3.4 Operátor *Con*

3.4.1 Množina $Con(S)$ všech sémantických důsledků množiny formulí S je definována rovností

$$Con(S) = \{\alpha \mid \alpha \text{ je formule a } S \models \alpha\}.$$

3.4.2 Tvrzení. Pro každé dvě množiny formulí S, T platí:

a) $Con(S) \neq \emptyset$.

Ano, je-li formule α tautologie, pak je sémantickým důsledkem libovolné množiny formulí S. To znamená, že $Con(S)$ obsahuje vždy alespoň všechny tautologie.

b) $S \subseteq Con(S)$.

Z 3.3.6 víme, že každá formule z množiny S je sémantickým důsledkem množiny S. Proto je $S \subseteq Con(S)$.

c) Jestliže $S \subseteq T$, pak $Con(S) \subseteq Con(T)$.

Přeformulujme toto tvrzení: Jestliže $S \subseteq T$, pak pro každou formuli φ, pro kterou $S \models \varphi$, máme také $T \models \varphi$. (Méně formálně: vyplývá-li nějaká formule z menší množiny předpokladů, vyplývá i z větší množiny předpokladů.)

Ukážeme, že pro libovolné pravdivostní ohodnocení u, ve kterém je pravdivá množina formulí T, platí $u(\varphi) = 1$. Máme pravdivostní ohodnocení u takové, že množina formulí T je pravdivá. Protože $S \subseteq T$, je v tomto ohodnocení pravdivá i množina S. Formule φ je sémantickým důsledkem S, a proto je $u(\varphi) = 1$.

d) $Con(S) = Con(Con(S))$.

Tuto vlastnost můžeme přepsat následujícím způsobem: Máme dány formule α, $\varphi_1, \varphi_2, \ldots, \varphi_k$, pro které platí

$$\{\varphi_1, \varphi_2, \ldots, \varphi_k\} \models \alpha$$

a $S \models \varphi_1, S \models \varphi_2, \ldots, S \models \varphi_k$, pak

$$S \models \alpha.$$

Uvažujme libovolné pravdivostní ohodnocení u takové, že S je pravdivá v u. Pak platí $u(\varphi_1) = 1$, $u(\varphi_2) = 1$, …, $u(\varphi_k) = 1$. To znamená, že v ohodnocení u je pravdivá celá množina $\{\varphi_1, \varphi_2, \ldots, \varphi_k\}$. Protože formule α je sémantický důsledek množiny $\{\varphi_1, \varphi_2, \ldots, \varphi_k\}$, máme $u(\alpha) = 1$.

3.4.3 Tvrzení. Pro množinu formulí S a formuli φ platí

$$S \models \varphi \quad \text{právě tehdy, když} \quad S \cup \{\neg\varphi\} \quad \text{je nesplnitelná.}$$

3.4.4 Poznámka. Je-li množina S nesplnitelná, pak $S \models \psi$ pro všechny formule ψ.

Ano, je-li množina S nesplnitelná, pak množina $S \cup \{\neg\psi\}$ je také nesplnitelná a proto podle tvrzení 3.4.3 platí $S \models \psi$.

Uvědomte si, že předcházející zdůvodnění je stejné jako bylo zdůvodnění vlastnosti 4 viz 4.

3.4.5 Věta. Pro formule φ a ψ platí

$$\varphi \models \psi \quad \text{právě tehdy, když} \quad \varphi \Rightarrow \psi \quad \text{je tautologie.}$$

3.4.6 Věta o dedukci. Pro množinu formulí S a formule φ a ψ platí

$$S \cup \{\varphi\} \models \psi \quad \text{právě tehdy, když} \quad S \models (\varphi \Rightarrow \psi).$$

3.5 Tautologická ekvivalence

Až dosud pro nás $p \wedge q$ a $q \wedge p$ byly dvě různé formule, byly to totiž různé posloupnosti znaků. Zajímá-li nás ovšem hlavně pravdivost formulí, pak se tyto dvě formule „od sebe neliší“.

3.5.1 Tautologická ekvivalence formulí. Řekneme, že formule φ a ψ jsou *tautologicky ekvivalentní* (také *sémanticky ekvivalentní*), jestliže $\varphi \models \psi$ a také $\psi \models \varphi$. Fakt, že φ a ψ jsou tautologicky ekvivalentní, označujeme $\varphi \models\!\!\!\!\models \psi$.

3.5.2 Pozorování. Formule φ a ψ jsou tautologicky ekvivalentní právě tehdy, když pro každé pravdivostní ohodnocení u platí $u(\varphi) = u(\psi)$.

3.5.3 Věta. Relace $\models\!\!\!\!\models$ na množině všech formulí $\mathcal{P}(A)$ je ekvivalence. Navíc, jsou-li α, β, γ a δ formule splňující $\alpha \models\!\!\!\!\models \beta$ a $\gamma \models\!\!\!\!\models \delta$, pak platí

1. $\neg\alpha \models\!\!\!\!\models \neg\beta$;
2. $(\alpha \wedge \gamma) \models\!\!\!\!\models (\beta \wedge \delta)$, $(\alpha \vee \gamma) \models\!\!\!\!\models (\beta \vee \delta)$,
   $(\alpha \Rightarrow \gamma) \models\!\!\!\!\models (\beta \Rightarrow \delta)$, $(\alpha \Leftrightarrow \gamma) \models\!\!\!\!\models (\beta \Leftrightarrow \delta)$.

3.5.4 Pro každé formule α, β a γ platí

1. $\alpha \wedge \alpha \models\!\!\!\!\models \alpha$, $\alpha \vee \alpha \models\!\!\!\!\models \alpha$ (idempotence $\wedge$ a $\vee$);
2. $\alpha \wedge \beta \models\!\!\!\!\models \beta \wedge \alpha$, $\alpha \vee \beta \models\!\!\!\!\models \beta \vee \alpha$ (komutativita $\wedge$ a $\vee$);
3. $\alpha \wedge (\beta \wedge \gamma) \models\!\!\!\!\models (\alpha \wedge \beta) \wedge \gamma$, $\alpha \vee (\beta \vee \gamma) \models\!\!\!\!\models (\alpha \vee \beta) \vee \gamma$ (asociativita $\wedge$ a $\vee$);
4. $\alpha \wedge (\beta \vee \alpha) \models\!\!\!\!\models \alpha$, $\alpha \vee (\beta \wedge \alpha) \models\!\!\!\!\models \alpha$ (absorpce $\wedge$ a $\vee$);
5. $\neg\neg\alpha \models\!\!\!\!\models \alpha$;
6. $\neg(\alpha \wedge \beta) \models\!\!\!\!\models (\neg\alpha \vee \neg\beta)$, $\neg(\alpha \vee \beta) \models\!\!\!\!\models (\neg\alpha \wedge \neg\beta)$ (de Morganova pravidla);
7. $\alpha \wedge (\beta \vee \gamma) \models\!\!\!\!\models (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$, $\alpha \vee (\beta \wedge \gamma) \models\!\!\!\!\models (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$ (distributivní zákony).

   Je-li navíc T libovolná tautologie a F libovolná kontradikce, pak

8. $T \wedge \alpha \models\!\!\!\!\models \alpha$, $T \vee \alpha \models\!\!\!\!\models T$, $F \wedge \alpha \models\!\!\!\!\models F$, $F \vee \alpha \models\!\!\!\!\models \alpha$;
9. $\alpha \wedge \neg\alpha \models\!\!\!\!\models F$, $\alpha \vee \neg\alpha \models\!\!\!\!\models T$.

3.5.5 Pozorování. Pro dvě formule φ a ψ platí $\varphi \models\!\mid \psi$ právě tehdy, když formule $\varphi \Leftrightarrow \psi$ je tautologie.

Vrátíme-li se k souvislosti s logickými obvody, můžeme říci, že dvě formule jsou tautologicky ekvivalentní právě tehdy, když jejich logické obvody realizují tutéž booleovskou funkci, tj. dávají stejné výstupy při stejných vstupech.

Pro pojem sémantického důsledku není v teorii logických obvodů přímý ekvivalent.

3.5.6 Booleovské funkce. *Booleovskou funkcí n* proměnných rozumíme funkci, která každé n-tici nul a jedniček přiřazuje buď nulu nebo jedničku; jedná se tedy o zobrazení $f\colon \{0,1\}^n \to \{0,1\}$. Místo booleovská funkce se často také říká *Booleova funkce*. Každé výrokové formuli odpovídá booleovská funkce — stačí se podívat na poslední sloupec pravdivostní tabulky formule. Dvě formule jsou tautologicky ekvivalentní právě tehdy, když oběma odpovídají stejné Booleovy funkce. V tomto smyslu najít „jednodušší“ formuli tautologicky ekvivalentní s danou formulí je jinak řečena úloha najít v nějakém smyslu jednodušší formuli (většinou kratší, nebo s menší hloubkou), která odpovídá stejné Booleově funkci. A to je úloha v teorii logických obvodů častá.

3.6 Další logické spojky

3.6.1 Unární logické spojky. Všechny unární Booleovy funkce (tj. Booleovy funkce jednoho argumentu) jsou dány v následující tabulce:

x	f_1	f_2	f_3	f_4
0	0	0	1	1
1	0	1	0	1

Funkce f_1 nemění svou hodnotu, je konstantní nepravda; pro nás to bude nová spojka F zvaná *kontradikce*. Obdobně funkce f_4 je konstatní pravda; pro nás to bude opět nová spojka T zvaná *tautologie*. Tyto dvě spojky, kontradikce a tautologie, mají tu vlastnost, že nezávisí na ohodnocení žádné logické proměnné (tj. závisí na „nula“ logických proměnných). Proto jim říkáme *nulární logické spojky.*

3.6.2 Binární logické spojky. Binárními booleovské funkce jsou v následující tabulce:

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

(Jestliže někomu v předcházející tabulce sloupce funkcí f_i připadají jako binární zápisy čísel 0 až 15, pak to není náhoda. Toto jsou všechny uspořádané čtveřice nul a jedniček uspořádané lexikograficky.)

Funkce f_0 je konstantní nepravda, je to kontradikce F. Obdobně poslední funkce f_{15} je tautologie T.

Funkce f_1 odpovídá formuli $x \wedge y$. Obdobně funkce f_7 odpovídá formuli $x \vee y$, funkce f_9 formuli $x \Leftrightarrow y$ a funkce f_{13} formuli $x \Rightarrow y$.

Funkce f_3 kopíruje proměnnou x, stejně tak funkce f_5 kopíruje proměnnou y. Funkce f_{10} odpovídá formuli $\neg y$. Podobně funkce f_{12} odpovídá formuli $\neg x$. Tedy se nejedná o možné „nové spojky“.

Funkce f_{11} odpovídá formuli $y \Rightarrow x$, tedy opět spojce $\Rightarrow$. Funkce f_2 a f_4 odpovídají po řadě formulím $\neg(x \Rightarrow y)$ a $\neg(y \Rightarrow x)$.

Zvláštní význam mají zbylé tři funkce f_6, f_8 a f_{14}, jimž odpovídají nové logické spojky.

3.6.3 Vylučovací nebo — XOR. Logická spojka $\oplus$, nazývaná *vylučovací nebo* (též *XOR*), je definována

$$x \oplus y \mathrel{\models\!\!\!\dashv} \neg(x \Leftrightarrow y).$$

Vylučovacímu nebo odpovídá funkce f_6.

3.6.4 Shefferův operátor — NAND. Logická spojka $|$, nazývaná *Shefferův operátor* (též *NAND*), je definována

$$x \mid y \mathrel{\models\!\!\!\dashv} \neg(x \wedge y).$$

Shefferovu operátoru odpovídá funkce f_{14}.

3.6.5 Peirceova šipka — NOR. Logická spojka $\downarrow$, nazývaná *Peirceova šipka* (též *NOR*), je definována

$$x \downarrow y \mathrel{\models\!\!\!\dashv} \neg(x \vee y).$$

Peirceově šipce odpovídá funkce f_8.