Zpracoval: hypspave@fel.cvut.cz

5. Výroková logika, formule výrokové logiky a jejich pravdivostní ohodnocení, splnitelné formule, tautologie, kontradikce, sémantický důsledek, tautologicky ekvivalentní formule. Binární relace a operace s binárními relacemi. Relace ekvivalence, třídy ekvivalence, faktorová množina. Relace uspořádání. (A7B01LOG)

I. Výroková logika.

(Výrok – tvrzení, o kterém lze rozhodnout, zda je pravdivé či nikoli.)

Výroky. Máme danou neprázdnou množinu A tzv. elementárních výroků (též jim říkáme logické nebo výrokové proměnné). Konečnou posloupnost prvků z množiny A, logických spojek a závorek nazýváme **výroková formule** (zkráceně jen formule), jestliže vznikla podle následujících pravidel:

1. Každá logická proměnná (elementární výrok) a ∈ A je výroková formule.
2. Jsou-li α,β, výrokové formule, pak $\neg\alpha$, $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha => \beta$, $(\alpha <=> \beta)$ jsou také výrokové formule.
3. Nic jiného než to, co vzniklo pomocí konečně mnoha použití bodů 1 a 2, není výroková formule.

Všechny formule, které vznikly z logických proměnných množiny A, značíme P (A).

II. Pravdivostní ohodnocení.

Pravdivostní ohodnocení je zobrazení u: P(A) -> {0; 1}, které splňuje pravidla:

(1) $\neg\alpha$ je pravdivá právě tehdy, když je α nepravdivá;
(2) $\alpha \wedge \beta$ je pravdivá právě tehdy, když α a β jsou obě pravdivé;
(3) $\alpha \vee \beta$ je nepravdivá právě tehdy, když α a β jsou obě nepravdivé;
(4) $\alpha => \beta$ je nepravdivá právě tehdy, když je pravdivá α a β nepravdivá;
(5) $\alpha <=> \beta$ je pravdivá právě tehdy, když buď obě formule α a β jsou pravdivé nebo obě jsou nepravdivé.

Pravdivostní tabulky. Vlastnosti, které pravdivostní ohodnocení musí mít, znázorňujeme též pomocí tzv. pravdivostních tabulek logických spojek. Jsou to:

α	$\neg\alpha$
0	1
1	0

α	β	$\alpha \wedge \beta$	$\alpha \vee \beta$	$\alpha \Rightarrow \beta$	$\alpha \Leftrightarrow \beta$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

III. Tautologie, kontradikce, splnitelné formule.

Formule se nazývá **tautologie**, jestliže je pravdivá ve všech pravdivostních ohodnoceních; nazývá se **kontradikce**, jestliže je nepravdivá ve všech pravdivostních ohodnoceních. Formule je **splnitelná**, jestliže existuje aspoň jedno pravdivostní ohodnocení, ve kterém je pravdivá.

IV. Tautologická ekvivalence.

Tautologická ekvivalence formulí. Řekneme, že formule φ a ψ jsou tautologicky ekvivalentní (také sémanticky ekvivalentní), jestliže pro každé pravdivostní ohodnocení u platí u(φ) = u(ψ).

Pro každé formule α, β, γ, δ platí:

- $\alpha \models\!\mid \alpha$,
- je-li $\alpha \models\!\mid \beta$, pak i $\beta \models\!\mid \alpha$,
- Je-li $\alpha \models\!\mid \beta$ a $\beta \models\!\mid \gamma$, pak i $\alpha \models\!\mid \gamma$.

Jsou-li α, β, γ a δ formule splňující $\alpha \models\!\mid \beta$ a $\gamma \models\!\mid \delta$, pak platí

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

Pro každé formule α, β, γ platí:

- $\alpha \wedge \alpha \models\!\mid \alpha$, $\alpha \vee \alpha \models\!\mid \alpha$ (idempotence $\wedge$ a $\vee$);
- $\alpha \wedge \beta \models\!\mid \beta \wedge \alpha$, $\alpha \vee \beta \models\!\mid \beta \vee \alpha$ (komutativita $\wedge$ a $\vee$);
- $\alpha \wedge (\beta \wedge \gamma) \models\!\mid (\alpha \wedge \beta) \wedge \gamma$, $\alpha \vee (\beta \vee \gamma) \models\!\mid (\alpha \vee \beta) \vee \gamma$ (asociativita $\wedge$ a $\vee$);
- $\alpha \wedge (\beta \vee \alpha) \models\!\mid \alpha$, $\alpha \vee (\beta \wedge \alpha) \models\!\mid \alpha$ (absorpce $\wedge$ a $\vee$);
- $\neg\neg\alpha \models\!\mid \alpha$;
- $\neg(\alpha \wedge \beta) \models\!\mid (\neg\alpha \vee \neg\beta)$, $\neg(\alpha \vee \beta) \models\!\mid (\neg\alpha \wedge \neg\beta)$ (de Morganova pravidla);
- $\alpha\wedge(\beta\vee\gamma) \models\!\mid (\alpha\wedge\beta)\vee(\alpha\wedge\gamma)$, $\alpha\vee(\beta\wedge\gamma) \models\!\mid (\alpha\vee\beta)\wedge(\alpha\vee\gamma)$ (distributivní zákony).
- $(\alpha \Rightarrow \beta) \models\!\mid (\neg\alpha \vee \beta)$.

Je-li navíc $\mathbf{T}$ libovolná tautologie a $\mathbf{F}$ libovolná kontradikce, pak

- $\mathbf{T} \wedge \alpha \models\!\mid \alpha$, $\mathbf{T} \vee \alpha \models\!\mid \mathbf{T}$, $\mathbf{F} \wedge \alpha \models\!\mid \mathbf{F}$, $\mathbf{F} \vee \alpha \models\!\mid \alpha$;
- $\alpha \wedge \neg\alpha \models\!\mid \mathbf{F}$, $\alpha \vee \neg\alpha \models\!\mid \mathbf{T}$.

Poznámka: Platí $\alpha \;= \beta$ právě tehdy, když $\alpha \Leftrightarrow \beta$ je tautologie.

V. Sémantický důsledek.

Splnitelná množina formulí. Řekneme, že množina formulí S je pravdivá v ohodnocení u, jestliže každá formule z S je pravdivá v u, tj. je-li u(φ) = 1 pro všechna φ ∈ S. Řekneme, že množina formulí S je splnitelná, jestliže existuje pravdivostní ohodnocení u, v němž je S pravdivá. V opačném případě se množina S nazývá nesplnitelná.

Sémantický důsledek. Řekneme, že formule φ je konsekventem, též sémantickým nebo tautologickým důsledkem množiny formulí S, jestliže φ je pravdivá v každém ohodnocení u, v němž je pravdivá S.

Fakt, že formule φ je konsekventem množiny S, označujeme S ⊨ φ. Je-li množina S prázdná, píšeme ⊨ φ místo 0⊨ φ.

Tvrzení:

1. Je-li S množina formulí a $\varphi \in S$, pak φ je konsekventem S, tj. $S \models \varphi$ pro každou $\varphi \in S$.
2. Tautologie je konsekventem každé množiny formulí S.
3. Formule φ je tautologie právě tehdy, když $\models \varphi$.
4. Každá formule je konsekventem nesplnitelné množiny formulí.
5. Máme dvě množiny formulí M a N, kde $M \subseteq N$. Pak každý konsekvent množiny M je také konsekventem množiny N, tj. je-li $M \models \varphi$, pak $N \models \varphi$.
6. Je-li φ konsekventem množiny formulí $\{\alpha_1, \ldots, \alpha_k\}$ a každá formule α_i je konsekventem množiny formulí S, pak φ je konsekventem S.

VI. Binární relace.

Relace (přesněji binární relace) z množiny A do množiny B je libovolná množina uspořádaných dvojic R ⊆ A × B. Jestliže A = B, mluvíme o relaci na množině A.

Každé zobrazení f : A -> B je relace (nebo přesněji definuje relaci); a to relace f z A do B definovaná x f y právě tehdy, když y = f(x). Ne každá relace z A do B je zobrazením množiny A do množiny B; k tomu, aby relace R byla zobrazením je třeba (a stačí), aby pro každé a ∈ A existovalo právě jedno b ∈ B takové, že a R b.

VII. Operace s relacemi.

Průnik relací, sjednocení relací a doplněk relace. Mějme dvě relace R a S z množiny A do množiny B. Pak průnikem relací R a S je relace R ∩ S; sjednocením těchto relací je relace R ∪ S; doplňkem relace R je relace R = (A × B) \ R.

Inversní relace. Mějme relaci R z množiny A do množiny B. Pak inversní relací k relaci R je relace R^{-1} z množiny B do množiny A definovaná takto: **x R^{-1} y právě tehdy, když y R x.**

Skládání relací. Mějme relaci R z množiny A do množiny B a S relaci z množiny B do množiny C. Pak složená relace R°S je relace z množiny A do množiny C definovaná předpisem:

$$a \, R \circ S \, c \quad \text{právě tehdy, když existuje } b \in B \text{ takové, že} \quad a \, R \, b \;\text{ a }\; b \, S \, c.$$

Tvrzení:

1. Skládání relací je asociativní. Přesněji, je-li R relace z množiny A do množiny B, relace S z množiny B do množiny C a relace T z množiny C do množiny D, pak platí:

$$R \circ (S \circ T) = (R \circ S) \circ T.$$

2. Skládání relací není komutativní.

VIII. Vlastnosti relací na množině.

Řekneme, že relace R na množině A je:

1. *reflexivní*, jestliže pro všechna $a \in A$ platí $a \, R \, a$;
2. *symetrická*, jestliže pro všechna $a, b \in A$ platí: je-li $a \, R \, b$, pak také $b \, R \, a$;
3. *antisymetrická*, jestliže pro všechna $a, b \in A$ platí: je-li $a \, R \, b$ a $b \, R \, a$, pak nutně $a = b$;
4. *tranzitivní*, jestliže pro všechna $a, b, c \in A$ platí: je-li $a \, R \, b$ a $b \, R \, c$, pak nutně $a \, R \, c$.

Relace ekvivalence. Relace R na množině A se nazývá ekvivalence, jestliže je reflexivní, symetrická a tranzitivní.

Třídy ekvivalence. Nechť R je ekvivalence na množině A. Třídou ekvivalence R odpovídající prvku a ∈ A nazýváme množinu R[a] ={b∈ A | $a \; R \; b$}.

Množinu všech tříd dané ekvivalence, tj. množinu {R[a] | a ∈ A} často nazýváme **faktorovou množinou** podle ekvivalence R a značíme A/R.

Nechť R je ekvivalence na množině A. Množina tříd ekvivalence má tyto vlastnosti:

1. Každý prvek $a \in A$ leží v $R[a]$ a platí rovnost $\bigcup\{R[a] \mid a \in A\} = A$.
2. Třídy ekvivalence $R[a]$ jsou po dvou disjunktní, tj. jestliže $R[a] \cap R[b] \neq \emptyset$, pak $R[a] = R[b]$.

IX. Uspořádání.

Relaci R na množině A nazveme uspořádání (částečné uspořádání), jestliže je reflexivní, antisymetrická a tranzitivní.

Největší a maximální prvek. Mějme množinu A a na ní relaci uspořádání $\preccurlyeq$.
1. Řekneme, že prvek a množiny A je největší prvek množiny A, jestliže pro všechny prvky $x \in A$ platí $x \preccurlyeq a$.
2. Řekneme, že prvek b množiny A je maximální prvek množiny A, jestliže neexistuje prvek $y \in A$, $y \neq b$, takový, že $b \preccurlyeq y$.

Tvrzení. Mějme množinu A a na ní uspořádání $\preccurlyeq$. Množina A má nejvýše jeden největší prvek; navíc, je-li a největší prvek množiny A, pak je jediným maximálním prvkem množiny A. Nemá-li množina A největší prvek, může mít několik maximálních prvků, anebo žádný.

Nejmenší a minimální prvek. Mějme množinu A a na ní relaci uspořádání $\preccurlyeq$. Řekneme, že prvek a množiny A nejmenší prvek množiny A, jestliže pro všechny prvky $x \in A$ platí $a \preccurlyeq x$. Řekneme, že prvek b množiny A je minimální prvek množiny A jestliže neexistuje prvek $y \in A$, $y \neq b$, takový, že $y \preccurlyeq b$.

Tvrzení. Mějme množinu A a na ní uspořádání $\preccurlyeq$. Množina A má nejvýše jeden nejmenší prvek. Pokud nejmenší prvek existuje, je jediným minimálním prvkem. Nemá-li množina A nejmenší prvek, může mít několik minimálních prvků, anebo žádný.

Nesrovnatelné prvky. Mějme množinu A a na ní uspořádání $\preccurlyeq$. Řekneme, že prvky $a, b \in A$ jsou nesrovnatelné, jestliže neplatí ani $a \preccurlyeq b$, ani $b \preccurlyeq a$.
Poznámka. Uvědomte si, že má-li uspořádání dva různé maximální prvky (dva různé minimální prvky), pak jsou tyto prvky nesrovnatelné.

Lineární uspořádání. Uspořádání $\preccurlyeq$ na množině A se nazývá lineární, též totální uspořádání, jestliže každé dva různé prvky jsou srovnatelné; tj. pro každé dva prvky $a, b \in A$ platí $a \preccurlyeq b$ nebo $b \preccurlyeq a$.