce $\mathbb{P}$, potom T *platí* v modelu v, pokud každý axiom $\varphi \in T$ platí ve v. V tom případě říkáme také, že v je *modelem* T, a píšeme $T \models \varphi$. Množinu všech modelů teorie T v jazyce $\mathbb{P}$ označíme $\mathrm{M}_{\mathbb{P}}(T)$.

Pracujeme-li s konečnou teorií, nebo přidáváme-li k nějaké teorii konečně mnoho nových axiomů, budeme používat následující zjednodušený zápis:

- $\mathrm{M}_{\mathbb{P}}(\varphi_1, \varphi_2, \ldots, \varphi_n)$ místo $\mathrm{M}_{\mathbb{P}}(\{\varphi_1, \varphi_2, \ldots, \varphi_n\})$,
- $\mathrm{M}_{\mathbb{P}}(T, \varphi)$ místo $\mathrm{M}_{\mathbb{P}}(T \cup \{\varphi\})$.

Všimněte si, že $\mathrm{M}_{\mathbb{P}}(T,\varphi) = \mathrm{M}_{\mathbb{P}}(T) \cap \mathrm{M}_{\mathbb{P}}(\varphi)$, $\mathrm{M}_{\mathbb{P}}(T) = \bigcap_{\varphi \in T} \mathrm{M}_{\mathbb{P}}(\varphi)$, a že pro konečnou teorii (podobně i pro spočetnou) platí

$$\mathrm{M}_{\mathbb{P}}(\varphi_1) \supseteq \mathrm{M}_{\mathbb{P}}(\varphi_1,\varphi_2) \supseteq \mathrm{M}_{\mathbb{P}}(\varphi_1,\varphi_2,\varphi_3) \supseteq \cdots \supseteq \mathrm{M}_{\mathbb{P}}(\varphi_1,\varphi_2,\ldots,\varphi_n).$$

Toho můžeme využít při hledání modelů hrubou silou.

[11] Alternativně bychom mohli při formalizaci syntaxe vyžadovat (alespoň pro spočetné jazyky), aby jazyk *byl* $\mathbb{P} = \{0,1,2,\ldots\}$ a symboly p_0, p_1, p, q, r používat jen pro zvýšení čitelnosti.

[12] Pro *platnost* používáme symbol $\models$, který čteme jako 'splňuje' nebo 'modeluje', v LaTeXu \models.

Příklad 2.2.9. Modely teorie $T = \{p \vee q \vee r, q \to r, \neg r\}$ (v jazyce $\mathbb{P} = \{p, q, r\}$) můžeme najít tak, najdeme tak, že nejprve najdeme modely výroku $\neg r$:

$$\mathrm{M}_{\mathbb{P}}(r) = \{(x, y, 0) \mid x, y \in \{0, 1\}\} = \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 0)\},$$

poté určíme, ve který z těchto modelů platí výrok $q \to r$:

- $(0, 0, 0) \models q \to r$,
- $(0, 1, 0) \not\models q \to r$,
- $(1, 0, 0) \models q \to r$,
- $(1, 1, 0) \not\models q \to r$,

Tedy $\mathrm{M}_{\mathbb{P}}(r, q \to r) = \{(0, 0, 0), (1, 0, 0)\}$. Výrok $p \vee q \vee r$ platí jen v prvním z těchto modelů, dostáváme tedy

$$\mathrm{M}_{\mathbb{P}}(r, q \to r, p \vee q \vee r) = \mathrm{M}_{\mathbb{P}}(T) = \{(1, 0, 0)\}.$$

Tento postup je efektivnější než určit množiny modelů jednotlivých axiomů a udělat jejich průnik. (Ale mnohem méně efektivní než postup založený na tablo metodě, který si ukážeme později.)

2.2.5 Další sémantické pojmy

V návaznosti na pojem platnosti budeme používat řadu dalších pojmů. Pro některé vlastnosti existuje více různých termínů, v závislosti na kontextu v jakém se vyskytnou.

Definice 2.2.10 (Sémantické pojmy)**.** Říkáme, že výrok φ (v jazyce $\mathbb{P}$) je

- *pravdivý*, *tautologie*, *platí (v logice/logicky)*, a píšeme $\models \varphi$, pokud platí v každém modelu (jazyka $\mathbb{P}$), $\mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}$,
- *lživý*, *sporný*, pokud nemá žádný model, $\mathrm{M}_{\mathbb{P}}(\varphi) = \emptyset$.[13]
- *nezávislý*, pokud platí v nějakém modelu, a neplatí v nějakém jiném modelu, tj. není pravdivý ani lživý, $\emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(\varphi) \subsetneq \mathrm{M}_{\mathbb{P}}$,
- *splnitelný*, pokud má nějaký model, tj. není lživý, $\mathrm{M}_{\mathbb{P}}(\varphi) \neq \emptyset$.

Dále říkáme, že výroky φ, ψ (ve stejném jazyce $\mathbb{P}$) jsou *(logicky) ekvivalentní*, píšeme $\varphi \sim \psi$ pokud mají stejné modely, tj.

$$\varphi \sim \psi \text{ právě když } \mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}(\psi).$$

Příklad 2.2.11. Například platí následující:

- výroky $\top$, $p \vee q \leftrightarrow q \vee p$ jsou pravdivé,
- výroky $\bot$, $(p \vee q) \wedge (p \vee \neg q) \wedge \neg p$ jsou lživé,
- výroky $p, p \wedge q$ jsou nezávislé, a také splnitelné, a

[13] Všimněte si, že být *lživý* není totéž, co nebýt *pravdivý*!

- následující výroky jsou ekvivalentní:
  - $p \sim p \vee p \sim p \vee p \vee p$,
  - $p \to q \sim \neg p \vee q$,
  - $\neg p \to (p \to q) \sim \top$.

Pojmy z Definice 2.2.10 můžeme také relativizovat vzhledem k dané teorii. To znamená, že se v jednotlivých definicích omezíme na modely této teorie:

Definice 2.2.12 (Sémantické pojmy vzhledem k teorii)**.** Mějme teorii T v jazyce $\mathbb{P}$. Říkáme, že výrok φ v jazyce $\mathbb{P}$ je

- *pravdivý v T*, *důsledek T*, *platí v T*, a píšeme $T \models \varphi$, pokud φ platí v každém modelu teorie T, neboli $\mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)$,
- *lživý v T*, *sporný v T*, pokud neplatí v žádném modelu T, neboli $\mathrm{M}_{\mathbb{P}}(\varphi) \cap \mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}(T, \varphi) = \emptyset$.
- *nezávislý v T*, pokud platí v nějakém modelu T, a neplatí v nějakém jiném modelu T, tj. není pravdivý v T ani lživý v T, $\emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(T, \varphi) \subsetneq \mathrm{M}_{\mathbb{P}}(T)$,
- *splnitelný v T*, *konzistentní s T*, pokud platí v nějakém modelu T, tj. není lživý v T, $\mathrm{M}_{\mathbb{P}}(T, \varphi) \neq \emptyset$.

A říkáme, že výroky φ, ψ (ve stejném jazyce $\mathbb{P}$) jsou *ekvivalentní v T*, *T-ekvivalentní*, píšeme $\varphi \sim_T \psi$ pokud platí v týchž modelech T, tj.

$$\varphi \sim_T \psi \text{ právě když } \mathrm{M}_{\mathbb{P}}(T, \varphi) = \mathrm{M}_{\mathbb{P}}(T, \psi).$$

Všimněte si, že pro prázdnou teorii $T = \emptyset$ platí $\mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}$ a výše uvedené pojmy pro T se proto shodují s původními. Opět si pojmy ilustrujeme na několika příkladech:

Příklad 2.2.13. Mějme teorii $T = \{p \vee q, \neg r\}$. Platí následující:

- výroky $q \vee p$, $\neg p \vee \neg q \vee \neg r$ jsou v T jsou pravdivé,
- výrok $\neg p \vee \neg q \vee r$ je v T lživý,
- výroky $p \leftrightarrow q, p \wedge q$ jsou v T nezávislé, a také splnitelné, a
- platí $p \vee r \sim_T q \vee r$ (ale $p \vee r \not\sim q \vee r$).

2.2.6 Univerzálnost logických spojek

V jazyce výrokové logiky používáme následující logické spojky: $\neg, \wedge, \vee, \to, \leftrightarrow$. To ale není jediná možná volba, k vybudování plnohodnotné logiky by nám stačila například negace a implikace,[14] nebo negace, konjunkce, a disjunkce.[15] A jak uvidíme níže, mohli bychom použít i jiné logické spojky. Naše volba je zlatou střední cestou mezi bohatostí vyjadřování na jedné straně, a úsporností syntaktických pravidel na straně druhé.

[14] Negaci potřebujeme k popisu stavu systému, a implikaci k popisu chování v čase.
[15] Ty stačí k vybudování logických obvodů.

Co myslíme tím, že je logika plnohodnotná? Řekneme, že množina logických spojek S je *univerzální*, pokud lze každou booleovskou funkci f vyjádřit jako pravdivostní funkci $f_{\varphi,\mathbb{P}}$ nějakého výroku φ vybudovaného z logických spojek z S (kde $|\mathbb{P}| = n$ je-li f n-ární funkce). Ekvivalentně, pro každý konečný jazyk $\mathbb{P}$ (řekněme, že n-prvkový) a každou množinu modelů $M \subseteq \mathrm{M}_{\mathbb{P}}$ musí existovat výrok φ takový, že $\mathrm{M}_{\mathbb{P}}(\varphi) = M$. (Ekvivalence těchto dvou vyjádření plyne z toho, že máme-li booleovskou funkci f a zvolíme-li $M = f^{-1}[1]$, potom $f_{\varphi,\mathbb{P}} = f$ právě když $\mathrm{M}_{\mathbb{P}}(\varphi) = M$.)

Tvrzení 2.2.14. *Množiny logických spojek* $\{\neg, \wedge, \vee\}$ *a* $\{\neg, \to\}$ *jsou univerzální.*

Důkaz. Mějme funkci $f\colon \{0,1\}^n \to \{0,1\}$, resp. množinu modelů $M = f^{-1}[1] \subseteq \{0,1\}^n$. Náš jazyk bude $\mathbb{P} = \{p_1, \ldots, p_n\}$. Pokud by množina M obsahovala jediný model, např. $v = (1,0,1,0)$ mohli bychom ji reprezentovat výrokem $\varphi_v = p_1 \wedge \neg p_2 \wedge p_3 \wedge \neg p_4$, který říká 'musím být model v'. Pro obecný model v bychom výrok φ_v zapsali takto:

$$\varphi_v = p_1^{v_1} \wedge p_2^{v_2} \wedge \cdots \wedge p_n^{v_n} = \bigwedge_{i=1}^{n} p_i^{v(p_i)} = \bigwedge_{p\in\mathbb{P}} p^{v(p)}$$

kde zavádíme následující užitečné značení: $p^{v(p)}$ je výrok p pokud $v(p) = 1$, a výrok $\neg p$ pokud $v(p) = 0$.

Obsahuje-li množina M více modelů, řekneme 'musím být alespoň jeden z modelů z M':

$$\varphi_M = \bigvee_{v\in M} \varphi_v = \bigvee_{v\in M} \bigwedge_{p\in\mathbb{P}} p^{v(p)}$$

Zřejmě platí $M_{\mathbb{P}}(\varphi_M) = M$ neboli $f_{\varphi_M,\mathbb{P}} = f$. (Pokud $M = \emptyset$, potom z definice $\bigvee_{v\in M} \varphi_v = \bot$.)[16]

Univerzálnost $\{\neg, \to\}$ plyne z univerzálnosti $\{\neg, \wedge, \vee\}$ a faktu, že konjunkci a disjunkci můžeme vyjádřit pomocí negace a implikace: $p \wedge q \sim \neg(p \to \neg q)$ a $p \vee q \sim \neg p \to q$. □

Poznámka 2.2.15. Všimněte si, že při konstrukci výroku φ_M je klíčové, že množina M je konečná (má nejvýše 2^n prvků). Kdyby byla nekonečná, symbol '$\bigvee_{v\in M}$' by znamenal 'disjunkci' nekonečně mnoha výroků, a výsledkem by tedy nebyl konečný nápis, tj. 'φ_M' by vůbec nebyl výrok. (Máme-li spočetně nekonečný jazyk $\mathbb{P}'$, potom ne každou podmnožinu $M \subseteq \mathrm{M}_{\mathbb{P}'}$ lze reprezentovat výrokem—takových podmnožin je nespočetně mnoho, zatímco výroků je jen spočetně mnoho.)

Jaké další logické spojky bychom mohli použít? Nulární booleovské funkce,[17] neboli konstanty 0, 1, bychom mohli zavést jako symboly TRUE a FALSE, my si ale vystačíme s výroky $\top, \bot$. Unární booleovské funkce jsou čtyři ($4 = 2^{2^1}$), ale negace je jediná 'zajímavá': ostatní jsou $f(x) = x$, $f(x) = 0$, a $f(x) = 1$. Zajímavých binárních logických spojek už je více, v přírodě se vyskytují například tyto:

- NAND neboli *Shefferova spojka*, někdy se používá symbol $p \uparrow q$, platí $p \uparrow q \sim \neg(p \wedge q)$,
- NOR neboli *Pierceova spojka*, někdy se používá symbol $p \downarrow q$, platí $p \downarrow q \sim \neg(p \vee q)$,

[16] Podobně jako součet prázdné množiny sčítanců je roven 0.

[17] Ve formalizaci matematiky resp. informatiky funkce arity 0 znamená, že nemá žádné vstupy, výstup tedy nemůže záviset na vstupu a je konstantní. Formálně, jde o funkce $f\colon \emptyset \to \{0,1\}$. Pokud je to matoucí, představte si, že funkce musí mít aritu alespoň 1, a místo 'nulární funkce' říkejme 'konstanta'.

- XOR, neboli *exclusive-OR*, někdy se píše také $\oplus$, platí $p \oplus q \sim (p \vee q) \wedge \neg(p \wedge q)$, neboli součet pravdivostní hodnot modulo 2.

Cvičení 2.2. Vyjádřete $(p \oplus q) \oplus r$ pomocí $\{\neg, \wedge, \vee\}$.

Cvičení 2.3. Ukažte, že {NAND} a také {NOR} jsou univerzální.

Cvičení 2.4. Uvažme ternární logickou spojku IFTE, kde $IFTE(p, q, r)$ je splněno, právě když platí 'if p then q else r'. Určete pravdivostní tabulku této logické spojky (tj. funkci f_{IFTE}) a ukažte, že $\{\text{TRUE}, \text{FALSE}, \text{IFTE}\}$ je univerzální.

2.3 Normální formy

Připomeňme, že výroky jsou ekvivalentní, pokud mají stejnou množinu modelů. Pro každý výrok existuje nekonečně mnoho ekvivalentních výroků; často se hodí vyjádřit výrok v nějakém 'hezkém' (užitečném) 'tvaru', tj. najít ekvivalentní výrok v daném tvaru. Takovému konceptu tvaru se v matematice říká *normální forma*. My si představíme dvě nejznámější: *konjunktivní normální formu (conjunctive normal form, CNF)* a *disjunktivní normální formu (DNF)*.

Používá se následující terminologie a značení:

- *Literál* ℓ je buď prvovýrok p nebo negace prvovýroku $\neg p$. Pro prvovýrok p označme $p^0 = \neg p$ a $p^1 = p$. Je-li ℓ literál, potom $\bar{\ell}$ označuje *opačný literál* k ℓ. Je-li $\ell = p$ (*pozitivní literál*), potom $\bar{\ell} = \neg p$, je-li $\ell = \neg p$ (*negativní literál*), potom $\bar{\ell} = p$
- *Klauzule (clause)* je disjunkce literálů $C = \ell_1 \vee \ell_2 \vee \cdots \vee \ell_n$. *Jednotková klauzule (unit clause)* je samotný literál ($n = 1$) a *prázdnou klauzulí* ($n = 0$) myslíme $\bot$.
- Výrok je *v konjunktivní normální formě (v CNF)* pokud je konjunkcí klauzulí. *Prázdný výrok v CNF* je $\top$.
- *Elementární konjunkce* je konjunkce literálů $E = \ell_1 \wedge \ell_2 \wedge \cdots \wedge \ell_n$. *Jednotková elementární klauzule* je samotný literál ($n = 1$). *Prázdná elementární konjunkce* ($n = 0$) je $\top$.
- Výrok je *v disjunktivní normální formě (v DNF)* pokud je disjunkcí elementárních konjunkcí. *Prázdný výrok v DNF* je $\bot$.

Příklad 2.3.1. Výrok $p \vee q \vee \neg r$ je v CNF (je to jediná klauzule) a zároveň v DNF (je to disjunkce jednotkových elementárních konjunkcí). Výrok $(p \vee q) \wedge (p \vee \neg q) \wedge \neg p$ je v CNF, výrok $\neg p \vee (p \wedge q)$ je v DNF.

Příklad 2.3.2. Výrok φ_v z důkazu Tvrzení 2.2.14 je v CNF (je to konjunkce jednotkových klauzulí, tj. literálů) a také v DNF (je to jediná elementární konjunkce). Výrok φ_M je v DNF.

Pozorování 2.3.3. *Všimněte si, že výrok v CNF je pravdivý, právě když každá jeho klauzule obsahuje dvojici opačných literálů. Podobně, výrok v DNF je splnitelný, pokud ne každá elementární konjunkce obsahuje dvojici opačných literálů.*

2.3.1 O dualitě

Všimněte si, že pokud ve výrokové logice zaměníme hodnoty pro pravdu a nepravdu, tj. 0 a 1, pravdivostní tabulka negace zůstává stejná, z konjunkce se stává disjunkce, a naopak. Tomuto konceptu se říká *dualita*; v logice uvidíme mnoho příkladů.

Platí $\neg(p \wedge q) \sim (\neg p \vee \neg q)$ a *z duality* víme také $\neg(\neg p \vee \neg q) \sim (\neg\neg p \wedge \neg\neg q)$, z čehož snadno odvodíme $\neg(p \vee q) \sim (\neg p \wedge \neg q)$.[18] Obecněji, n-ární booleovské funkce f, g jsou navzájem *duální*, pokud platí pokud $f(\neg x) = \neg g(x)$. Máme-li výrok φ vybudovaný z $\{\neg, \wedge, \vee\}$ a zaměníme-li v něm $\wedge$ a $\vee$, a znegujeme-li výrokové proměnné (resp. zaměníme-li literály za opačné literály), dostáváme výrok $\psi \sim \neg\varphi$ (tj. modely φ jsou nemodely ψ a naopak), a funkce $f_{\varphi,\mathbb{P}}, f_{\psi,\mathbb{P}}$ jsou navzájem duální.

Pojem DNF je duální k pojmu CNF, 'je pravdivý' je duální k 'není splnitelný', předchozí pozorování tedy můžeme chápat jako příklad duality. Ke každému tvrzení ve výrokové logice získáváme 'zdarma' tvrzení *duální*, vzniklé záměnou $\wedge$ and $\vee$, pravdy a nepravdy.

2.3.2 Převod do normální formy

Disjunktivní normální formu jsme již potkali, v důkazu Tvrzení 2.2.14. Klíčovou část důkazu bychom mohli zformulovat takto: 'Je-li jazyk konečný, lze každou množinu modelů *axiomatizovat* výrokem v DNF'. Z duality dostáváme také axiomatizaci v CNF, neboť doplněk množiny modelů je také množina modelů:

Tvrzení 2.3.4. *Mějme konečný jazyk $\mathbb{P}$ a libovolnou množinu modelů $M \subseteq \mathrm{M}_{\mathbb{P}}$. Potom existuje výrok φ_{DNF} v DNF a výrok φ_{CNF} v CNF takový, že $M = \mathrm{M}_{\mathbb{P}}(\varphi_{\mathrm{DNF}}) = \mathrm{M}_{\mathbb{P}}(\varphi_{\mathrm{CNF}})$. Konkrétně:*

$$\varphi_{\mathrm{DNF}} = \bigvee_{v \in M} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$
$$\varphi_{\mathrm{CNF}} = \bigwedge_{v \in \overline{M}} \bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}} = \bigwedge_{v \notin M} \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$$

Důkaz. Pro výrok φ_{DNF} viz důkaz Tvrzení 2.2.14, každá elementární konjunkce popisuje jeden model. Výrok φ_{CNF} je duální k výroku φ'_{DNF} sestrojenému pro doplněk $M' = \overline{M}$. Nebo můžeme dokázat přímo: modely klauzule $C_v = \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$ jsou všechny modely kromě v, $\mathrm{M}_C = \mathrm{M}_P \setminus \{v\}$, tedy každá klauzule v konjunkci zakazuje jeden nemodel. □

Tvrzení 2.3.4 dává návod, jak převádět výrok do disjunktivní nebo do konjunktivní normální formy:

Příklad 2.3.5. Uvažme výrok $\varphi = p \leftrightarrow (q \vee \neg r)$. Nejprve najdeme množinu modelů: $M = \mathrm{M}_\varphi = \{(0,0,1), (1,0,0), (1,1,0), (1,1,1)\}$. Nyní najdeme výroky $\varphi_{\mathrm{DNF}}, \varphi_{\mathrm{CNF}}$ podle Tvrzení 2.3.4, ty mají stejnou množinu modelů jako φ, jsou tedy ekvivalentní.

Výrok φ_{DNF} najdeme tak, že pro každý model sestrojíme elementární konjunkci vynucující právě tento model:

$$\varphi_{\mathrm{DNF}} = (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$$

Při konstrukci φ_{CNF} budeme potřebovat *nemodely* φ, $\overline{M} = \{(0,0,0), (0,1,0), (0,1,1), (1,0,1)\}$. Každá klauzule zakáže jeden nemodel:

$$\varphi_{\mathrm{CNF}} = (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r)$$

[18] Neboť p, q jsou proměnné, mohou za ně být dosazeny obě hodnoty 0 i 1, tedy je můžeme zaměnit za k nim opačné literály.

Důsledek 2.3.6. *Každý výrok (v libovolném, i nekonečném jazyce $\mathbb{P}$) je ekvivalentní nějakému výroku v CNF a nějakému výroku v DNF.*

Důkaz. I když je jazyk $\mathbb{P}$ nekonečný, výrok φ obsahuje jen konečně mnoho výrokových proměnných, můžeme tedy použít Tvrzení 2.3.4 pro jazyk $\mathbb{P}' = \mathrm{Var}(\varphi)$, a množinu modelů $M = \mathrm{M}_{\mathbb{P}'}(\varphi)$. Protože $M = \mathrm{M}_{\mathbb{P}'}(\varphi_{\mathrm{DNF}}) = \mathrm{M}_{\mathbb{P}'}(\varphi_{\mathrm{CNF}}) = M$, máme $\varphi \sim \varphi_{\mathrm{DNF}} \sim \varphi_{\mathrm{CNF}}$. □

Cvičení 2.5. Rozmyslete si, jak lze z DNF výroku snadno vygenerovat jeho modely, a z CNF výroku jeho nemodely.

Poznámka 2.3.7. Kdy lze axiomatizovat *teorii* výrokem v DNF nebo výrokem v CNF? Mějme jazyk $\mathbb{P}' = \mathrm{Var}(T)$ (tj. všechny výrokové proměnné vyskytující se v axiomech T). Má-li T v jazyce $\mathbb{P}'$ konečně mnoho modelů (tj. je-li $\mathrm{M}_{\mathbb{P}'}(T)$ konečná), můžeme sestrojit výrok v DNF, a má-li konečně mnoho *nemodelů*, můžeme sestrojit výrok v CNF. Obecně ale ne každou teorii lze axiomatizovat *jediným* výrokem v CNF nebo v DNF. Vždy můžeme převést jednotlivé axiomy do CNF (nebo DNF), a můžeme také axiomatizovat teorii jen pomocí (potenciálně nekonečně mnoha) klauzulí.

Tento způsob převodu do CNF resp. do DNF vyžaduje znalost množiny modelů výroku, je tedy poměrně neefektivní. A také výsledná normální forma může být velmi dlouhá. Ukážeme si ještě jeden postup.

Převod pomocí ekvivalentních úprav

Využijeme následujícího pozorování: Nahradíme-li nějaký podvýrok ψ výroku φ ekvivalentním výrokem ψ', výsledný výrok φ' bude také ekvivalentní φ. Nejprve si ukážeme postup na příkladě:

Příklad 2.3.8. Převedeme opět výrok $\varphi = p \leftrightarrow (q \vee \neg r)$. Nejprve se zbavíme ekvivalence, vyjádříme ji jako konjunkci dvou implikací. V dalším kroku odstraníme implikace, pomocí pravidla $\varphi \to \psi \sim \neg\varphi \vee \psi$:

$$\begin{aligned} p \leftrightarrow (q \vee \neg r) &\sim (p \to (q \vee \neg r)) \wedge ((q \vee \neg r) \to p) \\ &\sim (\neg p \vee q \vee \neg r) \wedge (\neg(q \vee \neg r) \vee p) \end{aligned}$$

Nyní si představme strom výroku, v dalším kroku chceme dostat negace na co nejnižší úroveň stromu, bezprostředně nad listy: využijeme toho, že $\neg(q \vee \neg r) \sim \neg q \wedge \neg\neg r$ a zbavíme se dvojité negace $\neg\neg r \sim r$. Dostáváme výrok

$$(\neg p \vee q \vee \neg r) \wedge ((\neg q \wedge r) \vee p)$$

Nyní již necháme literály nedotčené, a použijeme distributivitu $\wedge$ vůči $\vee$, nebo naopak, podle toho, zda chceme DNF nebo CNF. Pro převod do CNF použijeme úpravu $(\neg q \wedge r) \vee p \sim (\neg q \vee p) \wedge (r \vee p)$, kterou jsme dostali symbol $\vee$ na nižší úroveň stromu. (Nakreslete si!) Tím už dostáváme výrok v CNF, pro přehlednost ještě seřadíme literály v klauzulích:

$$(\neg p \vee q \vee \neg r) \wedge (p \vee \neg q) \wedge (p \vee r)$$

Při převodu do DNF bychom postupovali obdobně, opakovanou aplikací distributivity. Zde vyjdeme v CNF formy a zkombinujeme každý literál z první klauzule s každým literálem z druhé a s každým literálem z třetí klauzule. Všimneme si, že stejný literál nemusíme v elementární konjunkci opakovat dvakrát, a že obsahuje-li elementární klauzule dvojici opačných

literálů, je sporná, a můžeme ji tedy v DNF vynechat. Také můžeme vynechat elementární konjunkci E', pokud máme jinou elementární konjunkci E takovou, že E' obsahuje všechny literály obsažené v E, např. $E = p \wedge \neg r$ a $E' = (p \wedge q \wedge \neg r)$. (Rozmyslete si proč, a zformulujte duální zjednodušení při převodu do CNF.) Výsledný výrok v DNF je:

$$(\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r) \vee (p \wedge \neg r)$$

Nyní vypíšeme všechny potřebné ekvivalentní úpravy. Důkaz, že každý výrok lze převést do DNF a do CNF lze snadno provést indukcí podle struktury výroku (podle hloubky stromu výroku).

- Implikace a ekvivalence:

  $$\varphi \to \psi \sim \neg\varphi \vee \psi$$
  $$\varphi \leftrightarrow \psi \sim (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$$

- Negace:

  $$\neg(\varphi \wedge \psi) \sim \neg\varphi \vee \neg\psi$$
  $$\neg(\varphi \vee \psi) \sim \neg\varphi \wedge \neg\psi$$
  $$\neg\neg\varphi \sim \varphi$$

- Konjunkce (převod do DNF):

  $$\varphi \wedge (\psi \wedge \chi) \sim (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$$
  $$(\varphi \wedge \psi) \wedge \chi \sim (\varphi \wedge \chi) \vee (\psi \wedge \chi)$$

- Disjunkce (převod do CNF):

  $$\varphi \vee (\psi \vee \chi) \sim (\varphi \vee \psi) \wedge (\varphi \vee \chi)$$
  $$(\varphi \vee \psi) \vee \chi \sim (\varphi \vee \chi) \wedge (\psi \vee \chi)$$

Jak uvidíme v příští kapitole, CNF je v praxi mnohem důležitější než DNF (byť jde o duální pojmy). Při popisu reálného systému je přirozenější vyjádření pomocí konjunkce mnoha jednodušších vlastností, než jako jednu velmi dlouhou disjunkci. Existuje mnoho dalších forem reprezentace booleovských funkcí. Podobně jako datové struktury, vhodnou formu reprezentace volíme podle toho, jaké operace potřebujeme s funkcí dělat.[19]

2.4 Vlastnosti a důsledky teorií

Podívejme se nyní hlouběji na vlastnosti teorií. Podobně jako pro výroky řekneme, že dvě teorie T, T' v jazyce $\mathbb{P}$ jsou *ekvivalentní*, pokud mají stejnou množinu modelů:

$$T \sim T' \text{ právě když } \mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}(T')$$

Jde tedy o teorie vyjadřující tytéž vlastnosti, jen jinak vyjádřené (*axiomatizované*). Zajímat nás budou vlastnosti nezávislé na konkrétní *axiomatizaci*.

Příklad 2.4.1. Například teorie $T = \{p \to q, p \leftrightarrow r\}$ je ekvivalentní teorii $T' = \{(\neg p \vee q) \wedge (\neg p \vee r) \wedge (p \vee \neg r)\}$.

Definice 2.4.2 (Vlastnosti teorií)**.** Řekneme, že teorie T v jazyce $\mathbb{P}$ je

- *sporná*, jestliže v ní platí $\bot$ (spor), ekvivalentně, jestliže nemá žádný model, ekvivalentně, jestliže v ní platí všechny výroky,
- *bezesporná* (*splnitelná*), pokud není sporná, tj. má nějaký model,

[19] Viz například přednáška NAIL031 Reprezentace booleovských funkcí.

- *kompletní*, jestliže není sporná a každý výrok je v ní pravdivý nebo lživý (tj. nemá žádné nezávislé výroky), ekvivalentně, pokud má právě jeden model.

Rozmysleme si, proč platí ekvivalence vlastností v definici. Uvědomme si, že ve sporné teorii platí skutečně platí všechny výroky! Vskutku, výrok platí v T, pokud platí v každém modelu T, ty ale žádné nejsou. Naopak, pokud teorie má alespoň jeden model, v tomto modelu nemůže platit $\bot = p \wedge \neg p$.

A je-li teorie kompletní, nemůže mít dva různé modely $v \neq v'$. Výrok $\varphi_v = \bigwedge_{p \in \mathbb{P}} p^{v(p)}$ (který jsme potkali v důkazu Tvrzení 2.2.14) by totiž byl nezávislý v T, protože platí v modelu v ale ne v modelu v'. Naopak, má-li T jediný model v, potom každý výrok buď platí ve v, a tedy platí v T, nebo neplatí ve v a potom je lživý v T.

Příklad 2.4.3. Příkladem sporné teorie je třeba $T = \{p, p \to q, \neg q\}$. Teorie $T = \{p \vee q, r\}$ je bezesporná, ale není kompletní, například výrok $p \wedge q$ v ní není pravdivý (neplatí v modelu $(1, 0, 1)$) ale ani lživý (platí v modelu $(1, 1, 1)$). Teorie $T \cup \{\neg p\}$ je kompletní, jejím jediným modelem je $(0, 1, 1)$.

2.4.1 Důsledky teorií

Připomeňme, že důsledek teorie T je každý výrok, který v T platí (tj. platí v každém modelu T) a označme si *množinu všech důsledků* teorie T v jazyce $\mathbb{P}$ jako

$$\mathrm{Csq}_{\mathbb{P}}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}} \mid T \models \varphi\}$$

Pokud je teorie T v jazyce $\mathbb{P}$, můžeme psát:

$$\mathrm{Csq}_{\mathbb{P}}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}} \mid \mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)\}$$

(Dává ale smysl mluvit i o důsledcích teorie v nějakém menším jazyce, který je podmnožinou jazyka T).

Ukážeme si několik jednoduchých vlastností důsledků:

Tvrzení 2.4.4. *Mějme teorie T, T' a výroky $\varphi, \varphi_1, \ldots, \varphi_n$ v jazyce $\mathbb{P}$. Potom platí:*

(i) $T \subseteq \mathrm{Csq}_{\mathbb{P}}(T)$,

(ii) $\mathrm{Csq}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(\mathrm{Csq}_{\mathbb{P}}(T))$,

(iii) pokud $T \subseteq T'$, *potom* $\mathrm{Csq}_{\mathbb{P}}(T) \subseteq \mathrm{Csq}_{\mathbb{P}}(T')$,

(iv) $\varphi \in \mathrm{Csq}_{\mathbb{P}}(\{\varphi_1, \ldots, \varphi_n\})$ *právě když je výrok* $(\varphi_1 \wedge \cdots \wedge \varphi_n) \to \varphi$ *tautologie.*

Důkaz. Důkaz je snadný, použijeme-li, že φ je důsledek T právě když $\mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)$, a uvědomíme-li si následující vztahy:

- $\mathrm{M}(\mathrm{Csq}(T)) = \mathrm{M}(T)$,
- je-li $T \subseteq T'$ potom $\mathrm{M}(T) \supseteq \mathrm{M}(T')$,[20]
- $\psi \to \varphi$ je tautologie, právě když platí $\mathrm{M}(\psi) \subseteq \mathrm{M}(\varphi)$,
- $\mathrm{M}(\varphi_1 \wedge \cdots \wedge \varphi_n) = \mathrm{M}(\varphi_1, \ldots, \varphi_n)$.

□

Cvičení 2.6. Dokažte podrobně Tvrzení 2.4.4.

[20] Čím více vlastností předepíšeme, tím méně objektů je bude všechny splňovat.

2.4.2 Extenze teorií

Neformálně řečeno, rozšířením, neboli *extenzí* teorie T myslíme jakoukoliv teorii T', která splňuje vše, co platí v teorii T (a něco navíc, nejde-li o triviální případ). Modeluje-li T nějaký systém, lze ji rozšířit dvěma způsoby: přidáním dodatečných požadavků o systému (tomu budeme říkat *jednoduchá extenze*) nebo i rozšířením systému o nějaké nové části. Pokud ve druhém případě nemáme dodatečné požadavky na původní část systému, tedy platí-li o původní části totéž, co předtím, říkáme, že je extenze *konzervativní*.

Příklad 2.4.5. Vraťme se k úvodnímu příkladu o barvení grafů, Příklad 1.1.2. Teorie T_3 (úplná obarvení grafu zachovávající hranovou podmínku) je jednoduchou extenzí teorie T_1 (částečná obarvení množiny vrcholů bez ohledu na hrany). Teorie T_3' z Sekce 1.2.1 (přidání nového vrcholu do grafu) je konzervativní, ale ne jednoduchou extenzí T_3. A jde o extenzi T_1, která není ani jednoduchá ani konzervativní.

Uveďme nyní konečně formální definice:

Definice 2.4.6 (Extenze teorie)**.** Mějme teorii T v jazyce $\mathbb{P}$.

- *Extenze* teorie T je libovolná teorie T' v jazyce $\mathbb{P}' \supseteq \mathbb{P}$ splňující $\mathrm{Csq}_{\mathbb{P}}(T) \subseteq \mathrm{Csq}_{\mathbb{P}'}(T')$,
- je to *jednoduchá extenze*, pokud $\mathbb{P}' = \mathbb{P}$,
- je to *konzervativní extenze*, pokud $\mathrm{Csq}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(T') = \mathrm{Csq}_{\mathbb{P}'}(T') \cap \mathrm{VF}_{\mathbb{P}}$.

Extenze tedy znamená, že splňuje všechny důsledky původní teorie. Extenze je jednoduchá, pokud do jazyka nepřidáváme žádné nové výrokové proměnné, a konzervativní, pokud neměníme platnost tvrzení vyjádřitelných v původním jazyce, každý nový důsledek tedy musí obsahovat nějakou nově přidanou výrokovou proměnnou.

Co tyto pojmy znamenají *sémanticky*, v řeči modelů? Zformulujme nejprve obecné pozorování, které ihned poté ilustrujeme na příkladě:

Pozorování 2.4.7. *Je-li T teorie v jazyce $\mathbb{P}$ a T' teorie v jazyce $\mathbb{P}'$ obsahujícím jazyk P. Potom platí:*

- *T' je jednoduchou extenzí T, právě když $\mathbb{P}' = \mathbb{P}$ a $\mathrm{M}_{\mathbb{P}}(T') \subseteq \mathrm{M}_{\mathbb{P}}(T)$,*
- *T' je extenzí T, právě když $\mathrm{M}_{\mathbb{P}'}(T') \subseteq \mathrm{M}_{\mathbb{P}'}(T)$. Uvažujeme tedy modely teorie T nad rozšířeným jazykem $\mathbb{P}'$.*[21] *Jinými slovy,* restrikce[22] *libovolného modelu $v \in \mathrm{M}_{\mathbb{P}'}(T')$ na původní jazyk $\mathbb{P}$ musí být modelem T, mohli bychom psát $v\restriction_{\mathbb{P}} \in \mathrm{M}_{\mathbb{P}}(T)$ nebo:*

$$\{v\restriction_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} \subseteq \mathrm{M}_{\mathbb{P}}(T)$$

- *T' je konzervativní extenzí T, pokud je extenzí a navíc platí, že každý model T (v jazyce $\mathbb{P}$) lze nějak* expandovat *(rozšířit)*[23] *na model T' (v jazyce $\mathbb{P}'$), neboli* každý *model T (v jazyce $\mathbb{P}$) získáme restrikcí* nějakého *modelu T' na jazyk $\mathbb{P}$. Mohli bychom psát:*

$$\{v\restriction_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} = \mathrm{M}_{\mathbb{P}}(T)$$

[21] Pozor, nemůžeme psát $\mathrm{M}_{\mathbb{P}}(T')$, protože modely T' musí být ohodnoceními většího jazyka $\mathbb{P}'$, hodnoty jen pro proměnné z $\mathbb{P}$ nestačí k určení pravdivostní hodnoty. A nelze psát ani $\mathrm{M}_{\mathbb{P}'}(T') \subseteq \mathrm{M}_{\mathbb{P}}(T)$, jde o množiny vektorů jiné dimenze.

[22] *Restrikce* znamená zapomenutí hodnot pro nové výrokové proměnné, resp. smazání příslušných souřadnic při reprezentaci modelu vektorem.

[23] Přidáním hodnot pro nové výrokové proměnné, resp. přidáním odpovídajících souřadnic ve vektorové reprezentaci

- *T' je extenzí T a zároveň T je extenzí T', právě když $P' = \mathbb{P}$ a $\mathrm{M}_{\mathbb{P}}(T') = \mathrm{M}_{\mathbb{P}}(T)$, neboli $T' \sim T$.*

- *Kompletní jednoduché extenze T jednoznačně až na ekvivalenci odpovídají modelům T.*

Příklad 2.4.8. Mějme teorii $T = \{p \to q\}$ v jazyce $\mathbb{P} = \{p, q\}$. Teorie T_1 v jazyce $\mathbb{P}$ je jednoduchou extenzí T, máme $\mathrm{M}_{\mathbb{P}}(T_1) = \{(1,1)\} \subseteq \{(0,0),(0,1),(1,1)\} = \mathrm{M}_{\mathbb{P}}(T)$. Je to kompletní teorie, další kompletní jednoduché extenze teorie T jsou např. $T_2 = \{\neg p, q\}$ a $T_3 = \{\neg p, \neg q\}$. Každá kompletní jednoduchá extenze teorie T je ekvivalentní s T_1, T_2, nebo T_3.

Uvažme nyní teorii $T' = \{p \leftrightarrow (q \wedge r)\}$ v jazyce $\mathbb{P}' = \{p, q, r\}$. Je extenzí T, neboť $\mathbb{P} = \{p, q\} \subseteq \{p, q, r\} = \mathbb{P}'$ a platí:

$$\begin{aligned}\mathrm{M}_{\mathbb{P}'}(T') &= \{(0,0,0),(0,0,1),(0,1,0),(1,1,1)\} \\ &\subseteq \{(0,0,0),(0,0,1),(0,1,0),(0,1,0),(1,1,0),(1,1,1)\} = \mathrm{M}_{\mathbb{P}'}(T)\end{aligned}$$

Jinými slovy, zúžením modelů T' na jazyk $\mathbb{P}$ dostáváme $\{(0,0),(0,1),(1,0)\}$ což je podmnožina $\mathrm{M}_{\mathbb{P}}(T)$.

Protože platí dokonce $\{(0,0),(0,1),(1,0)\} = \mathrm{M}_{\mathbb{P}}(T)$, jinými slovy, každý model $v \in \mathrm{M}_{\mathbb{P}}(T)$ lze rozšířit na model $v' \in \mathrm{M}_{\mathbb{P}'}(T')$ (např. $(0,1)$ lze rozšířit dodefinováním $v'(r) = 0$ na model $(0,1,0)$), je T' dokonce konzervativní extenzí T. To znamená, že každý výrok v jazyce $\mathbb{P}$ platí v T, právě když platí v T'. Ale výrok $p \to r$ (který je v jazyce $\mathbb{P}'$, ale ne v jazyce $\mathbb{P}$) je novým důsledkem: platí v T' ale ne v T (viz model $(1,1,0)$).

Teorie $T'' = \{\neg p \vee q, \neg q \vee r, \neg r \vee p\}$ v jazyce $\mathbb{P}'$ je extenzí T, ale ne konzervativní extenzí, neboť v ní platí $p \leftrightarrow q$, což neplatí v T. Nebo také proto, že model $(0,1)$ teorie T nelze rozšířit na model teorie T'': $(0,1,0)$ ani $(0,1,1)$ nesplňují axiomy T''.

Teorie T je (jednoduchou) extenzí teorie $\{\neg p \vee q\}$ v jazyce $\mathbb{P}$ a naopak, $T \sim \{\neg p \vee q\}$. Je také, jako každá teorie, jednoduchou konzervativní extenzí sebe sama.

Cvičení 2.7. Ukažte (podrobně), že má-li teorie T kompletní konzervativní extenzi, potom je sama nutně kompletní.

2.5 Algebra výroků

V logice nás většinou[24] zajímají výroky (resp. teorie) *až na ekvivalenci.*[25] Na otázku 'Kolik existuje různých výroků v jazyce $\mathbb{P} = \{p, q, r\}$?' je správná odpověď 'Nekonečně mnoho.' Nejspíše nás ale zajímaly výroky *až na ekvivalenci* (neboli *navzájem neekvivalentní*). Těch je tolik, kolik existuje různých podmnožin modelů jazyka, tedy $2^{|\mathrm{M}_{\mathbb{P}}|} = 2^8 = 256$. Skutečně, mají-li dva výroky stejnou množinu modelů, jsou z definice ekvivalentní. A pro každou množinu modelů můžeme najít odpovídající výrok, např. v DNF (viz 2.3.4). Zkusme trochu složitější úvahu:

Příklad 2.5.1. Mějme teorii T v jazyce $\mathbb{P} = \{p, q, r\}$ mající právě pět modelů. Kolik existuje (až na ekvivalenci) výroků nad $\mathbb{P}$, které jsou nezávislé v teorii T? Označme $|\mathbb{P}| = n = 3$ a $|\mathrm{M}_{\mathbb{P}}(T)| = k = 5$.

Počítáme množiny $M = \mathrm{M}_{\mathbb{P}}(\varphi)$ a požadujeme, aby $\emptyset \neq M \cap \mathrm{M}_{\mathbb{P}}(T) \neq \mathrm{M}_{\mathbb{P}}(T)$. Máme tedy celkem $2^m - 2 = 6$ možností, jak může vypadat množina $M \cap \mathrm{M}_{\mathbb{P}}(T)$. A pro každý model

[24] Pokud např. neprovádíme konkrétní algoritmus založený na syntaktických úpravách, třeba převod do CNF.
[25] Můžeme je chápat jako jakési abstraktní 'vlastnosti' modelů bez ohledu na jejich konkrétní vyjádření.

jazyka, který není modelem T (těch je $2^n - m = 3$) můžeme zvolit libovolně, zda bude či nebude v M. Celkově tedy dostáváme $(2^m - 2) \cdot 2^{2^n - m} = 6 \cdot 2^{8-5} = 48$ možných množin M, tolik je tedy výroků nezávislých v T, až na ekvivalenci.

Podívejme se na věc abstraktněji. Formálně, uvažujeme množinu ekvivalenčních tříd $\sim$ na množině všech výroků $\mathrm{VF}_{\mathbb{P}}$, kterou označíme ${}^{\mathrm{VF}_{\mathbb{P}}}/{\sim}$. Prvky této množiny jsou množiny ekvivalentních výroků, např. $[p{\to}q]_\sim = \{p{\to}q, \neg p{\vee}q, \neg(p{\wedge}\neg q), \neg p{\vee}q{\vee}q, \dots\}$. A máme zobrazení $h : {}^{\mathrm{VF}_{\mathbb{P}}}/{\sim} \to \mathcal{P}(\mathrm{M}_{\mathbb{P}})$ (kde $\mathcal{P}(X)$ je množina všech podmnožin X) definované předpisem:

$$h([\varphi]_\sim) = \mathrm{M}(\varphi)$$

tj. třídě ekvivalentních výroků přiřadíme množinu modelů libovolného z nich. Je snadné ověřit, že toto zobrazení je korektně definované (nezáleží na tom, jaký výrok z třídy ekvivalence jsme si vybrali) a prosté, a že je-li jazyk $\mathbb{P}$ konečný, je h dokonce bijekce. (Ověřte!)

Na množině ${}^{\mathrm{VF}_{\mathbb{P}}}/{\sim}$ můžeme zavést operace $\neg, \wedge, \vee$ pomocí předpisu

$$\begin{aligned} \neg[\varphi]_\sim &= [\neg\varphi]_\sim \\ [\varphi]_\sim \wedge [\psi]_\sim &= [\varphi \wedge \psi]_\sim \\ [\varphi]_\sim \vee [\psi]_\sim &= [\varphi \vee \psi]_\sim \end{aligned}$$

tedy vybereme reprezentanta resp. reprezentanty, a provedeme operaci s nimi, např. 'konjunkce' tříd $[p \to q]_\sim$ a $[q \vee \neg r]_\sim$ je:

$$[p \to q]_\sim \wedge [q \vee \neg r]_\sim = [(p \to q) \wedge (q \vee \neg r)]_\sim$$

Přidáme-li také *konstanty* $\bot = [\bot]_\sim$ a $\top = [\top]_\sim$, dostáváme *(matematickou) strukturu*[26]

$$\mathbf{AV}_{\mathbb{P}} = \langle {}^{\mathrm{VF}_{\mathbb{P}}}/{\sim}; \neg, \wedge, \vee, \bot, \top \rangle$$

které říkáme *algebra výroků* jazyka $\mathbb{P}$. Je to příklad tzv. *Booleovy algebry*. To znamená, že její operace se 'chovají' jako operace $^-, \cap, \cup$ na množině všech podmnožin $\mathcal{P}(X)$ nějaké neprázdné množiny X, a konstanty odpovídají $\emptyset$, X (takové Booleově algebře říkáme *potenční algebra*).[27]

Zobrazení $h : {}^{\mathrm{VF}_{\mathbb{P}}}/{\sim} \to \mathcal{P}(\mathrm{M}_{\mathbb{P}})$ je tedy zobrazení z algebry výroků $\mathbf{AV}_{\mathbb{P}}$ *na* potenční algebru

$$\mathcal{P}(\mathrm{M}_{\mathbb{P}}) = \langle \mathcal{P}(\mathrm{M}_{\mathbb{P}}); ^-, \cap, \cup, \emptyset, \mathrm{M}_{\mathbb{P}} \rangle$$

a je-li jazyk konečný, je to bijekce. Toto zobrazení 'zachovává' operace a konstanty, tj. platí $h(\bot) = \emptyset$, $h(\top) = \mathrm{M}_{\mathbb{P}}$, a

$$\begin{aligned} h(\neg[\varphi]_\sim) &= \overline{h([\varphi]_\sim)} = \overline{\mathrm{M}(\varphi)} = \mathrm{M}_{\mathbb{P}} \setminus \mathrm{M}(\varphi) \\ h([\varphi]_\sim \wedge [\psi]_\sim) &= h([\varphi]_\sim) \cap h([\psi]_\sim) = \mathrm{M}(\varphi) \cap \mathrm{M}(\psi) \\ h([\varphi]_\sim \vee [\psi]_\sim) &= h([\varphi]_\sim) \cup h([\psi]_\sim) = \mathrm{M}(\varphi) \cup \mathrm{M}(\psi) \end{aligned}$$

Takovému zobrazení říkáme *homomorfismus* Booleových algeber, a je-li to bijekce, jde o *izomorfismus*.

[26] Struktura je neprázdná množina spolu s relacemi, operacemi, a konstantami. Například (orientovaný) graf, grupa, těleso, vektorový prostor. Struktury budou hrát důležitou roli v predikátové logice.

[27] Tj. splňují určité algebraické zákony, například distributivitu $\wedge$ vůči $\vee$. Booleovy algebry definujeme formálně později, uveďme ale ještě jeden důležitý příklad: množina všech n-bitových vektorů s operacemi $\sim$, &, | (po složkách) a s konstantami $(0, 0, \dots, 0)$ a $(1, 1, \dots, 1)$.

Poznámka 2.5.2. Tyto vztahy můžeme také využít při hledání modelů: například pro výrok $\varphi \to (\neg\psi \wedge \chi)$ platí (s využitím toho, že $\mathrm{M}(\varphi \to \varphi') = M(\neg\varphi \vee \varphi')$):

$$\mathrm{M}(\varphi \to (\neg\psi \wedge \chi)) = \overline{\mathrm{M}(\varphi)} \cup (\overline{\mathrm{M}(\psi)} \cap \mathrm{M}(\chi))$$

Všechny předchozí úvahy můžeme také relativizovat vzhledem k dané teorii T v jazyce $\mathbb{P}$, a to tak, že ekvivalenci $\sim$ nahradíme T-ekvivalencí $\sim_T$ a množinu modelů jazyka $\mathrm{M}_{\mathbb{P}}$ nahradíme množinou modelů teorie $\mathrm{M}_{\mathbb{P}}(T)$. Dostáváme:

$$\begin{aligned} h(\bot) &= \emptyset, \\ h(\top) &= \mathrm{M}(T) \\ h(\neg[\varphi]_{\sim_T}) &= \mathrm{M}(T) \setminus \mathrm{M}(T, \varphi) \\ h([\varphi]_{\sim_T} \wedge [\psi]_{\sim_T}) &= \mathrm{M}(T, \varphi) \cap \mathrm{M}(T, \psi) \\ h([\varphi]_{\sim_T} \vee [\psi]_{\sim_T}) &= \mathrm{M}(T, \varphi) \cup \mathrm{M}(T, \psi) \end{aligned}$$

Algebra výroků jazyka je tedy totéž co algebra výroků vzhledem k prázdné teorii. Z technických důvodů potřebujeme, aby $\mathrm{M}(T)$ byla neprázdná, tj. T musí být bezesporná. Shrňme naše úvahy:

Důsledek 2.5.3. *Je-li T bezesporná teorie nad* konečným *jazykem $\mathbb{P}$, potom je algebra výroků $\mathbf{AV}_{\mathbb{P}}$ izomorfní potenční algebře $\mathcal{P}(\mathrm{M}_{\mathbb{P}}(\mathbf{T})$ prostřednictvím zobrazení $h([\varphi]_{\sim_T}) = M(T, \varphi)$.*

Víme tedy, že negace, konjunkce, a disjunkce odpovídají doplňku, průniku a sjednocení množin modelů, a že chceme-li najít počet výroků až na ekvivalenci resp. T-ekvivalenci, stačí určit počet příslušných množin modelů. Shrňme si několik takových výpočtů ve formě tvrzení, jeho důkaz necháme jako cvičení.

Tvrzení 2.5.4. *Mějme n-prvkový jazyk $\mathbb{P}$ a bezespornou teorii T mající právě k modelů. Potom v jazyce $\mathbb{P}$ existuje* až na ekvivalenci*:*

- 2^{2^n} *výroků (resp. teorií),*
- 2^{2^n-k} *výroků pravdivých (resp. lživých) v T,*
- $2^{2^n} - 2 \cdot 2^{2^n-k}$ *výroků nezávislých v T,*
- 2^k *jednoduchých extenzí teorie T (z toho 1 sporná),*
- k *kompletních jednoduchých extenzí T.*

Dále až na T-ekvivalenci *existuje:*

- 2^k *výroků,*
- 1 *výrok pravdivý v T,* 1 *lživý v T,*
- $2^k - 2$ *výroků nezávislých v T.*

Cvičení 2.8. Zvolte vhodnou teorii T a ukažte na jejím příkladě, že platí Tvrzení 2.5.4.

Cvičení 2.9. Dokažte podrobně Tvrzení 2.5.4. (Nakreslete si Vennův diagram.)