

# Výroková logika.

Pokud bychom měli definovat pojem **logika**, asi bychom nejvýstižněji mohli říci, že je to studium argumentace. Logika se snaží kodifikovat správné postupy, pomocí nichž vyvozujeme platné závěry z daných informací. I když většina lidí při svých úvahách intuitivně dodržuje základní logické zákony, je přesto vhodné se snažit o jejich formalizaci. Ta nám pomáhá při složitějších situacích, kdy je třeba se vyznat ve velkém množství logických vztahů, ale možná ještě důležitější je její uplatnění při implementaci procesu dedukce do počítačových programů.

Jsou dvě základní úrovně klasické logiky: Nižší je výroková logika, kterou se v této části budeme zabývat, a vyšší, tzv. predikátová logika, o které se zmíníme později.

Pod pojmem **výrok** budeme rozumět tvrzení, o němž lze v principu rozhodnout, zda je pravdivé nebo nepravdivé. Tím se automaticky vylučují zvolání, rozkazy, otázky a věty, které jsou samy se sebou v rozporu. Výrok totiž musí splňovat dvě základní vlastnosti:

- Výrok je buď pravdivý nebo nepravdivý, třetí možnost neexistuje.
- Výrok nemůže být současně pravdivý i nepravdivý.

Uveďme si několik příkladů výroku.

Delfín je savec.  
Kruh je buď čtverec nebo trojúhelník.  
Shakespeare byl básník a námořní kapitán.  
Toto je krychle.

Situace s poslední větou není na první pohled příliš jasná, neboť nemůžeme rozhodnout, zda je tato věta pravdivá či nikoli, dokud nebude určeno, na co se vztahuje zájmeno „Toto“. Nicméně i poslední větu považujeme za výrok, neboť při interpretaci zájmena bude možné pravdivost či nepravdivost posoudit.

Co určitě nejsou výroky, jsou následující.

Kolikátého je dnes?  
Kdybych tohle tušil!  
Okamžitě vypadněte!  
Tato věta není pravdivá.

Poslední tvrzení není výrok, neboť porušuje dichotomii, kterou u výroků požadujeme. Toto tvrzení není ani pravdivé ani nepravdivé: Předpokládáme-li, že tvrzení je pravdivé, okamžitě dospíváme k závěru, že pravdivé není. Pokud naopak předpokládáme, že tvrzení

není pravdivé, pak po jeho opětovném přečtení vidíme, že obsah odpovídá skutečnosti. To se u nepravdivého tvrzení stát nemůže.

**Příklad.** Mějme seznam  $S = \{V_1, V_2, \dots, V_{50}\}$  výroků, kde  $k$ -tý výrok zní

$$V_k: \text{„Právě } k \text{ výroků na seznamu } S \text{ je nepravdivých.} \text{“}$$

Co můžeme vyvodit o pravdivosti či nepravdivosti výroků na seznamu  $S$ ?

První pozorování je, že výrok  $V_{50}$  nemůže být pravdivý, neboť pak by byly všechny výroky (včetně  $V_{50}$ ) nepravdivé. Takže alespoň jeden z výroků pravdivý je. Dále si všimneme, že není možné, aby dva různé výroky byly současně pravdivé. Z těchto dvou pozorování plyne, že na seznamu  $S$  je právě jeden pravdivý výrok. A tedy 49 je jich nepravdivých. Proto jediný pravdivý výrok je  $V_{49}$ .

## Formule výrokové logiky

Přikročme nyní k formalizaci. V běžném jazyce můžeme jednu myšlenku vyjádřit mnoha způsoby. Ve výrokové logice dáváme přednost jednoznačnosti. Proto je pro studium výroků vhodné užívat zápisu, který pracuje s velmi omezenou množinou symbolů, zvanou abeceda výrokové logiky. Přesto, že se abeceda skládá z malého počtu symbolů, umožňuje vyjadřovat základní logickou stavbu všech výroků.

**Definice 1.** *Abeceda výrokové logiky je tvořena symboly uvedenými v následující tabulce.*

Symbol	Název	Význam
(, )	<i>závorky</i>	
$\neg$	<i>negace</i>	<i>ne</i>
$\wedge$	<i>konjunkce</i>	<i>a</i>
$\vee$	<i>disjunkce</i>	<i>nebo (nevylučovací)</i>
$\Rightarrow$	<i>implikace</i>	<i>jestliže ..., pak</i>
$\Leftrightarrow$	<i>ekvivalence</i>	<i>právě, když</i>
$P, Q, R, \dots$	<i>výrokové proměnné</i>	<i>výroky</i>
$P_n, Q_n, R_n, \dots, n = 0, 1, 2, \dots$	<i>výrokové proměnné</i>	<i>výroky</i>

Symboly  $\neg, \wedge, \vee, \Rightarrow$ , and  $\Leftrightarrow$  se nazývají logické spojky. Výrokové proměnné označují jednotlivé výroky a jejich význam je na rozdíl od logických spojek v různých situacích různý. Množinu všech výrokových proměnných budeme značit  $\mathcal{V}$ .

Výroky ve tvaru implikace  $P \Rightarrow Q$  jsou v matematice velmi časté a užívá se pro ně celá řada různých ekvivalentních vyjádření:

- Jestliže platí  $P$ , pak platí  $Q$ .
- $P$  implikuje  $Q$ .
- $P$  je postačující podmínka pro  $Q$ .
- $Q$  vyplývá z  $P$ .
- $Q$  je nutná podmínka pro  $P$ .
- $Q$  platí, kdykoli platí  $P$ .

Má-li výrok tvar implikace  $P \Rightarrow Q$ , pak výrok tvaru  $\neg Q \Rightarrow \neg P$  se nazývá **kontrapozice**.

Zápisy studovaných výroků budeme chtít nazývat formulemi. V principu je takový zápis konečná posloupnost symbolů abecedy. Např.  $P \wedge Q$  nebo  $Q_1 P ((\Rightarrow \vee$  jsou příklady dvou konečných posloupností. Z nich pouze ta první může reprezentovat zápis výroku, a proto jen takové posloupnosti jsou pro nás zajímavé z hlediska studia. Musíme proto definovat pravidla, tzv. syntaxi, podle kterých lze vytvářet posloupnosti schopné označovat výroky.

**Definice 2.** *Formule výrokové logiky je konečná posloupnost symbolů abecedy vyhovující následující indukční konstrukci.*

- (i) *Výroková proměnná je formule.*
- (ii) *Jsou-li  $\varphi$  a  $\psi$  formule, pak  $(\varphi \wedge \psi)$ ,  $(\varphi \vee \psi)$ ,  $(\varphi \Rightarrow \psi)$ ,  $(\varphi \Leftrightarrow \psi)$  a  $(\neg\varphi)$  jsou formule.*

Množinu všech formulí označíme  $\mathcal{V}^*$ .

Slovo „induktivní“ v předešlé definici označuje speciální typ konstrukce, která se často vyskytuje jak v logice, tak i v ostatních odvětvích matematiky. Její princip je následující.

Vytváříme danou množinu tak, že začneme jejími základními prvky (v našem případě to jsou výrokové proměnné). To je požadavek (i) v Definici 2. Na tyto základní prvky opakovaně aplikujeme operace z bodu (ii). Takže po první aplikaci dostaneme např. formule typu

$$(P \wedge Q), \quad (R_1 \Leftrightarrow P_2), \quad (\neg Q_3), \quad \dots$$

Můžeme je nazývat formulemi prvního řádu. Formule druhého řádu jsou vygenerovány z již vytvořených formulí (což jsou výrokové proměnné a formule prvního řádu). Příklady takových nových formulí jsou

$$(\neg(P \wedge Q)), \quad ((R_1 \Leftrightarrow P_2) \vee (\neg Q_3)), \quad \dots$$

Tímto způsobem pokračujeme v konstrukci dalších úrovní. Je zřejmé, že každá formule vznikla z výrokových proměnných konečně mnoha aplikacemi operací z bodu (ii).

Pokud bychom se drželi přísně naší definice, brzy bychom zjistili, že se v zápisech vyskytuje příliš mnoho závorek. Např.  $P \wedge Q$  není formule, neboť podle našich pravidel je formulí pouze  $(P \wedge Q)$ . Podobně

$$(((P \vee Q) \vee R) \vee Q_1)$$

je formule, ale

$$P \vee Q \vee R \vee Q_1$$

není. Abychom si zápis usnadnili a učinili ho čitelnějším, přijmeme následující úmluvu.

- (i) Vnější závorky nebudeme psát. Tak zápisem  $P \wedge Q$  budeme rozumět  $(P \wedge Q)$ .
- (ii) Zavedeme preference mezi logickými spojkami. Negace váže silněji než konjunkce a disjunkce. Konjunkce a disjunkce váží silněji než implikace a ekvivalence. Např.

$$R_1 \wedge Q_2 \Rightarrow \neg P_3 \vee P \quad \text{je} \quad ((R_1 \wedge Q_2) \Rightarrow ((\neg P_3) \vee P)).$$

## J. TIŠER: VÝROKOVÁ LOGIKA

Do jaké míry budeme tuto konvenci používat záleží na naší volbě. V případě nebezpečí, že by mohla vzniknout dvojznačnost, raději uijeme více závorek než méně.

**Příklad.** Zapište formulemi následující výroky s využitím daných výrokových proměnných

$P$  : „Zpráva je skenována proti virům.“

$Q$  : „Zpráva přišla z neznámé adresy.“

- (i) Zpráva je skenována proti virům, kdykoli přijde z neznámé adresy.
- (ii) Zpráva přišla z neznámé adresy, ale nebyla skenována proti virům.
- (iii) Přijde-li zpráva z neznámé adresy, není skenována proti virům.
- (iv) Není pravda, že je nutné skenovat zprávu proti virům, přijde-li z neznámé adresy.

Řešení. (i)  $Q \Rightarrow P$ ; (ii)  $Q \wedge \neg P$ ; (iii)  $Q \Rightarrow \neg P$ ; (iv)  $\neg(Q \Rightarrow P)$ .

### Cvičení.

- (1) Které z následujících posloupností znaků jsou formule výrokového počtu?

$$PQ\vee, \quad (R_1 \wedge Q) \Rightarrow (T_2 \Leftrightarrow P), \quad (R \neg Q), \quad (P \vee \neg(S = Q)), \quad \neg\neg Q.$$

- (2) Označíme

$P$  : „Ptolemáios je Řek.“

$R$  : „Ramses je Egyptan.“

$Q_1$  : „Monet prodal svůj obraz.“

$Q_2$  : „Cézanne prodal svůj obraz.“

$Q_3$  : „Gauguin prodal svůj obraz.“

Zapište formulemi následující výroky.

- (a) Ptolemáios není Řek.
- (b) Ptolemáios je Řek, zatímco Ramses je Egyptan.
- (c) Je-li Ptolemáios Řek, není Ramses Egyptan.
- (d) Ptolemáios je Řek nebo, pokud není, Ramses není Egyptan.
- (e) Ptolemáios je Řek a Ramses je Egyptan nebo ani jedno z toho.
- (f) Monet jako jediný z trojice Monet, Cézanne a Gauguin prodal obraz.
- (g) Gauguin jako jediný z trojice Monet, Cézanne a Gauguin neprodal obraz.
- (h) Pouze jediný z trojice Monet, Cézanne a Gauguin prodal obraz.
- (i) Alespoň jeden z trojice Monet, Cézanne a Gauguin prodal obraz.
- (j) Alespoň dva z trojice Monet, Cézanne a Gauguin prodali obraz.

## J. TIŠER: VÝROKOVÁ LOGIKA

- (k) Nejvýše dva z trojice Monet, Cézanne a Gauguin prodali obraz.  
(l) Přesně dva z trojice Monet, Cézanne a Gauguin prodali obraz.
- (3) Mějme tvrzení  $T_1, T_2, \dots, k \in \mathbb{N}$ , která znějí:

$T_k$  : „Všechna tvrzení  $T_n$  jsou pro  $n > k$  nepravdivá.“

Ukažte, že žádné z tvrzení  $T_1, T_2, \dots$  není výrok.

- (4) U následujících výroků tvaru implikace určete, co je předpoklad a co je závěr. Ke každému výroku vyslovte opak a kontrapozici.
- (a) Jsou-li jablka žlutá, pak pomeranče jsou zelené.  
(b) Diferencovatelnost funkce  $f$  je postačující ke spojitosti  $f$ .  
(c) Funkce je omezená, je-li interovatelná.  
(d) Posloupnost je omezená, kdykoli je konvergentní.  
(e) Je nutné, aby  $n$  bylo prvočíslo, má-li být také  $2^n - 1$  prvočíslo.  
(f) Náš tým vyhraje, pouze pokud v něm bude Karel.
- (5) Která z následujících podmínek je nutná nebo postačující nebo nemá žádný vztah k výroku: „Číslo  $n$  je dělitelné 6.“
- (a)  $n$  je dělitelné 3.  
(b)  $n$  je dělitelné 9.  
(c)  $n$  je dělitelné 12.  
(d)  $n + 1$  je dělitelné 6.  
(e)  $n^2$  je dělitelné 3.  
(f)  $n^3$  je sudé a dělitelné 3.  
(g)  $n$  je součin sudého a lichého čísla.  
(h) Součet cifer je dělitelný 3.

### Výsledky.

- (1) Formule výrokové logiky jsou dvě: druhá a pátá, u které bereme v úvahu úmluvu o závorkách. U čtvrté vadí znaménko  $=$ , které nepatří do abecedy výrokové logiky.
- (2) (a)  $\neg P$ .  
(b)  $P \wedge R$ .  
(c)  $P \Rightarrow \neg R$ .  
(d)  $P \vee (\neg P \Rightarrow \neg R)$ .  
(e)  $(P \wedge R) \vee (\neg P \wedge \neg R)$ .  
(f)  $Q_1 \wedge \neg Q_2 \wedge \neg Q_3$ .  
(g)  $\neg Q_2 \wedge Q_1 \wedge Q_3$ .

- (h)  $(Q_1 \wedge \neg Q_2 \wedge \neg Q_3) \vee (\neg Q_1 \wedge Q_2 \wedge \neg Q_3) \vee (\neg Q_1 \wedge \neg Q_2 \wedge Q_3)$ .  
 (i)  $Q_1 \vee Q_2 \vee Q_3$ .  
 (j)  $(Q_1 \wedge Q_2 \wedge Q_3) \vee (\neg Q_1 \wedge Q_2 \wedge Q_3) \vee (Q_1 \wedge \neg Q_2 \wedge Q_3) \vee (Q_1 \wedge Q_2 \wedge \neg Q_3)$  nebo také  $(Q_1 \wedge Q_2) \vee (Q_1 \wedge Q_3) \vee (Q_2 \wedge Q_3)$ .  
 (k)  $\neg Q_1 \vee \neg Q_2 \vee \neg Q_3$ .  
 (l)  $(\neg Q_1 \wedge Q_2 \wedge Q_3) \vee (Q_1 \wedge \neg Q_2 \wedge Q_3) \vee (Q_1 \wedge Q_2 \wedge \neg Q_3)$ .
- (3) Nejprve si uvědomíme, že žádné tvrzení  $T_k$  nemůže být pravdivý výrok. Pripustíme-li, že nějaké  $T_k$  je pravdivý výrok, pak všechna tvrzení s vyšším indexem než  $k$  jsou nepravdivá. Speciálně  $T_{k+1}$  je nepravdivé. Avšak obsah tohoto údajně nepravdivého tvrzení je pravdivý, neboť říká, že všechna  $T_{k+2}, T_{k+3}, \dots$  jsou nepravdivá - spor. Zbývá možnost, že všechna  $T_k$  jsou nepravdivé výroky. Pak ale tvrzení každého  $T_k$  odpovídá skutečnosti, což u nepravdivého výroku nemůže nastat. Závěr celého rozboru je, že žádné  $T_k$  není výrok.
- (4) (a) Opak: Jablka jsou žlutá a pomeranče nejsou zelené.  
 Kontrapozice: Nejsou-li pomeranče zelené, pak nejsou jablka žlutá.  
 (b) Opak:  $f$  je diferencovatelná a není spojitá.  
 Kontrapozice: Není-li  $f$  spojitá, pak není diferencovatelná.  
 (c) Opak: Funkce je integrovatelná a neomezená.  
 Kontrapozice: Není-li funkce omezená, není ani integrovatelná.  
 (d) Opak: Posloupnost je konvergentní a neomezená.  
 Kontrapozice: Není-li posloupnost omezená, pak není konvergentní.  
 (e) Opak:  $n$  není prvočíslo a  $2^n - 1$  prvočíslo je.  
 Kontrapozice: Není-li  $n$  prvočíslo, není ani  $2^n - 1$  prvočíslo.  
 (f) Opak: Náš tým vyhrál i bez Karla.  
 Kontrapozice: Nebude-li v týmu Karel, tým nevzhraje.
- (5)  $P$  = postačující,  $N$  = nutná,  $0$  = nezávislá podmínka.  
 $P$ : (c), (f);  $N$ : (a), (e), (g), (h);  $0$ : (b), (d).

## Pravdivostní ohodnocení

V této části se budeme o něco podrobněji věnovat pravdivosti a nepravdivosti výroků. Chtěli bychom definovat, co to znamená, že jedna formule je logickým důsledkem jiné formule nebo množiny formulí. Např. by zcela jistě mělo platit, že formule  $P$  je důsledek formule  $P \wedge Q$ . Protože ať už formule  $P$  a  $Q$  označují jakýkoli výrok, z toho že  $P \wedge Q$  je pravdivé, musí plynout, že je pravdivé i  $P$ . Tato naše představa se dá vyjádřit zcela přesným způsobem. K tomu budeme potřebovat pojem *pravdivostní ohodnocení*.

Zafixujeme si množinu  $\{0, 1\}$  pravdivostních hodnot:

- 0** označující nepravdu,  
**1** označující pravdu.

Nyní můžeme přiřadit všem výrokovým proměnným z naší abecedy pravdivostní hodnotu **0** nebo **1**.

**Definice 3.** *Ohodnocení výrokových proměnných je každé zobrazení  $\nu$  z množiny  $\mathcal{V}$  do množiny  $\{0, 1\}$ ,  $\nu: \mathcal{V} \rightarrow \{0, 1\}$ .*

Zápis  $\nu(P) = 1$  čteme, že  $P$  je pravdivý výrok a  $\nu(P) = 0$  čteme, že  $P$  je nepravdivý výrok.

Rádi bychom ohodnocení výrokových proměnných rozšířili z množiny  $\mathcal{V}$  na množinu  $\mathcal{V}^*$  všech formulí. Toto rozšíření však musí respektovat následující pravidla. Jsou-li  $\varphi$  a  $\psi$  formule, pak

- (i)  $\nu(\neg\varphi) = \begin{cases} 0, & \text{když } \nu(\varphi) = 1, \\ 1 & \text{jinak.} \end{cases}$
- (ii)  $\nu(\varphi \wedge \psi) = \begin{cases} 1, & \text{když } \nu(\varphi) = 1 \text{ a } \nu(\psi) = 1, \\ 0 & \text{jinak.} \end{cases}$
- (iii)  $\nu(\varphi \vee \psi) = \begin{cases} 1, & \text{když } \nu(\varphi) = 1 \text{ nebo } \nu(\psi) = 1, \\ 0 & \text{jinak.} \end{cases}$
- (iv)  $\nu(\varphi \Rightarrow \psi) = \begin{cases} 0, & \text{když } \nu(\varphi) = 1 \text{ a } \nu(\psi) = 0, \\ 1 & \text{jinak.} \end{cases}$
- (v)  $\nu(\varphi \Leftrightarrow \psi) = \begin{cases} 1, & \text{když } \nu(\varphi) = \nu(\psi), \\ 0 & \text{jinak.} \end{cases}$

Ve zkrácené podobě můžeme uvedená pravidla sumarizovat v následující tabulce.

$\varphi$	$\psi$	$\neg\varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \Rightarrow \psi$	$\varphi \Leftrightarrow \psi$
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 1

**Definice 4.** *Rozšíření ohodnocení  $\nu$  výrokových proměnných z množiny  $\mathcal{V}$  na množinu  $\mathcal{V}^*$ , které přitom respektuje pravidla v Tabulce 1, budeme nazývat pravdivostní ohodnocení formulí (nebo jen krátce pravdivostní ohodnocení) a označovat jej opět písmenem  $\nu$ .*

V praxi obvykle nerozlišujeme mezi ohodnocením výrokových proměnných a jeho rozšířením na všechny formule. Mluvíme jednoduše o pravdivostní hodnotě formule  $\varphi$  při ohodnocení  $\nu$ .

Pozastavme se na chvíli u Tabulky 1. Do jaké míry odpovídají pravidla v ní uvedená naší intuici? Určitě nikdo nebude překvapen, že pravdivostní hodnota  $\varphi$  je **1** právě, když pravdivostní hodnota  $\neg\varphi$  je **0**. Jiná věc je ale v případě implikace. Rozhodnutí dát hodnotu **1** formuli  $\varphi \Rightarrow \psi$ , když např. obě formule  $\varphi$  a  $\psi$  mají hodnotu **0**, může někoho znepokojit. Abychom rozptýlili tuto pochybnost, položme si otázku: V jaké situaci bychom označili implikaci  $\varphi \Rightarrow \psi$  za nepravdivou? Asi budeme souhlasit s tím, že pouze v případě, kdy předpoklad  $\varphi$  je pravdivý, ale závěr  $\psi$  nepravdivý. To však znamená, že všem ostatním případům musíme přiznat hodnotu **1**.

Pravdivostní ohodnocení implikace, které máme v Tabulce 1, vede rovněž k tomu, že následující dva výroky jsou pravdivé, i když se nám to na první pohled bude zdát podivné.

Je-li číslo 3 dělitelné 7, pak je číslo 3 sudé.

Je-li číslo 4 dělitelné 7, pak je číslo 4 sudé.

První typ je  $(\mathbf{0} \Rightarrow \mathbf{0})$  a druhý  $(\mathbf{0} \Rightarrow \mathbf{1})$ .

V Definici 4 jsme zavedli pravdivostní ohodnocení, jako rozšíření jakéhokoli zobrazení  $\nu$  z množiny výrokových proměnných na všechny formule. Zatím však nevíme, zda-li takové rozšíření vůbec existuje a když ano, je-li jediné nebo je jich více? Následující věta odpovídá na tuto otázku.

**Věta 5.** *Mějme  $\nu: \mathcal{V} \rightarrow \{\mathbf{0}, \mathbf{1}\}$  ohodnocení výrokových proměnných. Pak existuje jediné rozšíření  $\nu: \mathcal{V}^* \rightarrow \{\mathbf{0}, \mathbf{1}\}$  na množinu všech formulí takové, že je pravdivostním ohodnocením, tj. zachovává pravidla Tabulky 1.*

**Důkaz.** Důkaz provedeme indukcí podle řádu formule. Pro účely tohoto důkazu nazveme výrokové proměnné formulemi řádu 0. Formule řádu  $n$  jsou ty, které vznikly z formulí řádu 0 nejvýše  $n$ -násobnou aplikací bodu (ii) z Definice 2.

Krok 1: Na formulích řádu 0 je  $\nu$  jednoznačně zadané.

Krok 2: Předpokládejme, že jsme  $\nu$  jednoznačně rozšířili na formule až do řádu  $n$ . Každá formule řádu  $(n + 1)$ , která není řádu  $n$ , je vytvořena z formulí řádu  $n$  jednou z pěti operací uvedených v Definici 2 (ii). Tabulka 1 definuje rozšíření  $\nu$  pro tyto formule, a to jednoznačným způsobem. Tím jsme dokázali, že  $\nu$  má jednoznačné rozšíření na všechny formule až do řádu  $(n + 1)$ .  $\square$

Rozšiřování pravdivostního ohodnocení popsané v předchozí Větě 5 není pro nás ve skutečnosti nic nového. Provádíme jej pokaždé, když vyplňujeme pravdivostní tabulku nějaké formule. Pravdivostní tabulka uvádí pravdivostní hodnotu dané formule při všech možných ohodnoceních výrokových proměnných.

**Příklad.** Vytvoříme pravdivostní tabulku pro formuli  $\varphi = (P \wedge Q) \vee (\neg P \Rightarrow R)$ .

$P$	$Q$	$R$	$P \wedge Q$	$\neg P \Rightarrow R$	$(P \wedge Q) \vee (\neg P \Rightarrow R)$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$

První tři sloupce tabulky odpovídají třem výrokovým proměnným formule  $\varphi$  a obsahují všechny trojice vytvořené ze symbolů  $\mathbf{0}$  a  $\mathbf{1}$ . Takových je  $2^3 = 8$ . Pokud by formule obsahovala  $n$  proměnných, příslušná tabulka by měla  $2^n$  řádků. Je rozumné si zvolit system pro vyplňování  $\mathbf{0}$  a  $\mathbf{1}$  do prvních sloupců tabulky, abychom na nějakou kombinaci nezapoměli. Zde jsme zvolili lexikografické uspořádání.



Pravdivostní tabulku můžeme používat i v opačném směru: Známe-li hodnotu formule, chceme vyvodit možné hodnoty výrokových proměnných. Tento typ se obvykle hodí v tzv. logických hádankách.

**Příklad.** Tři osoby  $A$ ,  $B$  a  $C$  jsou podezřelé ze spáchání zločinu. Vypověděly následující:

$A$  : „ $B$  je vinen a  $C$  je neviný.“

$B$  : „Je-li vinen  $A$ , je vinen i  $C$ .“

$C$  : „Jsem nevinen, ale alespoň jeden z  $A$  a  $B$  je vinen.“

Jaké jsou odpovědi na otázky:

- (i) Mohou být všechny tři výpovědi pravdivé?
- (ii) Jsou-li všichni neviní, kdo vypovídal křivě?
- (iii) Jsou-li výpovědi pravdivé, kdo je pachatel?
- (iv) Mluví-li neviní pravdu a viníci lžou, kdo je pachatel?

Označíme si postupně  $A$ ,  $B$  a  $C$  výroky „ $A$  je nevinen“, „ $B$  je nevinen“ a „ $C$  je nevinen“. Pak jednotlivé výpovědi jsou formule

$$\neg B \wedge C, \quad \neg A \Rightarrow \neg C, \quad C \wedge (\neg A \vee \neg B).$$

K odpovědím na položené otázky potřebujeme pravdivostní tabulku pro tři výše uvedené formule.

$A$	$B$	$C$	$\neg B \wedge C$	$\neg A \Rightarrow \neg C$	$C \wedge (\neg A \vee \neg B)$
0	0	0	0	1	0
0	0	1	1	0	1
0	1	0	0	1	0
0	1	1	0	0	1
1	0	0	0	1	0
1	0	1	1	1	1
1	1	0	0	1	0
1	1	1	0	1	0

Odpovědi na otázky jsou následující:

- (i) Ano, vidíme to v 6. řádku.
- (ii) Křivě vypovíдалy osoby  $A$  a  $C$ , viz poslední řádek.
- (iii) Ze 6. řádku plyne, že pachatel je  $B$ .
- (iv) Podmínka v otázce znamená, že pravdivostní hodnoty musí vyhovovat třem rovnostem

$$\nu(A) = \nu(\neg B \wedge C), \quad \nu(B) = \nu(\neg A \Rightarrow \neg C) \quad \text{a} \quad \nu(C) = \nu(C \wedge (\neg A \vee \neg B)).$$

První rovnost je splněna v řádcích 1, 3, 4, 6. V rámci nich je druhá rovnost splněna pouze v řádku 3. V tomto řádku platí i třetí rovnost, takže odpověď je, že pachateli jsou osoby  $A$  a  $C$ .

## Cvičení.

- (1) Utvořte pravdivostní tabulku formule  $(P \vee Q) \wedge \neg(P \wedge Q)$  (vylučovací disjunkce).
- (2) Utvořte pravdivostní tabulku formule  $(P \Rightarrow (\neg Q \wedge Q)) \Leftrightarrow \neg P$ .
- (3) Na ostrově žijí dva druhy obyvatel: pravdomluvní a lháři. Ti první mluví za všech okolností pravdu, ti druzí stále lžou.
  - (a) Potkáme dva obyvatele  $P$  a  $Q$  a zeptáme se: „Je někdo z vás lhář?“  $P$  odpoví: „Alespoň jeden z nás je lhář“. Lze určit, kdo jsou  $P$  a  $Q$ ?
  - (b) Potkáme dva obyvatele  $P$  a  $Q$  a zeptáme se  $P$ : „Je někdo z vás lhář?“  $P$  odpoví: „Je-li  $Q$  lhář, pak i já jsem lhář“. Kdo jsou  $P$  a  $Q$ ?
  - (c) Potkáme dva obyvatele a zeptáme se: „Je někdo z vás pravdomluvný?“ Z odpovědi bylo možné určit, kdo je kdo. Jaká byla odpověď a jaký je náš závěr?
  - (d) Potkáme tři obyvatele  $P$ ,  $Q$  a  $R$  a zeptáme se  $P$ : „Jste lhář?“  $P$  něco odpověděl, ale my jsme to přeslechli. Zeptáme se tedy  $Q$ : „Co říkal  $P$ ?“  $Q$  odpověděl: „Řekl, že je lhář.“ Pak se ozval  $R$ : „Nevěřte  $Q$ , je to lhář.“ Kdo je kdo?
- (4) Mějme karty takové, že každá má na jedné straně písmeno a na druhé straně číslo. Vidíme před sebou položené tyto čtyři karty:

$S \quad U \quad 3 \quad 8$

Pravidlo zní: Pokud je písmeno samohláska, na druhé straně je sudé číslo. Kolik karet musíme otočit, abychom zjistili, zda tyto čtyři karty vyhovují pravidlu?

- (5) Pro která pravdivostní ohodnocení proměnných  $P_1, \dots, P_n$  je pravdivá níže uvedená formule?
  - (a)  $(P_1 \Rightarrow P_2) \wedge \dots \wedge (P_{n-1} \Rightarrow P_n)$ ,
  - (b)  $(P_1 \Rightarrow P_2) \wedge \dots \wedge (P_{n-1} \Rightarrow P_n) \wedge (P_n \Rightarrow P_1)$ ,
  - (c) Konjunkce formulí  $(P_i \Rightarrow \neg P_j)$  přes všechny dvojice indexů  $i \neq j$ . Formálně zapsáno:  $\bigwedge_{i \neq j} (P_i \Rightarrow \neg P_j)$ .

## Výsledky.

- (1)  $\nu((P \vee Q) \wedge \neg(P \wedge Q)) = \mathbf{1}$  právě, když  $\nu(P) \neq \nu(Q)$ .
- (2) Pravdivostní hodnota je  $\mathbf{1}$  ve všech ohodnoceních.
- (3)
  - (a)  $P$  je pravdomluvný,  $Q$  je lhář.
  - (b) Oba jsou pravdomluvní.
  - (c) Odpověď byla NE, odpovídající byl lhář a druhý byl pravdomluvný.
  - (d)  $R$  je pravdomluvný,  $Q$  je lhář a  $P$  nelze určit.
- (4) Dvě karty  $U$  a  $3$ .
- (5)
  - (a) Existuje číslo  $k \in \{0, 1, \dots, n\}$ , že  $\nu(P_i) = \mathbf{0}$  pro  $i \leq k$  a  $\nu(P_i) = \mathbf{1}$  pro  $i > k$ .
  - (b) Buď  $\nu(P_i) = \mathbf{0}$  pro všechna  $i$  nebo  $\nu(P_i) = \mathbf{1}$  pro všechna  $i$ .
  - (c)  $\nu(P_i) = \mathbf{1}$  pro nejvýše jeden index  $i$ .

## Logický důsledek

Nyní zavedeme pojem, který odráží naši představu o logickém vyplývání.

**Definice 6.** *Mějme formuli  $\varphi$  a množinu formulí  $\Sigma$ . Řekneme, že  $\varphi$  je logický důsledek formulí z množiny  $\Sigma$  (nebo  $\Sigma$  logicky implikuje  $\varphi$ ), je-li formule  $\varphi$  pravdivá v každém ohodnocení, ve kterém jsou pravdivé všechny formule v množině  $\Sigma$ . Značíme  $\Sigma \models \varphi$ .*

V tomto kontextu nazýváme formule v množině  $\Sigma$  předpoklady a formuli  $\varphi$  závěrem. Pokud  $\varphi$  není logický důsledek množiny  $\Sigma$ , značíme  $\Sigma \not\models \varphi$ .

Je-li  $\Sigma$  jednoprvková množina,  $\Sigma = \{\psi\}$ , píšeme  $\psi \models \varphi$  místo  $\{\psi\} \models \varphi$ . Nastane-li situace, že  $\psi \models \varphi$  a současně  $\varphi \models \psi$ , pak říkáme, že  $\psi$  a  $\varphi$  jsou logicky (nebo také tautologicky či sémanticky) ekvivalentní a píšeme  $\psi \models \varphi$ .

**Příklad.** Uvažujme množinu  $\Sigma = \{P, P \Rightarrow Q\}$ . Ukážeme, že  $\Sigma \models Q$ .

Pravdivostní tabulka je následující:

$P$	$Q$	$P \Rightarrow Q$
<b>0</b>	<b>0</b>	<b>1</b>
<b>0</b>	<b>1</b>	<b>1</b>
<b>1</b>	<b>0</b>	<b>0</b>
<b>1</b>	<b>1</b>	<b>1</b>

Jediný případ, kdy jsou obě formule v  $\Sigma$  interpretovány jako pravdivé, je poslední řádek. Ale tam je pravdivá i formule  $Q$ . Proto platí, že  $\Sigma \models Q$ .

Z Definice 6 plyne, že nutná a postačující podmínka k  $\Sigma \models \varphi$  je existence pravdivostního ohodnocení  $\nu$ , které všechny formule v  $\Sigma$  interpretuje jako pravdivé, ale  $\nu(\varphi) = \mathbf{0}$ . Jako ukázkou vezměme množinu  $\Sigma = \{P, Q \Rightarrow P\}$  a otestujme, zda  $\Sigma \models Q$ . Pravdivostní tabulka je podobná tabulce z předešlého příkladu.

$P$	$Q$	$Q \Rightarrow P$
<b>0</b>	<b>0</b>	<b>1</b>
<b>0</b>	<b>1</b>	<b>0</b>
<b>1</b>	<b>0</b>	<b>1</b>
<b>1</b>	<b>1</b>	<b>1</b>

Zde třetí řádek svědčí o tom, že  $\Sigma \not\models Q$ , neboť obě formule v množině  $\Sigma$  jsou interpretovány jako pravdivé, ale hodnota  $Q$  je **0**. Na tom nic nezmění ani fakt, že čtvrtý řádek dává hodnotu **1** jak formulím v  $\Sigma$ , tak proměnné  $Q$ . Stojí za povšimnutí, že z množiny  $\Sigma$  neplyne ani  $\neg Q$ ,  $\Sigma \not\models \neg Q$ .

**Příklad.** Ověříme, že formule  $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$  a  $P \Leftrightarrow Q$  jsou logicky ekvivalentní. Za tím účelem sestavíme pravdivostní tabulku obou formulí.

$P$	$Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$
<b>0</b>	<b>0</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>
<b>0</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>
<b>1</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>0</b>
<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>

Z tabulky vidíme, že v každém ohodnocení, kdy je první formule pravdivá, je pravdivá i druhá, což znamená, že

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P) \models (P \Leftrightarrow Q).$$

Ale i naopak, je-li pravdivá druhá z formulí, je pravdivá i první, tedy

$$(P \Leftrightarrow Q) \models (P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

Dohromady máme  $(P \Rightarrow Q) \wedge (Q \Rightarrow P) \models (P \Leftrightarrow Q)$ .

Poučení z výše uvedeného příkladu je, že prohlásit dvě formule  $\varphi$  a  $\psi$  za logicky ekvivalentní, je to samé jako říci, že formule  $\varphi$  a  $\psi$  mají tutéž pravdivostní tabulku. To se nám bude ještě hodit.

Podívejme se nyní na zvláštní případ logického důsledku, kdy množina předpokladů je prázdná,  $\Sigma = \emptyset$ . Jaká formule  $\varphi$  je logickým důsledkem prázdné množiny formulí,  $\emptyset \models \varphi$ ? Intuitivně to znamemá, že závěr  $\varphi$  má být pravdivý, kdykoli jsou pravdivé předpoklady. Zde žádné předpoklady nejsou, takže  $\varphi$  musí být pravdivé „samo o sobě“. Jinými slovy,  $\nu(\varphi) = \mathbf{1}$  pro každé pravdivostní ohodnocení  $\nu$ . Takové formule se nazývají tautologie.

**Definice 7.** *Formule  $\varphi$  se nazývá tautologie, pokud  $\nu(\varphi) = \mathbf{1}$  pro každé pravdivostní ohodnocení  $\nu$ . Zápís je  $\models \varphi$ .*

Asi nejjednodušší tautologie je  $(P \vee \neg P)$ . Opak tautologie je formule zvaná kontradikce.

**Definice 8.** *Formule  $\varphi$  se nazývá kontradikce, pokud  $\nu(\varphi) = \mathbf{0}$  pro každé pravdivostní ohodnocení  $\nu$ . Zápís je  $\models \neg\varphi$ .*

Příklad kontradikce je  $(P \wedge \neg P)$ . Je rovněž zřejmé, že negace tautologie je kontradikce a negace kontradikce je tautologie. Když si připomeneme, že dvě formule jsou logicky ekvivalentní právě, když mají identické pravdivostní tabulky, ihned vidíme, že všechny tautologie jsou mezi sebou logicky ekvivalentní a rovněž všechny kontradikce jsou mezi sebou logicky ekvivalentní.

**Příklad.** Ověřte, že formule  $Q_1 \Rightarrow (Q_2 \Rightarrow (Q_3 \Rightarrow Q_1))$  je tautologie.

Způsob, který vždy funguje, je pomocí pravdivostní tabulky. Pro tři proměnné je to ještě zvládnutelné, ale pro více proměnných to přestává být schůdné. Jiná možnost, vhodná zejména při implikacích, je metoda sporem. Předpokládáme, že formule je nepravdivá. Implikace je nepravdivá pouze v jediném případě: předpoklad má hodnotu  $\mathbf{1}$  a závěr  $\mathbf{0}$ . To znamená, že

$$\nu(Q_1) = \mathbf{1} \quad \text{a} \quad \nu(Q_2 \Rightarrow (Q_3 \Rightarrow Q_1)) = \mathbf{0}.$$

Je-li  $\nu(Q_1) = \mathbf{1}$ , je i  $\nu(Q_3 \Rightarrow Q_1) = \mathbf{1}$  bez ohledu na hodnotu  $Q_3$ . Odtud plyne, že i  $Q_2 \Rightarrow (Q_3 \Rightarrow Q_1)$  je pravdivé, a tím celá původní formule. Což je spor, který ukazuje, že při žádném pravdivostním ohodnocení nemůže být  $Q_1 \Rightarrow (Q_2 \Rightarrow (Q_3 \Rightarrow Q_1))$  nepravdivá formule.

Logický důsledek i tautologie jsou definovány pomocí pravdivostního ohodnocení. Navíc v obou případech hrají hlavní roli ta ohodnocení, která příslušným formulím dávají hodnotu  $\mathbf{1}$ . Nepřekvapí nás proto, že mezi logickým důsledkem a tautologií je těsný vztah.

**Věta 9.** *Mějme formule  $\varphi_1, \varphi_2, \dots, \varphi_n$  a  $\psi$ . Následující je ekvivalentní:*

- (i)  $\{\varphi_1, \varphi_2, \dots, \varphi_n\} \models \psi$ , tj.  $\psi$  je logickým důsledkem množiny  $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ .
- (ii)  $\models (\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n) \Rightarrow \psi$ , tj.  $(\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n) \Rightarrow \psi$  je tautologie.

**Důkaz.** Předpokládejme, že je splněn bod (i) a ověříme, že implikace

$$(1) \quad (\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n) \Rightarrow \psi$$

je tautologie. Mějme libovolné ohodnocení  $\nu$ . Pokud je  $\nu(\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n) = \mathbf{0}$ , je implikace pravdivá. Pokud je  $\nu(\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n) = \mathbf{1}$ , pak musí být pravdivé všechny formule  $\varphi_1, \varphi_2, \dots, \varphi_n$ . V tom případě je podle (i) pravdivé i  $\psi$ , a tím i celá implikace.

Nyní naopak předpokládejme, že platí bod (ii) a ověříme, že  $\psi$  je logický důsledek množiny  $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ . Za tím účelem mějme pravdivostní ohodnocení  $\nu$  takové, že  $\nu(\varphi_1) = \dots = \nu(\varphi_n) = \mathbf{1}$ . Protože víme, že implikace (1) je tautologie, a tedy pravdivá, musí být nutně  $\nu(\psi) = \mathbf{1}$ .  $\square$

Z Věty 9 vyplývá, že logickou ekvivalenci můžeme redukovat na tautologii a naopak. Navíc platí tvrzení, že  $\varphi \models \psi$  právě, když  $\models (\varphi \Leftrightarrow \psi)$ . Je-li totiž  $\varphi \models \psi$ , pak je splněno  $\varphi \models \psi$  i  $\psi \models \varphi$ . Podle Věty 9 to značí, že obě formule  $\varphi \Rightarrow \psi$  a  $\psi \Rightarrow \varphi$  jsou tautologiemi. Jejich konjunkce je samozřejmě opět tautologie, která není nic jiného než  $\varphi \Leftrightarrow \psi$ .

Uvedeme si několik často užívaných a užitečných logických ekvivalencí.

$$\begin{aligned} \text{dvojitá negace:} & \quad \neg\neg P \models P \\ \text{nahrazení implikace:} & \quad (\varphi \Rightarrow \psi) \models \neg\varphi \vee \psi \\ \text{kontrapozice:} & \quad (\varphi \Rightarrow \psi) \models (\neg\psi \Rightarrow \neg\varphi) \\ \text{de Morganova pravidla:} & \quad \neg(\varphi \wedge \psi) \models \neg\varphi \vee \neg\psi \\ & \quad \neg(\varphi \vee \psi) \models \neg\varphi \wedge \neg\psi \\ \text{distributivní zákony:} & \quad \varphi \wedge (\psi \vee \theta) \models (\varphi \wedge \psi) \vee (\varphi \wedge \theta) \\ & \quad \varphi \vee (\psi \wedge \theta) \models (\varphi \vee \psi) \wedge (\varphi \vee \theta) \end{aligned}$$

Poslední důležitý pojem spojený s pravdivostním ohodnocením je splnitelnost množiny formulí.

**Definice 10.** *Mějme množinu  $\Sigma$  formulí. Řekneme, že je splnitelná (nebo že má model), jestliže existuje pravdivostní ohodnocení, ve kterém jsou všechny formule v  $\Sigma$  pravdivé.*

Užíváme-li alternativní terminologii, tj. že  $\Sigma$  má model, pak modelem rozumíme právě to ohodnocení, ve kterém jsou všechny formule z  $\Sigma$  interpretovány jako pravdivé. Pokud se množina  $\Sigma$  skládá z jediné formule  $\varphi$ ,  $\Sigma = \{\varphi\}$ , mluvíme o splnitelnosti formule  $\varphi$ . V takovém případě je splnitelnost  $\varphi$  to samé, jako říci, že  $\varphi$  není kontradikce.

**Příklad.** Zjistěte, zda je splnitelná množina

$$\Sigma = \{(P \Rightarrow Q) \Rightarrow R, \neg P \vee R, \neg P \wedge Q \wedge R, Q \Leftrightarrow (P \vee R)\}.$$

Formule obsahují jen tři proměnné, proto je možné úlohu řešit pravdivostní tabulkou.

$P$	$Q$	$R$	$(P \Rightarrow Q) \Rightarrow R$	$\neg P \vee R$	$\neg P \wedge Q \wedge R$	$Q \Leftrightarrow (P \vee R)$
0	0	0	0	1	0	1
0	0	1	1	1	0	0
0	1	0	0	1	0	0
0	1	1	1	1	1	1
1	0	0	1	0	0	0
1	0	1	1	1	0	0
1	1	0	0	0	0	1
1	1	1	1	1	0	1

Ze čtvrtého řádku vyvozujeme, že množina  $\Sigma$  je splnitelná.

Je zřejmé, že každá podmnožina splnitelné množiny je rovněž splnitelná. Speciálně, prázdná množina je splnitelná.

Uvažujme množinu formulí. Přiřadíme-li formulím nějaký význam, stanou se z nich výroky. Pak splnitelnost množiny formulí znamená, že příslušné výroky jsou konzistentní, tj. nejsou navzájem ve sporu. V rovině formulí je tedy splnitelnost to samé jako konzistence v rovině výroků.

**Věta 11.** *Mějme formuli  $\varphi$  a množinu formulí  $\Sigma$ . Následující je ekvivalentní:*

- (i)  $\Sigma \models \varphi$ ,
- (ii)  $\Sigma \cup \{\neg\varphi\}$  není splnitelná.

**Důkaz.** Předpokládejme, že  $\Sigma \models \varphi$  a že  $\nu$  je pravdivostní ohodnocení, ve kterém jsou všechny formule v  $\Sigma$  pravdivé. Protože  $\varphi$  je logickým důsledkem  $\Sigma$ , je  $\nu(\varphi) = 1$ . Pak je ale množina  $\Sigma \cup \{\neg\varphi\}$  nespjitelná.

Nyní naopak předpokládejme, že  $\Sigma \cup \{\neg\varphi\}$  je nespjitelná. Mějme ohodnocení  $\nu$ , ve kterém jsou všechny formule v  $\Sigma$  pravdivé. Pak nutně musí platit, že  $\nu(\neg\varphi) = 0$ , neboť v opačném případě by byla množina  $\Sigma \cup \{\neg\varphi\}$  splnitelná. Odtud plyne, že  $\nu(\varphi) = 1$ .  $\square$

Poznamenejme, že z Věty 11 vyplývá, že logickým důsledkem nespjitelné množiny je každá formule.

V jedné z dalších sekcí budeme diskutovat testování splnitelnosti pomocí efektivnější metody než je pravdivostní tabulka. S pomocí Věty 11 tím získáme i efektivnější způsob ověřování logického důsledku.

## Cvičení.

- (1) Které z následujících formulí jsou tautologie, které kontradikce a které jsou splnitelné.
  - (a)  $\neg(P \Rightarrow \neg P)$ ;
  - (b)  $P \vee (P \Rightarrow \neg P)$ ;
  - (c)  $P \vee (Q \vee \neg Q)$ ;
  - (d)  $\neg((P \vee \neg P) \Rightarrow Q)$ ;

- (e)  $\neg P \vee \neg(P \Rightarrow Q)$ ;
- (f)  $((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$ ;
- (g)  $(P \vee \neg Q) \Rightarrow \neg(Q \vee \neg P)$ ;
- (h)  $((P \Rightarrow Q) \Rightarrow P) \wedge \neg P$ ;
- (i)  $(P \Rightarrow Q) \vee (Q \Rightarrow R) \vee \neg(\neg P \vee R)$ ;
- (j)  $\neg(\neg P \Leftrightarrow Q) \Rightarrow (R \vee \neg Q)$ ;
- (k)  $((P \wedge R) \Rightarrow Q) \Leftrightarrow (R \wedge \neg(P \Rightarrow Q))$ .

(2) Určete, které z naznačených logických důsledků jsou správné.

- (a)  $\{\neg P \Rightarrow Q, \neg P \Rightarrow \neg Q\} \models P$ .
- (b)  $\{P \wedge Q, P \Rightarrow R, Q \Rightarrow S\} \models R \wedge S$ .
- (c)  $\{\neg R, \neg(P \wedge \neg R), \neg P \Rightarrow \neg Q\} \models \neg Q$ .

(3) Ukažte, že formule  $(P \Rightarrow (Q \Rightarrow (R \Leftrightarrow (Q \Rightarrow P))))$  a  $P \Rightarrow (Q \Rightarrow R)$  jsou logicky ekvivalentní.

(4) Ukažte, že formule  $P \Leftrightarrow (Q \Leftrightarrow R)$  a  $(P \Leftrightarrow Q) \Leftrightarrow R$  jsou logicky ekvivalentní. Platnost asociativního zákona by nás mohla vést k tomu, že bychom psali krátce  $P \Leftrightarrow Q \Leftrightarrow R$ . Tuto formuli však obvykle interpretujeme, že  $P, Q, R$  jsou buď všechny pravdivé nebo všechny nepravdivé, což **není** ekvivalentní ani jedné z formulí  $P \Leftrightarrow (Q \Leftrightarrow R)$  a  $(P \Leftrightarrow Q) \Leftrightarrow R$ .

(5) Množina formulí  $\mathcal{F}$  se nazývá **nezávislá**, když pro každou  $\varphi \in \mathcal{F}$  platí, že není logickým důsledkem ostatních formulí z  $\mathcal{F}$ , tj.  $\mathcal{F} \setminus \{\varphi\} \not\models \varphi$ . Která z následujících množin je nezávislá?

- (a)  $\{P \Rightarrow Q, Q \Rightarrow R, R \Rightarrow P\}$ ;
- (b)  $\{P \Rightarrow Q, Q \Rightarrow R, P \Rightarrow R\}$ ;
- (c)  $\{P, Q, P \Rightarrow R, R \Rightarrow Q\}$ ;
- (d)  $\{P_1, P_1 \wedge P_2, P_1 \wedge P_2 \wedge P_3, \dots, P_1 \wedge \dots \wedge P_n, \dots\}$ . Má tato množina nějakou nezávislou podmnožinu?

(6) Uvažujme všechny formule tří proměnných  $P, Q, R$ .

- (a) Kolik je jich, až na logickou ekvivalenci, pravdivých přesně v pěti pravdivostních ohodnoceních?
- (b) Kolik je jich, až na logickou ekvivalenci, logickým důsledkem  $P \vee Q$ ?

(Víme, že formule je jednoznačně určena, až na logickou ekvivalenci, svojí pravdivostní tabulkou.)

### Výsledky.

(1) Tautologie: (b), (c), (f), (i). Kontradikce: (h), (k). Splnitelné: (a), (d), (e), (g), (j).

- (2) Všechny logické důsledky platí.
- (5) (a) Množina je nezávislá.  
 (b) Množina není nezávislá, např.  $\{P \Rightarrow Q, Q \Rightarrow R\} \models P \Rightarrow R$ .  
 (c) Množina není nezávislá, např.  $\{P, P \Rightarrow R, R \Rightarrow Q\} \models Q$ .  
 (d) Pouze prázdná množina a jednoprvkové podmnožiny jsou nezávislé. Obsahuje-li podmnožina alespoň dvě formule, pak nejkratší formule v dané podmnožině je logickým důsledkem zbylých formulí.
- (6) (a) Formule  $\varphi$  o třech proměnných má osmiřádkovou pravdivostní tabulku. Z nich si zvolíme 5 řádků, kde bude stát ohodnocení **1**. To lze učinit  $\binom{8}{5} = 56$  způsoby.  
 (b) Osmiřádková tabulka pro formuli  $\varphi$  obsahuje 6 řádků, kde má  $P$  nebo  $Q$  ohodnocení **1**. Na těchto řádcích musí mít hodnotu **1** i formule  $\varphi$ . Na zbylých dvou řádcích mohou být hodnoty **0** nebo **1**. To lze doplnit čtyřmi způsoby. Počet hledaných formulí je tak 4.

## Booleovské funkce

Zatím jsme používali pět logických spojek:  $\neg, \wedge, \vee, \Rightarrow$  a  $\Leftrightarrow$ . Je zřejmé, že těchto pět známých spojek nepředstavuje jedinou možnost. Získali bychom něco přidáním nových spojek k abecedě? Nebo naopak ztratili bychom něco vynecháním nějaké ze spojek, které máme? Abychom odpověděli na tyto otázky, připomeňme si příklady logických ekvivalencí z předchozí sekce. Ukazují nám, že např.  $\varphi \Rightarrow \psi$  je ekvivalentní formuli  $\neg\varphi \vee \psi$ . Pokud vypustíme z abecedy implikaci, nic neztrácíme, protože ji můžeme modelovat pomocí zbylých spojek. Podobná situace by byla, kdybychom rozšířili naši abecedu o nějakou novou logickou spojku. Takové rozšíření by nám nic nového nepřineslo, protože každou formuli v rozšířené abecedě bychom mohli ekvivalentně nahradit formulí v původní abecedě.

Abychom odůvodnili předchozí argumentaci, bude vhodné si zavést pojem booleovské funkce.

**Definice 12.** Každá funkce  $B: \{0, 1\}^n \rightarrow \{0, 1\}$  se nazývá ( $n$ -ární) booleovská funkce,  $n \in \mathbb{N}$ .

V případě  $n = 1$  a  $n = 2$  užíváme názvy „unární“ a „binární“. Příklad unární booleovské funkce je

$$B(0) = 1, B(1) = 0.$$

Binární booleovská funkce je např.

$$B(0, 0) = 1, B(0, 1) = 1, B(1, 0) = 0, B(1, 1) = 0.$$

Obecně,  $n$ -ární booleovská funkce je funkce  $n$  proměnných, které nabývají hodnot pouze **0** a **1**.

Důležitý případ nastává, když je booleovská funkce odvozena z nějaké formule  $\varphi$ . Je-li např.  $\varphi = P \wedge Q$ , můžeme utvořit pravdivostní tabulku a pomocí ní booleovskou funkci definovat.



$P$	$Q$	$P \wedge Q$	$B(X_1, X_2)$
<b>0</b>	<b>0</b>	<b>0</b>	$B(\mathbf{0}, \mathbf{0}) = \mathbf{0}$
<b>0</b>	<b>1</b>	<b>0</b>	$B(\mathbf{0}, \mathbf{1}) = \mathbf{0}$
<b>1</b>	<b>0</b>	<b>0</b>	$B(\mathbf{1}, \mathbf{0}) = \mathbf{0}$
<b>1</b>	<b>1</b>	<b>1</b>	$B(\mathbf{1}, \mathbf{1}) = \mathbf{1}$

Booleovskou funkci odvozenou z formule  $\varphi$  budeme značit  $B_\varphi$  a říkat, že  $B_\varphi$  je realizována formulí  $\varphi$ . Obecná definice je následující:

**Definice 13.** *Mějme formuli  $\varphi = \varphi(P_1, \dots, P_n)$  obsahující výrokové proměnné  $P_1, \dots, P_n$ . Booleovská funkce  $B_\varphi(X_1, \dots, X_n)$  realizovaná formulí  $\varphi$  je funkce, pro kterou platí*

$$B_\varphi(\nu(P_1), \dots, \nu(P_n)) = \nu(\varphi)$$

pro všechna pravdivostní ohodnocení  $\nu$ .

Vyvstává přirozená otázka, zda lze každou booleovskou funkci realizovat nějakou formulí. Než odpovíme na tuto otázku v plné obecnosti bude užitečné se podívat na konkrétní příklad.

Mějme booleovskou funkci  $B$  zadanou:

$$\begin{aligned} B(\mathbf{0}, \mathbf{0}, \mathbf{0}) &= \mathbf{0}, \\ B(\mathbf{0}, \mathbf{0}, \mathbf{1}) &= \mathbf{1}, \\ B(\mathbf{0}, \mathbf{1}, \mathbf{0}) &= \mathbf{0}, \\ B(\mathbf{0}, \mathbf{1}, \mathbf{1}) &= \mathbf{1}, \\ B(\mathbf{1}, \mathbf{0}, \mathbf{0}) &= \mathbf{1}, \\ B(\mathbf{1}, \mathbf{0}, \mathbf{1}) &= \mathbf{0}, \\ B(\mathbf{1}, \mathbf{1}, \mathbf{0}) &= \mathbf{0}, \\ B(\mathbf{1}, \mathbf{1}, \mathbf{1}) &= \mathbf{1}. \end{aligned}$$

Jedna možnost, jak sestavit formuli  $\varphi$ , že  $B_\varphi = B$ , je následující.

**Metoda A:**

Sestavíme seznam všech trojic  $(X_1, X_2, X_3)$ , ve kterých je  $B(X_1, X_2, X_3) = \mathbf{1}$ . Ke každé trojici napíšeme vhodnou konjunkci, která má hodnotu  $\mathbf{1}$  právě pro ohodnocení dané touto trojicí pravdivostních hodnot.

$$\begin{aligned} \mathbf{001} & \quad \neg P_1 \wedge \neg P_2 \wedge P_3, \\ \mathbf{011} & \quad \neg P_1 \wedge P_2 \wedge P_3, \\ \mathbf{100} & \quad P_1 \wedge \neg P_2 \wedge \neg P_3, \\ \mathbf{111} & \quad P_1 \wedge P_2 \wedge P_3. \end{aligned}$$

Když nyní položíme

$$\begin{aligned} \varphi &= (\neg P_1 \wedge \neg P_2 \wedge P_3) \vee (\neg P_1 \wedge P_2 \wedge P_3) \\ &\quad \vee (P_1 \wedge \neg P_2 \wedge \neg P_3) \vee (P_1 \wedge P_2 \wedge P_3), \end{aligned}$$

pak  $\varphi$  je pravdivá jen pro výše vypsané trojice hodnot a nepravdivá ve všech ostatních. Jinými slovy,  $B_\varphi = B$ .

Nemáme žádný apriorní důvod preferovat trojice  $(X_1, X_2, X_3)$ , kde hodnota funkce  $B(X_1, X_2, X_3) = \mathbf{1}$ . Můžeme provést podobnou konstrukci i pro trojice, ve kterých je  $B(X_1, X_2, X_3) = \mathbf{0}$ .

**Metoda B:**

Zde vytvoříme seznam trojic, pro které je  $B(X_1, X_2, X_3) = \mathbf{0}$ . Napravo od každé trojice napíšeme disjunci, která má hodnotu  $\mathbf{0}$  právě pro ohodnocení dané touto trojicí.

$$\begin{array}{ll} \mathbf{000} & P_1 \vee P_2 \vee P_3, \\ \mathbf{010} & P_1 \vee \neg P_2 \vee P_3, \\ \mathbf{101} & \neg P_1 \vee P_2 \vee \neg P_3, \\ \mathbf{110} & \neg P_1 \vee \neg P_2 \vee P_3. \end{array}$$

Položíme-li

$$\begin{aligned} \varphi &= (P_1 \vee P_2 \vee P_3) \wedge (P_1 \vee \neg P_2 \vee P_3) \\ &\quad \wedge (\neg P_1 \vee P_2 \vee \neg P_3) \wedge (\neg P_1 \vee \neg P_2 \vee P_3), \end{aligned}$$

pak bude  $\varphi$  nepravdivá jen pro trojice vypsané výše a pravdivá ve všech ostatních případech. Tj.  $B_\varphi = B$ .

**Věta 14.** *Mějme  $n$ -ární booleovskou funkci  $B$ . Pak existuje formule  $\varphi$  závislá na  $n$  proměnných, která realizuje funkci  $B$ ,  $B = B_\varphi$ .*

**Důkaz.** Ke konstrukci můžeme užít kterýkoli ze dvou přístupů uvedených před větou. Provedeme např. detailně Metodu A a Metodu B jen stručně okomentujeme.

Je-li  $B = \mathbf{0}$ , pak  $\varphi = P \wedge \neg P$ .

Můžeme tedy předpokládat, že existují body z definičního oboru  $\{\mathbf{0}, \mathbf{1}\}^n$ , kde  $B$  nabývá hodnoty  $\mathbf{1}$ . Řekněme, že takových bodů je  $k$  a my jsme si je všechny vypsali:

$$\begin{array}{c} (X_{11}, X_{12}, \dots, X_{1n}) \\ (X_{21}, X_{22}, \dots, X_{2n}) \\ \vdots \\ (X_{k1}, X_{k2}, \dots, X_{kn}) \end{array}$$

Pro každou vypsanou  $n$ -tici vytvoříme konjunkci proměnných, která bude mít hodnotu  $\mathbf{1}$  právě jen pro ohodnocení uvedené v  $n$ -tici. Pro  $i = 1, \dots, k$  a  $j = 1, \dots, n$  položíme

$$\theta_{ij} = \begin{cases} P_j & \text{je-li } X_{ij} = \mathbf{1} \\ \neg P_j & \text{je-li } X_{ij} = \mathbf{0}. \end{cases}$$

Příslušná konjunkce pro  $i$ -tý řádek je  $\psi_i = \theta_{i1} \wedge \theta_{i2} \wedge \dots \wedge \theta_{in}$ . Všimněme si, že  $\psi_i$  je pravdivá jen pro jediný výběr pravdivostního ohodnocení, a to pro  $(X_{i1}, X_{i2}, \dots, X_{in})$ . Nakonec formule  $\varphi$ ,

$$\varphi = \psi_1 \vee \psi_2 \vee \dots \vee \psi_k.$$

Nyní je jasné, že booleovská funkce  $B_\varphi$  realizovaná formulí  $\varphi$  nabývá hodnoty  $\mathbf{1}$  v bodech uvedených na seznamu výše a  $\mathbf{0}$  všude jinde. Takže  $B_\varphi = B$ .

Kdybychom se rozhodli pro Metodu B, podíváme se nejdříve, zda existuje bod definičního oboru  $\{\mathbf{0}, \mathbf{1}\}^n$ , kde hodnota funkce je  $\mathbf{0}$ . Pokud ne, je formule  $\varphi = P \vee \neg P$ . Jinak příslušná formule vypadá

$$\varphi = \psi_1 \wedge \psi_2 \wedge \cdots \wedge \psi_k,$$

kde

$$\psi_i = \theta_{i1} \vee \theta_{i2} \vee \cdots \vee \theta_{in_i} \quad \text{a} \quad \theta_{ij} = \begin{cases} P_j & \text{je-li } X_{ij} = \mathbf{0} \\ \neg P_j & \text{je-li } X_{ij} = \mathbf{1} \end{cases}.$$

□

Podle právě dokázané věty je každá booleovská funkce realizovaná formulí. Formule, která danou funkci realizuje není jediná. Jakákoli s ní logicky ekvivalentní realizuje stejnou booleovskou funkci.

Důsledek předchozí věty je rovněž fakt, že logických spojek je dostačující (dokonce více než dostačující) množství pro realizaci všech booleovských funkcí. Představme si, že bychom rozšířili jazyk výrokového počtu o nějakou novou exotickou logickou spojku. Každá formule  $\tilde{\varphi}$  v tomto rozšířeném jazyce realizuje booleovskou funkci  $B_{\tilde{\varphi}}$ . Podle předchozí věty ale existuje formule  $\varphi$  v původním jazyce, která rovněž realizuje  $B_{\tilde{\varphi}}$ . Formule  $\tilde{\varphi}$  má tak ekvivalentní protějšek ve formuli  $\varphi$ , vyjádřené v původním nerozšířeném jazyce.

Poslední poznámka se týká názvu „booleovský“. Množina  $\{\mathbf{0}, \mathbf{1}\}$  je obdařena algebraickou strukturou: booleovským součinem a booleovským součtem. První operace je totožná s obyčejným součinem čísel. Druhá se od normálního sčítání liší v jediném bodě, a to, že

$$\mathbf{1} + \mathbf{1} = \mathbf{0},$$

což je sčítání modulo 2. Množina  $\{\mathbf{0}, \mathbf{1}\}$  s výše uvedenými operacemi je důležitý případ obecnější matematické struktury nazývané booleovská algebra. Do dalších detailů zde nebudeme zacházet, nicméně ve cvičení (1) níže je vidět, jak má pět logických spojek své protějšky v booleovských operacích.

## Cvičení.

- (1) Mějme dvě formule  $\varphi$  a  $\psi$ , které realizují booleovské funkce  $B_\varphi$  a  $B_\psi$ . Pomocí pravdivostní tabulky ověřte následující rovnosti. Znaménko  $+$  má význam booleovského součtu.

- (a)  $B_{\neg\varphi} = \mathbf{1} + B_\varphi$ ,
- (b)  $B_{\varphi \wedge \psi} = B_\varphi B_\psi$ ,
- (c)  $B_{\varphi \vee \psi} = B_\varphi + B_\psi + B_\varphi B_\psi$ ,
- (d)  $B_{\varphi \Rightarrow \psi} = \mathbf{1} + B_\varphi + B_\varphi B_\psi$ ,
- (e)  $B_{\varphi \Leftrightarrow \psi} = \mathbf{1} + B_\varphi + B_\psi$ .

- (2) Mějme formule  $\varphi$  a  $\psi$ . Ukažte, že

- (a)  $\varphi \models \psi$  právě, když  $B_\varphi \leq B_\psi$ .
- (b)  $\varphi \models \psi$  právě, když  $B_\varphi = B_\psi$ .
- (c)  $\models \varphi$  právě, když  $B_\varphi = \mathbf{1}$ .

## Tvary DNF a CNF

Z důkazu Věty 14 plyne ještě jedno poučení. Formule, která realizuje danou booleovskou funkci je velmi specifického tvaru. Jediné logické spojky, které obsahuje, jsou  $\neg$ ,  $\wedge$  a  $\vee$ . Dvě metody užité při konstrukci nám dávají dva kanonické tvary formulí.

**Definice 15.** *Formule, která je rovna pouze výrokové proměnné nebo negaci výrokové proměnné, se krátce nazývá literál.*

*Formule  $\varphi$  je v disjunktivním normálovém tvaru (DNF), když*

$$\varphi = \psi_1 \vee \psi_2 \vee \cdots \vee \psi_k,$$

*kde všechny  $\psi_i$  jsou konjunkcemi literálů, tj.  $\psi_i = \theta_{i1} \wedge \theta_{i2} \wedge \cdots \wedge \theta_{in_i}$  a  $\theta_{ij}$  jsou literály.*

*Podobně formule  $\varphi$  je v konjunktivním normálovém tvaru (CNF), když*

$$\varphi = \psi_1 \wedge \psi_2 \wedge \cdots \wedge \psi_k,$$

*kde všechny  $\psi_i$  jsou disjunktivními literály, tj.  $\psi_i = \theta_{i1} \vee \theta_{i2} \vee \cdots \vee \theta_{in_i}$  a  $\theta_{ij}$  jsou literály.*

Dvě metody užité v důkaze Věty 14 dávají

**Důsledek.** *Každá formule je logicky ekvivalentní formulí ve tvaru DNF i CNF.*

Převedeme formulí  $(\neg P \Rightarrow Q) \Rightarrow (R \Rightarrow P)$  do CNF i do DNF. Při tomto převodu nemusíme jít cestou přes booleovské funkce a Metodu A a B. Mnohem kratší je aplikovat pravidla, která zachovávají logickou ekvivalenci.

$$\begin{aligned} (\neg P \Rightarrow Q) \Rightarrow (R \Rightarrow P) &\models \text{eliminace krajních implikací} \\ (\neg\neg P \vee Q) \Rightarrow (\neg R \vee P) &\models \text{odstranění dvojité negace} \\ (P \vee Q) \Rightarrow (\neg R \vee P) &\models \text{eliminace implikace} \\ \neg(P \vee Q) \vee (\neg R \vee P) &\models \text{de Morganovo pravidlo} \\ (\neg P \wedge \neg Q) \vee \neg R \vee P &\models \text{distributivní zákon} \\ (\neg P \vee \neg R \vee P) \wedge (\neg Q \vee \neg R \vee P) & \end{aligned}$$

Poslední řádek je tvar CNF dané formule. Tvar DNF máme dokonce už v předposledním řádku.

Každá tautologie má CNF i DNF tvar jednoduchý:  $P \vee \neg P$ . Obdobně každá kontradikce má CNF i DNF tvar  $P \wedge \neg P$ .

Protože každá booleovská funkce může být realizována formulí užívající pouze spojky  $\{\neg, \wedge, \vee\}$ , říkáme, že množina spojek  $\{\neg, \wedge, \vee\}$  je **úplná**. Úplnost této množiny může být ještě zlepšena:

**Věta 16.** *Množiny  $\{\neg, \wedge\}$  a  $\{\neg, \vee\}$  jsou úplné.*

**Důkaz.** Protože  $\{\neg, \wedge, \vee\}$  je úplná množina spojek, stačí, pro první případ, modelovat disjunkci pomocí nějaké kombinace negace a konjunkce. Toho dosáhneme de Morganovým pravidlem  $P \vee Q \models \neg(\neg P \wedge \neg Q)$ . Stejně postupujeme i ve druhém případě.  $\square$

Můžeme jít ještě dále a ptát se, zda existuje nějaká zvláštní logická spojka, která sama o sobě tvoří úplnou množinu? Taková opravdu existuje, značí se  $|$  a nazývá se Shefferův operátor. Je definován  $P|Q := \neg(P \wedge Q)$  nebo následující tabulkou.

P	Q	P Q
0	0	1
0	1	1
1	0	1
1	1	0

Pomocí Shefferova operátoru můžeme modelovat např. negaci a konjunkci:

$$\neg P \models P|P$$

$$P \wedge Q \models (P|Q)|(P|Q)$$

Z Věty 16 teď plyne, že množina  $\{| \}$  je úplná.

### Cvičení.

(1) Převeďte následující formule do tvaru CNF a DNF.

- (a)  $\neg(P \Leftrightarrow Q)$ ,
- (b)  $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow P$ ,
- (c)  $(P \Leftrightarrow \neg Q) \Leftrightarrow R$ ,
- (d)  $P \Rightarrow (\neg Q \Leftrightarrow R)$ ,
- (e)  $(\neg P \wedge (\neg Q \Leftrightarrow P)) \Rightarrow ((Q \wedge \neg P) \vee P)$ .

(2) Definujme binární spojku  $(P \downarrow Q) \models \neg(P \vee Q)$ . Ukažte, že množina  $\{\downarrow\}$  je úplná množina spojek.

(3) Ukažte, že  $\{\neg, \rightarrow\}$  je úplná množina spojek. Množiny  $\{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$  a  $\{\neg, \Leftrightarrow\}$  nejsou úplné.

(4) Označíme symbolem  $\natural$  novou logickou spojku definovanou

$$\nu(\natural(PQR)) = \begin{cases} \mathbf{1} & \text{pokud alespoň dvě proměnné z } P, Q, R \text{ mají ohodnocení } \mathbf{1}, \\ \mathbf{0} & \text{jinak.} \end{cases}$$

Nalezněte tvar DNF formule  $\varphi = \natural(PQR)$ .

### Výsledky.

- (1) (a) CNF:  $(P \vee Q) \wedge (\neg P \vee \neg Q)$ ; DNF:  $(P \wedge \neg Q) \vee (\neg P \wedge Q)$ .
  - (b) CNF i DNF je stejný,  $P \vee Q$ .
  - (c) CNF:  $(\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee \neg R)$ ;  
DNF:  $(\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge \neg R)$ .
  - (d) CNF:  $(\neg P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee R)$ ; DNF:  $\neg P \vee (Q \wedge \neg R) \vee (\neg Q \wedge R)$ .
  - (e) Formule je tautologie,  $P \vee \neg P$ .
- (2) Podle Věty 16 stačí modelovat pomocí  $\downarrow$  negaci a disjunkci:  $\neg P \models P \downarrow P$ ,  $P \vee Q \models (P \downarrow Q) \downarrow (P \downarrow Q)$ .

- (3) Podle Věty 16 stačí modelovat  $\vee$  pomocí  $\neg, \Rightarrow$ :  $P \vee Q \models \neg P \Rightarrow Q$ .  
 Pomocí spojky  $\vee, \wedge, \Rightarrow, \Leftrightarrow$  nelze modelovat negaci. Uvažujme formule  $\varphi(P)$  proměnné  $P$  tvořené pouze spojkami z  $\{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$ . Vlastnost každé takové formule  $\varphi$  je, že je pravdivá, kdykoli  $\nu(P) = \mathbf{1}$ . (Rozmyslete!) Proto nemůže platit  $\varphi(P) \models \neg P$ .  
 Podobně pomocí spojky  $\neg, \Leftrightarrow$  nelze modelovat konjunkci (ani disjunkci). Uvažujme formule  $\varphi(P, Q)$  proměnných  $P, Q$  tvořené pouze spojkami z  $\{\neg, \Leftrightarrow\}$ . Vlastnost každé takové formule  $\varphi$  je, že při záměně  $P, Q$  na  $\neg P, \neg Q$  se pravdivostní hodnota  $\varphi$  nezmění,  $\nu(\varphi(P, Q)) = \nu(\varphi(\neg P, \neg Q))$ . (Rozmyslete!) Proto nemůže platit  $\varphi(P, Q) \models P \wedge Q$ . (Jiný způsob důkazu může být, že výše uvedené formule  $\varphi(P, Q)$  mají pravdivostní tabulku obsahující vždy sudý počet  $\mathbf{1}$ . Proto nemohou být ekvivalentní s  $P \wedge Q$ .)
- (4)  $\varphi \models (P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R)$ .

## Rezoluční metoda

V této části popíšeme metodu, jak rychle rozhodnout, je-li formule logickým důsledkem nějaké zadané množiny formulí. K tomu využijeme Větu 11, která nám logický důsledek redukuje na splnitelnost množiny formulí.

Problem splnitelnosti množiny formulí má velkou praktickou důležitost. Metoda pravdivostní tabulky, vhodná pro formule s nízkým počtem proměnných, roste z hlediska počtu operací exponenciálně s počtem proměnných. Např. při 100 proměnných, by tabulkovou metodu nezvládl ani nejvýkonější počítač.

K popisu rezoluční metody potřebujeme několik nových termínů. **Klauzule** je každá disjunkce literálů,  $\theta_1 \vee \dots \vee \theta_n$ . S klauzulí jsme se už setkali (i když jsme tento termín nepoužívali) ve tvaru CNF. Tvar CNF je vlastně konjunkcí klauzulí.

Mějme klauzuli  $\psi = \theta_1 \vee \theta_2 \vee \dots \vee \theta_n$ . Můžeme ji rovněž psát ve tvaru

$$\{\theta_1, \theta_2, \dots, \theta_n\},$$

kde čárka nahrazuje logickou spojku  $\vee$ . Tak se můžeme na klauzuli dívat jako na množinu literálů  $\psi = \{\theta_1, \theta_2, \dots, \theta_n\}$ . To nám umožní mluvit např. o sjednocení klauzulí nebo množinovém rozdílu klauzulí či o prázdné klauzuli. Navíc tato konvence eliminuje jak pořadí literálů, tak jejich opakování v klauzuli:  $\theta_1 \vee \theta_2 \vee \theta_1$  je jednoduše  $\{\theta_1, \theta_2\}$ .

**Definice 17.** Řekneme, že klauzule  $\psi_1$  a  $\psi_2$  jsou v rezoluční relaci podle literálu  $\theta$ , pokud jedna z nich obsahuje  $\theta$  a druhá  $\neg\theta$ .

Mějme dvě klauzule  $\psi_1$  a  $\psi_2$  v rezoluční relaci podle  $\theta$ , že  $\theta \in \psi_1$  a  $\neg\theta \in \psi_2$ . Rezolventa klauzulí  $\psi_1$  a  $\psi_2$  podle  $\theta$  je nová klauzule označená

$$R_\theta(\psi_1, \psi_2) = (\psi_1 \setminus \{\theta\}) \cup (\psi_2 \setminus \{\neg\theta\}).$$

Dvě klauzule  $\psi_1 = \{P_1, Q, R\}$  a  $\psi_2 = \{\neg Q, R, R_1, \neg Q_2\}$  jsou v rezoluční relaci podle  $Q$ . Jejich rezolventa vznikne tak, že z první odebereme  $Q$ , ze druhé  $\neg Q$  a zbytky sjednotíme:

$$R_Q(\psi_1, \psi_2) = \{P_1, R, R_1, \neg Q_2\}.$$

Klauzule mohou být v rezoluční relaci i podle více než jednoho literálu. Např. klauzule  $\psi_3 = \{P_1, Q, \neg R\}$  je s klauzulí  $\psi_2$  v rezoluční relaci podle  $Q$  i podle  $R$ . Můžeme vytvořit rezolventy podle každého z literálů  $Q$  a  $R$ :

$$R_Q(\psi_3, \psi_2) = \{P_1, \neg R, R, R_1, \neg Q_2\}, \quad R_R(\psi_3, \psi_2) = \{P_1, Q, \neg Q, R_1, \neg Q_2\}.$$

Pokud nastane případ, že dvojice klauzulí je  $\{P\}$  a  $\{\neg P\}$ , pak rezolventa podle  $P$  je prázdná klauzule,  $R_P(P, \neg P) = \emptyset$ . Prázdná klauzule není splnitelná. (Pozor, prázdná množina klauzulí splnitelná je!)

Nyní popíšeme postup, jak zjistit zda  $\{\varphi_1, \dots, \varphi_m\} \models \varphi$  pomocí tzv. rezoluční metody. Podle Věty 11 stačí testovat splnitelnost množiny  $\{\varphi_1, \dots, \varphi_m, \neg\varphi\}$ .

### Algoritmus rezoluční metody.

1. Všechny formule v množině  $\{\varphi_1, \dots, \varphi_m, \neg\varphi\}$  přepíšeme do CNF a vytvoříme množinu  $\Sigma = \{\psi_1, \psi_2, \dots, \psi_n\}$  klauzulí.
2. Redukce počtu klauzulí:
  - (a) Klauzule, které jsou tautologiemi, vynecháme.
  - (b) Obsahuje-li nějaká neprázdná klauzule  $\psi'$  jinou klauzuli  $\psi$ ,  $\psi' \supset \psi$ , klauzuli  $\psi'$  vynecháme.
  - (c) Obsahuje-li klauzule  $\psi$  takový literál  $\theta$ , že opačný literál  $\neg\theta$  se ve zbylých klauzulích nevyskytuje, klauzuli  $\psi$  vynecháme.
3. Zvolíme si literál  $\theta$ , podle kterého lze vytvářet rezolventy a k množině  $\Sigma$  přidáme všechny možné rezolventy podle  $\theta$ .
4. Odebereme všechny klauzule obsahující  $\theta$  nebo  $\neg\theta$ , výslednou množinu označíme jako  $\Sigma$  a vracíme se do bodu 2.

Celý proces končí vždy v bodě 3. Buď tam jako výstup celého algoritmu vznikne prázdná klauzule, což je nesplnitelná množina. V tom případě je i původní množina  $\Sigma$  nesplnitelná, a tedy  $\{\varphi_1, \dots, \varphi_m\} \models \varphi$ . Nebo už nebude existovat žádný literál, podle kterého lze dále vytvářet rezolventy. To znamená, že výstupem je splnitelná množina. Tím také  $\Sigma$  je splnitelná a  $\{\varphi_1, \dots, \varphi_m\} \not\models \varphi$ .

**Příklad.** Pomocí rezoluční metody zjistěte, zda  $Q \vee S$  je logickým důsledkem množiny  $\{P \vee Q, R \Rightarrow S, \neg P \vee S, \neg Q \vee R\}$ .

**Krok 1.** Nejprve převedeme všechny formule v množině do tvaru CNF. Kromě  $R \Rightarrow S$  už ostatní formule v požadovaném tvaru jsou, takže s využitím pravidla o eliminaci implikace píšeme

$$R \Rightarrow S \equiv \neg R \vee S.$$

Zbývá k těmto formulím přidat negaci testovaného důsledku:

$$\neg(Q \vee S) \equiv \neg Q \wedge \neg S.$$

Problem jsme redukovali na zjišťování splnitelnosti či nesplnitelnosti množiny klauzulí  $\Sigma = \{P \vee Q, \neg R \vee S, \neg P \vee S, \neg Q \vee R, \neg Q, \neg S\}$ .

**Krok 2.** Klausule  $\neg Q \vee R$  obsahuje klauzuli  $\neg Q$ . Proto klauzuli  $\neg Q \vee R$  vynecháme. Máme teď množinu

$$\Sigma = \{P \vee Q, \neg R \vee S, \neg P \vee S, \neg Q, \neg S\}.$$

V ní se vyskytuje literál  $\neg R$  bez svého protějšku  $R$ . Proto vypustíme i klauzuli  $\neg R \vee S$ . Do 3. kroku algoritmu vstupujeme s množinou

$$\Sigma = \{P \vee Q, \neg P \vee S, \neg Q, \neg S\}.$$

Další kroky jsou zachyceny v následující tabulce, kterou si vysvětlíme.

	$S$	$P$	$Q$
$P \vee Q$		1	
$\neg P \vee S$	1		
$\neg Q$			0
$\neg S$	0		
	$\neg P$	0	
		$Q$	1
			$\emptyset$

Na počátku vyplníme první sloupec tabulky zadanými klauzulemi.

**Krok 3.** Zvolíme proměnnou, podle které budeme vytvářet rezolventy. Zde jsme se rozhodli pro  $S$ . (Pro tuto volbu nebyl žádný zvláštní důvod, mohli jsme zvolit jakoukoli proměnnou  $P$ ,  $Q$ ,  $S$ .) Zvolenou proměnnou  $S$  napíšeme do druhého sloupce nahoru. V tomto sloupci vyznačíme symbolem 1 řádky s formulí obsahující  $S$ , a symbolem 0 řádky, kde je formule obsahující  $\neg S$ . Pak vytvoříme všechny rezolventy podle  $S$ , tj. všechny kombinace řádků s 0 a 1. Zde nám přibyla jedna rezolventa  $\neg P$  připsaná dolů do druhého sloupce.

**Krok 4.** Z dalšího postupu (už navždy) vyloučíme všechny formule mající na svém řádku vepsaný symbol 0 nebo 1.

Množina klauzulí vzniklá po Kroku 4 je  $\{P \vee Q, \neg Q, \neg P\}$ . S ní se vracíme do Kroku 2. Žádná redukce teď k dispozici není, proto přistupujeme ke Kroku 3.

Krok 3. Zvolili jsme proměnnou  $P$  pro vytváření rezolvent a napsali ji do třetího sloupce. Vyznačíme řádky, kde je formule obsahující  $P$  nebo  $\neg P$  symbolem 1 nebo 0 a vytvoříme všechny množné rezolventy. Zde přibyla pouze jediná rezolventa  $Q$ , která je dopsaná do třetího sloupce dolů. Krok 4 teď redukuje množinu klauzulí na  $\{\neg Q, Q\}$ . V této chvíli už vidíme, že další rezolventa bude prázdná klauzule, zadaná množina je tak nespjitelná a  $Q \vee S$  je logickým důsledkem. V tabulce je pro úplnost čtvrtý sloupec doplněn.

**Příklad.** Zjistíme, že formule  $\neg(P \vee (\neg Q \Rightarrow \neg R))$  je logický důsledek množiny  $\{S \vee (\neg Q \Rightarrow R), \neg(S \wedge \neg T), (\neg S \wedge P) \Rightarrow Q, \neg T \vee R, \neg T \Rightarrow \neg(Q \wedge R)\}$ .

**Krok 1.** Formule převedeme do tvaru CNF. (Kromě třetí formule, ta už ve tvaru CNF je.)

$$\begin{aligned} S \vee (\neg Q \Rightarrow R) &\equiv S \vee Q \vee R, \\ \neg(S \wedge \neg T) &\equiv \neg S \vee T, \\ (\neg S \wedge P) \Rightarrow Q &\equiv S \vee \neg P \vee Q, \\ \neg T \Rightarrow \neg(Q \wedge R) &\equiv T \vee \neg Q \vee \neg R. \end{aligned}$$



Zbývá převést negaci testovaného důsledku:

$$P \vee (\neg Q \Rightarrow \neg R) \models P \vee Q \vee \neg R.$$

Úlohu jsme převedli na otázku, zda je či není splnitelná množina

$$\Sigma = \{S \vee Q \vee R, \neg S \vee T, S \vee \neg P \vee Q, \neg T \vee R, T \vee \neg Q \vee \neg R, P \vee Q \vee \neg R\}.$$

**Krok 2.** Zde k žádné redukci nedochází. Přepíšeme si formule do tabulky a začneme Krok 3.

**Krok 3.** Budeme vytvářet rezolventy např. podle  $T$ . Ve sloupci s označením  $T$  máme symbolem **1** označeny řádky, kde se vyskytuje  $T$  a symbolem **0** řádky s výskytem  $\neg T$ . Rezolventa z formulí ve 2. a 4. řádku je  $\neg S \vee R$ . Tu zapíšeme dolů do druhého sloupce. Rezolventa formulí ve 4. a 5. řádku je tautologie, kterou vynecháme.

	$T$	
$S \vee Q \vee R$		x
$\neg S \vee T$	1	
$S \vee \neg P \vee Q$		x
$\neg T \vee R$	0	
$T \vee \neg Q \vee \neg R$	1	
$P \vee Q \vee \neg R$		x
	$\neg S \vee R$	

**Krok 4.** Po odebrání klauzulí obsahujících  $T$  nebo  $\neg T$  zbývá množina

$$\Sigma = \{S \vee Q \vee R, S \vee \neg P \vee Q, P \vee Q \vee \neg R, \neg S \vee R\},$$

se kterou se vracíme do Kroku 2.

Krok 2. Všimneme si, že literál  $Q$  se zde vyskytuje bez protějšku  $\neg Q$ . Formule obsahující  $Q$  můžeme vynechat. V tabulce jsou označeny x. Zbyla jediná formule  $\neg S \vee R$ , která je splnitelná. Proto  $\neg(P \vee (\neg Q \Rightarrow \neg R))$  není logický důsledek zadané množiny formulí.

Někdy v průběhu rezoluční metody k vytváření rezolvent vůbec nedojde. To když se množina klauzulí při Kroku 2 zredukuje na prázdnou množinu.

**Příklad.** Pomocí rezoluční metody zjistěte, zda  $P \Rightarrow (\neg Q \vee R)$  je logickým důsledkem množiny  $\{(R \wedge T) \Rightarrow S, S \Rightarrow (P \Leftrightarrow Q), (P \vee R) \Rightarrow S\}$ .

Převědeme všechny formule v množině do tvaru CNF a nakonec přidáme negaci testovaného závěru.

$$\begin{aligned} (R \wedge T) \Rightarrow S &\models \neg R \vee \neg T \vee S. \\ S \Rightarrow (P \Leftrightarrow Q) &\models \neg S \vee (P \Leftrightarrow Q) \\ &\models \neg S \vee ((P \Rightarrow Q) \wedge (Q \Rightarrow P)) \\ &\models \neg S \vee ((\neg P \vee Q) \wedge (\neg Q \vee P)) \\ &\models (\neg S \vee \neg P \vee Q) \wedge (\neg S \vee \neg Q \vee P). \\ (P \vee R) \Rightarrow S &\models (\neg P \wedge \neg R) \vee S \\ &\models (\neg P \vee S) \wedge (\neg R \vee S). \\ \neg(P \Rightarrow (\neg Q \vee R)) &\models \neg(\neg P \vee \neg Q \vee R) \\ &\models P \wedge Q \wedge \neg R. \end{aligned}$$

Vzniklé klauzule napíšeme do prvního sloupce tabulky a začneme s redukcí podle Kroku 2.

$\neg R \vee \neg T \vee S$	x	
$\neg S \vee \neg P \vee Q$	x	
$\neg S \vee \neg Q \vee P$	x	
$\neg P \vee S$		x
$\neg R \vee S$	x	
$P$		
$Q$		
$\neg R$		x

Klauzule  $\neg R$  z posledního řádku je obsažena v klauzulích na 1. a 5. řádku. Tyto klauzule vynecháme (naznačeno symbolem x v prvním sloupci). Klauzule  $Q$  v předposledním řádku je obsažena v klauzuli na 2. řádku. Rovněž  $P$  je částí klauzule na 3. řádku. Proto klauzule z 2. a 3. řádku také vypouštíme. Po této redukcí zbyly čtyři klauzule (nemají x v prvním sloupci). V nich se literál  $S$  vyskytuje bez svého protějšku  $\neg S$ . Klauzuli ze 4. řádku vypouštíme (naznačeno symbolem x ve druhém sloupci). Zůstala množina  $\{P, Q, \neg R\}$ . Ta je zjevně splnitelná. Můžeme však pokračovat v redukcí podle bodu 2(c) algoritmu a vynechat i klauzule  $P, Q, \neg R$ . Zbyde prázdná množina, která je vždy splnitelná. Proto  $P \Rightarrow (\neg Q \vee R)$  není důsledkem zadané množiny formulí.

Podívejme se ještě jednou na algoritmus rezoluční metody. Kroky 2 – 4 modifikují vstupní množinu klauzulí tak, že k ní přidají všechny rezolventy podle zvoleného literálu  $\theta$  a následně odstraní všechny klauzule obsahující  $\theta$  nebo  $\neg\theta$ . Abychom mohli algoritmus prohlásit za korektní, musíme ověřit, že vstupní a výstupní (tj. modifikovaná) množina klauzulí jsou ekvivalentní z hlediska splnitelnosti. Ověření korektnosti je v následující větě.

**Věta 18.** *Mějme množinu klauzulí  $\Sigma = \{\psi_1, \psi_2, \dots, \psi_n\}$  a literál  $\theta$ . Označíme si množinu*

$$\Sigma_0 := \{\psi \in \Sigma \mid \psi \text{ obsahuje } \theta \text{ nebo } \neg\theta\}.$$

*Pak  $\Sigma$  je splnitelná právě, když je splnitelná množina*

$$\tilde{\Sigma} := \Sigma \cup \{R_\theta(\psi_i, \psi_j) \mid \psi_i, \psi_j \text{ jsou v rezoluční relaci podle } \theta\} \setminus \Sigma_0.$$

**Důkaz.** Tvrzení je ve tvaru ekvivalence, musíme tak dokázat dvě implikace.

Předpokládejme, že  $\Sigma$  je splnitelná, tj. existuje pravdivostní ohodnocení  $\nu$ , ve kterém jsou všechny klauzule v  $\Sigma$  pravdivé. V prvním kroku ukážeme, že v tomto ohodnocení jsou pravdivé i všechny rezolventy podle  $\theta$ .

Mějme klauzule  $\psi_i, \psi_j \in \Sigma$ , které jsou v rezoluční relaci podle  $\theta$ :  $\theta \in \psi_i$  a  $\neg\theta \in \psi_j$ . Je-li  $\nu(\theta) = \mathbf{1}$ , pak nutně

$$\nu(\psi_j \setminus \{\neg\theta\}) = \mathbf{1},$$

neboť celá klauzule  $\psi_j$  je pravdivá v ohodnocení  $\nu$ . Tím ovšem je pravdivá i každá klauzule obsahující  $\psi_j$ , speciálně rezolventa. Je-li naopak  $\nu(\theta) = \mathbf{0}$ , musí být pravdivá klauzule  $\psi_i \setminus \{\theta\}$ , a tedy i rezolventa. Všechny rezolventy přidané k množině  $\Sigma$  jsou tak v ohodnocení  $\nu$  pravdivé. To znamená, že množina

$$\Sigma \cup \{R_\theta(\psi_i, \psi_j) \mid \psi_i, \psi_j \text{ jsou v rezoluční relaci podle } \theta\}$$

je splnitelná. Tím je splnitelná i každá její podmnožina, speciálně  $\tilde{\Sigma}$ .

Pro důkaz opačné implikace předpokládejme, že množina

$$\tilde{\Sigma} = \Sigma \cup \{R_{\theta}(\psi_i, \psi_j) \mid \psi_i, \psi_j \text{ jsou v rezoluční relaci podle } \theta\} \setminus \Sigma_{\theta}$$

je splnitelná pomocí pravdivostního ohodnocení  $\nu$ . Je důležité si všimnout, že žádná klauzule v této množině neobsahuje  $\theta$  ani  $\neg\theta$ . Naším plánem je rozšířit ohodnocení  $\nu$  i na literál  $\theta$  tak, aby se všechny klauzule v množině  $\Sigma_0$  staly pravdivými.

Podívejme se na množinu těch klauzulí  $\psi \in \Sigma_0$ , které obsahují literál  $\theta$ , ale neobsahují  $\neg\theta$ . Jestli pro všechny takové klauzule platí, že  $\nu(\psi \setminus \{\theta\}) = \mathbf{1}$ , položíme  $\nu(\theta) = \mathbf{0}$ . Tato volba zaručuje, že všechny klauzule v  $\Sigma_0$  jsou interpretovány jako pravdivé.

Zbývá možnost, že existuje nějaká klauzule  $\psi_i \in \Sigma_0$  obsahující  $\theta$  a přitom  $\nu(\psi_i \setminus \{\theta\}) = \mathbf{0}$ . V tom případě položíme  $\nu(\theta) = \mathbf{1}$ . Jak to vypadá nyní s pravdivostními hodnotami ostatních klauzulí v množině  $\Sigma_0$ ? Obsahuje-li klauzule literál  $\theta$ , je zřejmě pravdivá. V opačném případě máme klauzuli  $\psi_j \in \Sigma_0$ , která obsahuje  $\neg\theta$  (a neobsahuje  $\theta$ ). Z předpokladu víme, že rezolventa  $R_{\theta}(\psi_i, \psi_j)$  je pravdivá v ohodnocení  $\nu$ , tj. je pravdivá klauzule

$$(\psi_i \setminus \{\theta\}) \cup (\psi_j \setminus \{\neg\theta\}).$$

Protože první část pravdivá není, musí být pravdivá druhá. To však znamená, že je pravdivá i celá klauzule  $\psi_j$ . Ukázali jsme, že ohodnocení  $\nu$  lze vždy rozšířit na literál  $\theta$  tak, aby v množině  $\Sigma_0$  byly všechny klauzule pravdivé.

Protože  $\Sigma = (\Sigma \setminus \Sigma_0) \cup \Sigma_0$ , můžeme důkaz uzavřít: První množina  $\Sigma \setminus \Sigma_0$  obsahuje klauzule pravdivé v ohodnocení  $\nu$  podle předpokladu a o druhé množině  $\Sigma_0$  jsme to právě ukázali.  $\square$

## Cvičení.

(1) Rozhodněte pomocí rezoluční metody, zda platí

(a)  $\{(P \Rightarrow Q) \Rightarrow R, (P \wedge R) \Leftrightarrow S, Q \vee \neg S \vee T, T \Rightarrow (S \wedge Q \wedge R)\} \models \neg T \vee S.$

(b)  $\{P \Rightarrow (Q \wedge R), (P \vee S) \Leftrightarrow T, Q \vee \neg R \vee S, Q \Rightarrow S\} \models \neg Q \wedge R.$

(c)  $\{(P \Rightarrow Q) \Rightarrow (R \Rightarrow S), (Q \Rightarrow R) \Rightarrow (S \Rightarrow P)\} \models (R \Rightarrow (P \vee S)) \wedge ((Q \wedge R) \Rightarrow S).$

(d)  $\{(R \wedge T) \Rightarrow S, S \Rightarrow (P \Leftrightarrow Q), T \vee \neg S, (P \vee S \vee R) \Rightarrow S\} \models (P \wedge \neg Q) \Rightarrow R.$

(e)  $\{P \Rightarrow \neg(R \vee Q), (Q \wedge S) \Rightarrow \neg P, \neg S \vee R, R \Leftrightarrow \neg(P \wedge S)\} \models R \Rightarrow S.$

## Výsledky.

(1) (a) Převodem do CNF vznikne množina klauzulí

$$P \vee R, \neg Q \vee R, \neg P \vee \neg R \vee S, P \vee \neg S, R \vee \neg S, Q \vee \neg S \vee T, S \vee \neg T, Q \vee \neg T, R \vee \neg T, T, \neg S,$$

která není splnitelná.  $\neg T \vee S$  je důsledkem.

(b) Převodem do CNF vznikne množina klauzulí

$$\neg P \vee Q, \neg P \vee R, \neg P \vee T, \neg S \vee T, P \vee S \vee \neg T, Q \vee \neg R \vee S, \neg Q \vee S, \\ Q \vee \neg R,$$

která je splnitelná.  $\neg Q \wedge R$  není důsledkem.

(c) Převodem do CNF vznikne množina klauzulí

$$P \vee \neg R \vee S, \neg Q \vee \neg R \vee S, P \vee Q \vee \neg S, Q \vee R, R, R \vee \neg S, \neg P \vee Q, \\ \neg P \vee R, \neg P \vee S, Q \vee \neg S, R \vee \neg S, \neg S,$$

která není splnitelná.  $(R \Rightarrow (P \vee S)) \wedge ((Q \wedge R) \Rightarrow S)$  je důsledkem.

(d) Převodem do CNF vznikne množina klauzulí (po vypuštění tautologií)

$$\neg R \vee S \vee \neg T, \neg P \vee Q \vee \neg S, P \vee \neg Q \vee \neg S, \neg S \vee T, \neg P \vee S, \neg R \vee S, P, \\ \neg Q, \neg R,$$

která je splnitelná.  $(P \wedge \neg Q) \Rightarrow R$  není důsledkem.

(e) Převodem do CNF vznikne množina klauzulí

$$\neg P \vee \neg R, \neg P \vee \neg Q, \neg P \vee \neg Q, \neg P \vee \neg S, R \vee \neg S, P \vee R, R \vee S, R, \neg S,$$

která je splnitelná.  $R \Rightarrow S$  není důsledkem.

# Nahlédnutí do predikátové logiky.

## Abeceda a syntaxe

V této části se podíváme na rozšíření výrokové logiky, na tzv. predikátovou logiku, někdy také nazývanou logika prvního řádu.

Výroková logika, i když má zcela základní důležitost, přece jen postrádá větší výrazovou a formulační schopnost potřebnou nejen v matematice. Podívejme se například na výrok

„Za každým úspěšným mužem stojí ambiciózní žena.“

Výroková logika by poskytla pouze jeho pravdivostní hodnotu. Nás však teď nezajímá pravdivostní hodnota, ale vnitřní struktura výroku. Řekneme jej v trochu jiné formě:

„Je-li někdo úspěšným mužem, pak za ním stojí ambiciózní žena.“

Teď je jasné, že má tvar implikace. Můžeme v přeformulaci pokročit ještě dále do tvaru, který není příliš elegantní, nicméně více odhaluje logickou strukturu.

„Je-li  $x$  úspěšný muž, pak existuje ambiciózní žena  $y$ , stojící za mužem  $x$ .“

Kromě objektů označených proměnnými  $x, y$  se zde vyskytují i jejich vlastnosti: „být mužem“, „být ženou“, „být úspěšný“ a „být ambiciózní“. Dokonce zde objevíme i relaci mezi  $x, y$ , a to „objekt  $y$  stojí za objektem  $x$ “. Označíme si tyto vlastnosti:

$M(x)$	...	$x$ je muž,
$Z(x)$	...	$x$ je žena,
$U(x)$	...	$x$ je úspěšný,
$A(x)$	...	$x$ je ambiciózní,
$S(y, x)$	...	$y$ stojí za $x$ .

S tímto označením můžeme udělat další krok ve formalizaci.

„Kdykoli  $x$  splňuje  $M(x)$  a  $U(x)$ , pak existuje  $y$ , že  $Z(y)$ ,  $A(y)$  a  $S(y, x)$ .“

Zbývá nahradit slova „kdykoli“ a „existuje“. K tomu slouží tzv. kvantifikátory, obecný  $\forall$  a existenční  $\exists$ . První znamená „pro každý“ nebo „pro jakýkoli“, druhý pak „existuje“. Teď už jsme schopni přepsat původní výrok v čistě formálním tvaru:

$$\forall x (M(x) \wedge U(x) \Rightarrow \exists y Z(y) \wedge A(y) \wedge S(y, x)).$$

Vlastnosti přiřazené objektům se nazývají *predikáty*. To je nový pojem, který výroková logika nemá. Kromě predikátů je abeceda predikátové logiky rozšířena o další složky.

**Definice 19.** *Abeceda predikátové logiky je tvořena symboly uvedenými v následující tabulce.*

Symbol	Název	Význam
(, )	<i>závorky</i>	
$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$	<i>logické spojky</i>	
$\exists$	<i>existenční kvantifikátor</i>	<i>existuje ...</i>
$\forall$	<i>obecný kvantifikátor</i>	<i>pro všechny ...</i>
$x, y, z, \dots$	<i>proměnné</i>	<i>proměnné</i>
$a, b, c, \dots$	<i>konstanty</i>	<i>individuální objekty</i>
$f, g, h, \dots$	<i>funkční symboly</i>	<i>objekty</i>
$F, G, H, \dots$	<i>predikáty</i>	<i>vlastnosti objektů</i>

Podíváme se na nové prvky abecedy podrobněji. Význam kvantifikátorů je jasný z tabulky. Obecný kvantifikátor se často reprezentuje i frázemi „každý“, „jakýkoli“ nebo „kdykoli“. Existenční kvantifikátor může mít kromě významu „existuje“ i interpretaci „nějaký“ nebo „pro nějaký“.

Proměnné zastupují jednotlivé objekty. Můžeme je indexovat, např.  $x_1, x_2, \dots$ , takže jich je v principu nekonečně mnoho. Je možné také předem specifikovat, v jaké množině proměnné uvažujeme. Tato množina se pak nazývá **univerzum**. Např. řekneme-li, že univerzum je množina  $\mathbb{R}$  reálných čísel, pak všechny proměnné budou reálná čísla. Řekneme-li, že univerzum je množina všech lidí, pak proměnné  $x, y, z, \dots$  budou označovat lidi. Univerzum je definiční obor kvantifikátorů. Není-li univerzum předem určené, pak je tvořeno všemi objekty.

Některé prvky v univerzu můžeme odlišit od ostatních tím, že jim dáme specifická jména. Takové objekty se nazývají konstanty. V případě univerza  $\mathbb{R}$  to mohou být čísla  $0, \pi, e$  atd. Je-li univerzum množina lidí, pak konstanty mohou být např.  $a = \text{Julius Caesar}$  nebo  $b = \text{Ema Destinová}$  apod.

V matematice se pracuje s funkcemi. V predikátové logice se nazývají funkční symboly. Funkční symbol  $f$  o  $n$  proměnných je zobrazení

$$f: \mathcal{U}^n \longrightarrow \mathcal{U},$$

kde  $\mathcal{U}$  je univerzum. Máme-li zvoleno  $\mathcal{U} = \mathbb{R}$ , pak funkční symboly jsou např.

$$f(x) = x^2, \quad g(x, y) = x + y, \quad h(x_1, \dots, x_n) = \sqrt{x_1^2 + \dots + x_n^2}, \text{ atd.}$$

Je-li  $\mathcal{U} = \{\text{lidé}\}$ , pak  $f(x)$  může označovat otce člověka  $x$ ,  $g(x, y, z)$  nejchytřejšího z osob  $x, y, z$  apod.

O významu predikátů jsme se zmínili v souvislosti s úvodním příkladem. Setkali jsme se s predikáty  $M, Z, U$  a  $A$  jedné proměnné a predikátem  $S$  dvou proměnných. Obecně ke každému predikátu a funkčnímu symbolu je přiřazeno číslo  $n$ , tzv. arita. Udává, na kolika proměnných příslušný symbol závisí. V případě  $n = 1$  a  $n = 2$  užíváme názvy „unární“ a „binární“. Na  $n$ -ární predikát  $F$  také můžeme pohlížet jako na zobrazení,

$$F: \mathcal{U}^n \longrightarrow \{\text{výroky}\}.$$

Z toho je patrný základní rozdíl mezi funkčním symbolem a predikátem. Hodnota funkčního symbolu je vždy prvek univerza (tj. objekt), zatímco hodnota predikátu je výrok.

**Příklad.** Označme při univerzu  $\mathcal{U} = \{\text{lidé}\}$  následující konstantu, funkční symbol a predikát:

$$a = \text{Rembrandt}, \quad f(x) = \text{otec člověka } x, \quad F(x) \dots x \text{ je otcem.}$$

Pak  $f(a)$  je Rembrandtův otec a  $f(f(a))$  Rembrandtův děd z otcovy strany.  $F(a)$  je výrok „Rembrandt je otcem“ a složení  $F(f(a))$  výrok „Rembrandtův otec je otcem“. Složení v opačném pořadí  $f(F(a))$  nemá smysl, neboť by označovalo člověka, který je otcem výroku  $F(a)$ . Stejně nesmyslné je  $F(F(a))$ .

Poučení z předešlého příkladu je, že predikáty nelze dosazovat do jiných predikátů nebo do funkčních symbolů. Uvedeme si nyní přesná syntaktická pravidla pro sestavování správných formulí predikátové logiky.

**Definice 20.** *Term je buď proměnná nebo konstanta nebo  $f(t_1, \dots, t_n)$ , kde  $f$  je  $n$ -ární funkční symbol a  $t_1, \dots, t_n$  jsou termy.*

Term je ekvivalentní tomu, co jsme dříve nazývali objekt. Můžeme si povšimnout, že definice má podobnou induktivní strukturu jako Definice 2 formule ve výrokové logice. Proměnné a konstanty bychom mohli nazývat termy nultého řádu. Termy prvního řádu se sestávají z termů nultého řádu spolu s výrazy vzniklými dosazením termů nultého řádu do funkčních symbolů. A tak postupujeme dále k termům vyšších řádů.

Následující krok je definice *atomické formule*. Atomická formule hraje v predikátové logice stejnou roli jako hraje výroková proměnná ve výrokové logice.

**Definice 21.** *Mějme  $n \geq 0$ , termy  $t_1, \dots, t_n$  (ne nutně různé) a  $n$ -ární predikát  $F$ . Pak*

$$F(t_1, \dots, t_n)$$

*je atomická formule.*

Protože jsme dovolili, aby počet termů v predikátu  $F$  byl i  $n = 0$ , dostali jsme v tomto krajním případě vlastně výrokovou proměnnou. Z tohoto nadhledu můžeme výrokové proměnné považovat za atomické formule vzniklé z 0-árního predikátu.

Nyní jsme připraveni definovat formuli v predikátové logice.

**Definice 22.** *Formule predikátové logiky splňuje jeden z následujících požadavků:*

- (i) *Atomická formule je formule.*
- (ii) *Jsou-li  $\varphi$  a  $\psi$  formule, pak  $(\neg\varphi)$ ,  $(\varphi \wedge \psi)$ ,  $(\varphi \vee \psi)$ ,  $(\varphi \Rightarrow \psi)$  a  $(\varphi \Leftrightarrow \psi)$  jsou formule.*
- (iii) *Je-li  $\varphi$  formule a  $x$  proměnná, pak  $\forall x \varphi$  a  $\exists x \varphi$  jsou formule.*

Stejně jako ve výrokové logice učiníme i zde úmluvu, která zabrání nadužívání závorek. Vnější závorky psát nebudeme. K preferencím vazeb mezi logickými spojkami přidáme navíc, že kvantifikátory váží silněji než všechny ostatní logické spojky.

Poslední poznámka se týká znaménka rovnosti,  $=$ . Nepatří do abecedy predikátové logiky jak je zavedena v Definici 19. Abychom mohli rovnost užívat měli bychom si označit speciální predikát např.

$$I(x, y) \dots x \text{ a } y \text{ jsou totožné.}$$

Všude pak místo  $x = y$  psát  $I(x, y)$ . Je to jednak nepohodlné a jednak rovnítko je natolik zažitý symbol, že si ho k abecedě predikátové logiky jednoduše přidáme a budeme ho bez obav užívat.

## Cvičení.

(1) Který z následujících výrazů jsou formule predikátové logiky?

- (a)  $\forall x F(a, x)$ ,
- (b)  $\neg(\exists y G(y) \Rightarrow G(b))$ ,
- (c)  $F \wedge (x)G(x)$ ,
- (d)  $\exists x \exists x H(x, x)$ ,
- (e)  $G(a) \wedge \forall a H(a)$ ,  $a$  je konstanta,
- (f)  $\forall x \forall y \exists x (F(x, z) \Rightarrow H(y))$ ,
- (g)  $\exists F F(x, y)$ ,
- (h)  $\exists z \forall x h(x, z)$ , kde  $h(x, z)$  je funkční symbol.

## Výsledky.

- (1) (a) Je formule, jde o atomickou fomuli  $F(x, a)$  s kvantifikátorem.
- (b) Je formule, jde o negaci kvantifikované formule  $G(y) \Rightarrow G(b)$ .
- (c) Není formule, výraz  $(x)$  nemohl vzniknout povolenými operacemi.
- (d) Je formule, i když zopakování  $\exists x$  nemá příliš smysl, nicméně neporušuje pravidla Definice 22.
- (e) Není formule, kvantifikovat přes konstanty není povoleno.
- (f) Je formule, formule  $(F(x, z) \Rightarrow H(y))$  je třikrát kvantifikovaná.
- (g) Není formule, nelze kvantifikovat přes predikáty.
- (h) Není formule, neboť  $h(x, z)$  není atomická formule.

## Formalizace výroků

I v predikátové logice existuje analogie de Morganových pravidel, zde se týká záměny negace a kvantifikátoru. Je-li  $\varphi$  formule, pak

$$\neg(\forall x \varphi) \text{ je to samé jako } \exists x \neg\varphi.$$

Analogicky,

$$\neg(\exists x \varphi) \text{ je to samé jako } \forall x \neg\varphi.$$

Následuje-li několik kvantifikátorů za sebou, uvedená pravidla aplikujeme opakovaně. Např.

$$\neg(\forall x \forall y \exists z \varphi) \text{ je to samé jako } \exists x \exists y \forall z \neg\varphi.$$

Podívejme se nyní nakolik je důležité pořadí kvantifikátorů ve formuli. Jedná-li o kvantifikátory stejného typu, lze pořadí libovolně měnit.

$$\forall x \forall y F(x, y) \text{ je to samé jako } \forall y \forall x F(x, y).$$



Analogicky,

$$\exists x \exists y F(x, y) \text{ je to samé jako } \exists y \exists x F(x, y).$$

V případě různých kvantifikátorů je situace naprosto odlišná. Kromě kvantifikátorů lze totiž zaměnit i proměnné. Tím vzniknou čtyři možné kombinace a každá z nich má obecně jiný význam. Jako ilustrace poslouží následující příklad.

**Příklad.** Mějme univerzum  $\mathcal{U} = \{\text{lidé}\}$  a predikát  $O(x, y)$  s významem „ $x$  oklamal  $y$ “. Vypíšeme si všechny čtyři varianty pořadí a k nim jejich významy.

$$\begin{aligned} \forall x \exists y O(x, y) & \text{ Každý někoho oklamal.} \\ \forall y \exists x O(x, y) & \text{ Každého někdo oklamal.} \\ \exists x \forall y O(x, y) & \text{ Někdo oklamal všechny.} \\ \exists y \forall x O(x, y) & \text{ Někoho oklamali všichni.} \end{aligned}$$

Přesný význam kvantifikátoru  $\exists$  je „existuje alespoň jeden“. Často je třeba kvantifikovat také formulace „existuje právě jeden“ nebo „existuje nejvýše jeden“. Ukážeme si jakou formalizaci mají taková slovní spojení. Označme si predikátem  $V(x)$  nějakou obecnou vlastnost objektu  $x$ . Výrok „Existuje alespoň jeden objekt s vlastností  $V$ “ má jednoduchou formalizaci,

$$\exists x V(x).$$

O něco složitější je „Existuje nejvýše jeden objekt s vlastností  $V$ “. Znamená to, že buď neexistuje žádný objekt s vlastností  $V$  nebo existuje právě jeden objekt s vlastností  $V$ . Nejefektivnější způsob formalizace spočívá v tom, že vyloučíme existenci dvou *různých* objektů s vlastností  $V$ :

$$\forall x \forall y V(x) \wedge V(y) \Rightarrow (x = y).$$

A konečně „Existuje právě jeden objekt s vlastností  $V$ “ je spojení obou výše uvedených výroků:

$$\left( \exists x V(x) \right) \wedge \left( \forall x \forall y V(x) \wedge V(y) \Rightarrow (x = y) \right).$$

## Cvičení.

- (1) Formalizujte následující výroky.
  - (a) Každá věc je totožná sama se sebou.
  - (b) Nic se neliší od všeho.
  - (c) Všechno je s něčím totožné.
  - (d) Jsou-li dvě věci totožné s třetí věcí, jsou všechny tři věci identické.
  - (e) Všechny věci jsou totožné samy se sebou právě, když žádná věc se neodlišuje sama od sebe.
  - (f) Existují právě dva objekty.
- (2) Pomocí predikátu  $Z(x, y)$ : „ $x$  zná  $y$ “ formalizujete v univerzu  $\mathcal{U} = \{\text{lidé}\}$  následující výroky.

- (a) Každý někoho zná.  
 (b) Někdo zná všechny.  
 (c) Všichni znají jednoho.  
 (d) Každý zná někoho, kdo ho nezná.  
 (e) Někdo zná všechny, kteří ho znají.  
 (f) Existuje-li někdo, kdo nezná sám sebe, pak ho znají všichni ostatní.
- (3) Pomocí uvedených predikátů a funkčních symbolů formalizujte následující výroky.
- (a) Alespoň dva lidé vynalezli parní stroj. ( $C(x)$ :  $x$  je člověk,  $V(x, y)$ :  $x$  vynalezl  $y$ ,  $a$  = parní stroj.)  
 (b) Nejvýše dva lidé vynalezli parní stroj. ( $C(x)$ :  $x$  je člověk,  $V(x, y)$ :  $x$  vynalezl  $y$ ,  $a$  = parní stroj.)  
 (c) Nikdo kromě Dostojevského nenapsal „Zločin a trest“. ( $C(x)$ :  $x$  je člověk,  $N(x, y)$ :  $x$  napsal  $y$ ,  $a$  = Dostojevskij,  $b$  = Zločin a trest.)  
 (d) Nejnadanější fyzik je Einstein. ( $F(x)$ :  $x$  je fyzik,  $N(x, y)$ :  $x$  je nadanější než  $y$ ,  $e$  = Einstein.)
- (4) Pomocí uvedených predikátů formalizujte následující výroky.
- (a) Existuje věc ležící mezi libovolnými jinými věcmi. ( $M(x, z, y)$ :  $x$  leží mezi  $y$  a  $z$ .)  
 (b) Mezi každými dvěma věcmi leží opět jedna věc. ( $M(x, z, y)$ :  $x$  leží mezi  $y$  a  $z$ .)  
 (c) Mezi každými dvěma věcmi leží právě jedna věc. ( $M(x, z, y)$ :  $x$  leží mezi  $y$  a  $z$ .)  
 (d) Někdo má všechno štěstí. ( $C(x)$ :  $x$  je člověk,  $M(x, y)$ :  $x$  má  $y$ ,  $K(x)$ :  $x$  je kousek štěstí.)  
 (e) V jisté době na žádném místě nikdo nežil. ( $D(x)$ :  $x$  je doba,  $M(x)$ :  $x$  je místo,  $C(x)$ :  $x$  je člověk,  $Z(x, y, z)$ :  $x$  žil v  $y$  během  $z$ .)  
 (f) Někoho lze klamat stále, všechny lze klamat po jistou dobu, ale nelze všechny klamat stále. ( $D(x)$ :  $x$  je doba,  $C(x)$ :  $x$  je člověk,  $K(x, y, z)$ :  $x$  klame  $y$  během  $z$ .)
- (5) Pomocí uvedených predikátů a funkčních symbolů formalizujte následující výroky.
- (a) Nejvýše jeden člověk si koupí obraz od Raffaela, pokud je vůbec nějaký Raffaelův obraz na prodej. ( $C(x)$ :  $x$  je člověk,  $R(x)$ :  $x$  je Raffaelův obraz,  $P(x)$ :  $x$  je na prodej,  $K(x, y)$ :  $x$  si koupí  $y$ .)  
 (b) Kromě Bacha a Vivaldiho existuje právě jediný další barokní skladatel. ( $b$  = J. S. Bach,  $v$  = A. Vivaldi,  $B(x)$ :  $x$  je barokní skladatel.)  
 (c) Kardinál Borgia bude papežem, bude-li volit sám sebe a budou-li ho volit alespoň dva další kardinálové. ( $b$  = Alexander Borgia,  $K(x)$ :  $x$  je kardinál,  $P(x)$ :  $x$  je papež,  $V(x, y)$ :  $x$  volí  $y$ .)

- (d) Portrétoval-li vůbec někdo císaře Maxmiliána, pak to mohl být právě jediný z dvojice Tizian nebo Veronese. ( $m$  = císař Maxmilián II,  $t$  = Tizian,  $v$  = Veronese,  $P(x, y)$ :  $x$  namaloval portrét  $y$ .)
- (e) Až na dva, žádný jiný návštěvník nepřišel pozdě. ( $N(x)$ :  $x$  je návštěvník,  $P(x)$ :  $x$  přišel pozdě.)

### Výsledky.

- (1) (a)  $\forall x (x = x)$ .  
 (b)  $\forall x \exists y (x = y)$ .  
 (c) Stejně jako (b).  
 (d)  $\forall x \forall y \forall z (x = z) \wedge (y = z) \Rightarrow ((x = y) \wedge (y = z) \wedge (z = x))$ .  
 (e)  $\forall x (x = x) \Leftrightarrow \neg(\exists y \neg(y = y))$ , tj.  $\forall x (x = x) \Leftrightarrow \forall y (y = y)$ .  
 (f)  $\exists x \exists y (\neg(x = y) \wedge \forall z (z = x) \vee (z = y))$ .
- (2) (a)  $\forall x \exists y Z(x, y)$ .  
 (b)  $\exists x \forall y Z(x, y)$ .  
 (c)  $\exists x \forall y Z(y, x)$ .  
 (d)  $\forall x \exists y Z(x, y) \wedge \neg Z(z, x)$ .  
 (e)  $\exists x \forall y (\neg Z(y, x) \Rightarrow Z(x, y))$ .  
 (f)  $\forall x (\neg Z(x, x) \Rightarrow \forall y Z(y, x))$ .
- (3) (a)  $\exists x \exists y C(x) \wedge C(y) \wedge V(x, a) \wedge V(y, a) \wedge \neg(x = y)$ .  
 (b)  $\forall x \forall y \forall z C(x) \wedge C(y) \wedge C(z) \wedge V(x, a) \wedge V(y, a) \wedge V(z, a) \Rightarrow (x = y) \vee (y = z) \vee (z = x)$ .  
 (c)  $\forall x C(x) \wedge N(x, b) \Rightarrow (x = a)$ .  
 (d)  $\forall x F(x) \Rightarrow N(e, x)$ .
- (4) (a)  $\exists x \forall y \forall z M(x, y, z)$ .  
 (b)  $\forall x \forall y \exists z M(z, x, y)$ .  
 (c)  $\forall x \forall y (\exists z M(z, x, y) \wedge \forall w M(w, x, y) \Rightarrow (z = w))$ .  
 (d)  $\exists x C(x) \wedge (\forall y K(y) \Rightarrow M(x, y))$ .  
 (e)  $\exists x D(x) \wedge (\forall y \forall z C(y) \wedge M(z) \Rightarrow \neg Z(y, z, x))$ .  
 (f)  $(\exists x \forall y \exists z C(x) \wedge D(y) \wedge C(z) \wedge K(z, x, y)) \wedge (\exists x D(x) \wedge (\forall y \exists z C(y) \wedge C(z) \wedge K(z, y, x))) \wedge \neg(\forall x \forall y \exists z D(x) \wedge C(y) \wedge C(z) \wedge K(z, y, x))$ .
- (5) (a)  $\forall x (R(x) \wedge P(x) \Rightarrow (\forall y \forall z C(y) \wedge C(z) \wedge K(y, x) \wedge K(z, x) \Rightarrow (y = z)))$ .

- (b)  $B(b) \wedge B(v) \wedge \exists x (B(x) \wedge \neg(x = b) \wedge \neg(x = v) \wedge$   
 $(\forall y B(y) \Rightarrow (y = b) \vee (y = v) \vee (y = x)))$ .
- (c)  $(V(b, b) \wedge \forall x \forall y K(x) \wedge K(y) \wedge V(x, b) \wedge V(y, b) \wedge \neg(x = y)) \Rightarrow P(b)$ .
- (d)  $\forall x P(x, m) \Rightarrow ((x = t) \wedge \neg(x = v)) \vee ((\neg(x = t) \wedge (x = v)))$ .
- (e)  $\exists x \exists y N(x) \wedge N(y) \wedge P(x) \wedge P(y) \wedge \neg(x = y) \wedge$   
 $(\forall z N(z) \wedge \neg(z = x) \wedge \neg(z = y) \Rightarrow \neg P(z))$ .