TEORETICKÁ INFORMATIKA 3. ČÁST

Úvod do logiky

Václav Vais

Obsah

Předmluva

Tento materiál se snaží seznámit čtenáře s elementárními principy logiky a jejich uplatněním při studiu informatických oborů. Vzhledem ke svému rozsahu si materiál neklade vyšší cíle, než zprostředkovat čtenáři **základní orientaci** v těchto okruzích:

- logická výstavba deduktivních věd,
- výroková logika a její potenciál pro řešení logických úloh a dokazování pravdivosti tvrzení,
- algebra logiky jako nástroj pro analýzu a návrh kombinačních a sekvenčních číslicových zařízení.

Materiál je určen pro studenty inženýrských, zejména informatických oborů. Text se snaží alespoň částečně kompenzovat dlouhodobý deficit ve výuce logiky na středních školách i absenci takového předmětu mezi povinými předměty ve studijních plánech většiny technických oborů na vysokých školách. Text pokrývá jeden okruh, kterému se věnuje předmět KIV/TI ve druhém ročníku bakalářského studia studijního programu Inženýrská informatika (bohužel jen v omezeném čase na konci semestru).

Stejně jako v předmluvě k předchozím dílům musím konstatovat, že **text není záznamem přednášek, rozsahem i podrobnostmi značně přesahuje objem, který obvykle bývá k danému tématu odpřednášen (a který také bývá zkoušen).**

Při tvorbě textu jsem se v teoretických partiích opět snažil neustupovat z matematické přesnosti, ale prezentované pojmy a postupy doplňovat podrobným slovním vysvětlením (tam, kde jsem to považoval za vhodné, jsem někdy přistoupil i k méně přesným, nicméně názornějším formulacím; takové formulace jsou obvykle uvedeny v uvozovkách).

U zkoušky z předmětu KIV/TI bude vyžadována znalost v rozsahu přednášek, tj. v rozsahu zveřejněných přednáškových slajdů, tedy ne v rozsahu tohoto rozšiřujícího textu. Jeho prostudováním ovšem může motivovaný student získat širší nadhled nad přednášenou problematikou. Kromě toho by měly „vysvětlující“ části textu napomoci k pochopení těch teoretických partií, které mohou být pro posluchače při dnešní úrovni obecných matematických znalostí a intenzitě návštěv kontaktních výukových akcí obtížnější.

Václav Vais
září 2019

1. Logika

1.1. Úvod

Logika je disciplína, která se zabývá metodami správného (*korektního*) usuzování, tedy způsoby vyvozování pravdivých závěrů (*důsledků*) z pravdivých (= ověřených) poznatků (předpokladů).

Logika se začala vyvíjet jako součást filosofie už v období antiky, za jejího zakladatele je považován Aristoteles ze Stageiry (384 př. n. l. – 322 př. n. l.). V současnosti je logika vnímána jako široká oblast na rozhraní filosofie a matematiky.

Logika zkoumá pouze formu sdělení, nikoli jeho obsah. Logicky správná *dedukce* představuje posloupnost kroků, z nichž každý splňuje kritéria zabezpečující, že jsou-li pravdivé předpoklady, je pravdivý i závěr. Dedukcí z malého počtu výchozích poznatků odvozujeme poznatky další. Dedukce je obecnou metodou deduktivních věd, zejména matematiky. Naproti tomu v empirických vědách se obvykle používá myšlenková metoda *indukce* (zobecňování), když se z jednotlivých poznatků (například z výsledků konkrétních měření nebo pozorování) vytvářejí obecné hypotézy.

Postupným zaváděním matematické notace do „filosofické“ logiky dospěl vývoj k **formální logice**, která definuje a studuje abstraktní odvozovací pravidla (jakési „formy úsudků“), jejichž platnost nezávisí na významu pojmů, které v nich vystupují. Formální logika tedy zkoumá obsahové logické myšlení prostřednictvím formálních logických systémů.

Otázky, jež nám formální logika pomáhá řešit: je konkrétní tvrzení pravdivé? Lze toto tvrzení dokázat? Lze toto tvrzení vyvrátit? Formální logika pracuje s pojmy *důkaz, teorie, model, bezespornost, úplnost, rozhodnutelnost*.

Dalším vývojem formální logiky se jako samostatná disciplína vyvinula **matematická logika**. Matematická logika studuje vyvozování jako práci se symboly popisujícími abstraktní matematické objekty. Cílem snah matematiků v první polovině 20. století bylo vytvořit formální jazyk, ve kterém by bylo možné zapsat libovolné matematické tvrzení, definovat způsob, jak z malé množiny předpokladů (axiomů) odvodit „celou matematiku” a moci o každém tvrzení algoritmicky rozhodnout, zda toto tvrzení platí. Až brněnský rodák Kurt Gödel v roce 1931 dokázal, že to možné není (Gödelovy věty o neúplnosti). Přesto je matematická logika cenným nástrojem, protože poskytuje jazyk pro práci s matematickými tvrzeními a postupy, jak v něm vyvozovat důsledky (tedy dokazovat matematická tvrzení).

1.2. Axiomatická výstavba formálních teorií

Axiomatická výstavba teorií je založena na *axiomech* — výchozích tvrzeních dané teorie, které se nedokazují (nepochybuje se o nich, jejich platnost se předpokládá například na základě zkušeností, výsledků experimentů, apod). Z axiomů se dedukcí odvozují další tvrzení – důsledky. Základním požadavkem kladeným na axiomy je *bezespornost* (důsledkem axiomů nesmí být současně nějaké tvrzení i jeho negace) a *nezávislost* (žádný axiom není důsledkem ostatních axiomů).

Teorie lze formalizovat, tedy popisovat pomocí symbolů. Tvrzení pak dostanou podobu *formulí.* Pravidla pro odvozování důsledků pak budou reprezentována určitými operacemi nad těmito formulemi.

Pro dokazování tvrzení ve formálních teoriích slouží *formální důkaz*. Existuje několik přístupů ke konstrukci formálních důkazů lišících se systémy pravidel použitých pro dokazování. Tyto systémy se nazývají *kalkuly* (alternativně *logické kalkuly, důkazové kalkuly, odvozovací systémy…..*).

Logický kalkul je *korektní*, pokud každé tvrzení, jež v něm lze vyvodit (tedy dokázat), je pravdivé.

Logický kalkul je *úplný*, pokud v něm každé tvrzení, jež je pravdivé, lze dokázat, a každé tvrzení, jež pravdivé není, lze vyvrátit (tedy dokázat jeho negaci). Pokud existují tvrzení, která nelze ani dokázat, ani vyvrátit, je logický kalkul *neúplný.*

V logice se rozlišují dva druhy axiomů – *logické axiomy* a *vlastní axiomy* nějaké teorie. Vlastními axiomy (někteří autoři pro ně používají termín *speciální axiomy*) je charakterizována každá konkrétní teorie. Teorie z formálního hlediska není nic jiného než množina vlastních axiomů. Požadavky, které jsou na vlastní axiomy kladeny - aby to byly syntakticky správné formule (*dobře utvořené formule*) a aby byly bezesporné. Oproti tomu logické axiomy se nevztahují přímo k žádné konkrétní teorii, ale charakterizují konkrétní logický kalkul (vyjadřují obecně platná pravidla rozumového odvozování v daném logickém systému).

1.2.1. Hierarchie logických kalkulů

Logické kalkuly lze charakterizovat podle jazykových prostředků, které používají. Obvykle jsou to logické spojky, proměnné, symboly pro funkce a relace a kvantifikátory.

Uveďme příklady typických tvrzení, s nimiž jsme se mohli setkat v průběhu středoškolského studia, aniž bychom si tehdy uvědomili jejich přímou souvislost s logickými kalkuly:

(1) Půjdou-li na večírek Martin s Petrem, nepůjde tam Lucie.

Formalizováno: $(M \wedge P) \rightarrow \neg L$,

kde *M* představuje elementární výrok *Martin půjde na večírek,*
P představuje elementární výrok *Petr půjde na večírek,*
L představuje elementární výrok *Lucie půjde na večírek,*
$\wedge$, $\rightarrow$ a $\neg$ jsou logické spojky.

(2) Existuje nejmenší přirozené číslo (= existuje přirozené číslo x takové, že pro všechna přirozená čísla y platí $x \leq y$).

Formalizováno: $\exists x \, \forall y \;\; x \leq y$,

kde x a y představují prvky z množiny přirozených čísel,
$\exists$ a $\forall$ jsou kvantifikátory,
$\leq$ je relační operátor nad množinou přirozených čísel.

(3) Princip matematické indukce (= platí-li nějaké tvrzení $V(x)$ pro $x = n_0$ a platí-li, že z platnosti tvrzení V pro obecné x vyplývá platnost tvrzení V pro $x + 1$, pak tvrzení V platí pro všechna přirozená čísla $x \geqq n_0$).

Formalizováno: $\forall V \left(V(n_0) \wedge \forall x \, (V(x) \rightarrow V(x+1)) \right) \rightarrow \forall x \, (x \geqq n_0 \rightarrow V(x))$,

kde V představuje nějaké tvrzení parametrizované přirozeným číslem (např. „součet vnitřních úhlů konvexního n-úhelníka je $(n-2) \cdot 180$ stupňů“),
n_0 je konstanta z množiny přirozených čísel (tj. nejmenší číslo, pro které tvrzení V platí),
x představuje (libovolný) prvek z množiny přirozených čísel,
$\exists$ a $\forall$ jsou kvantifikátory,
$\wedge$ a $\rightarrow$ jsou logické spojky,
$\geqq$ je relační operátor nad množinou přirozených čísel.

Porovnáme-li výše uvedené formalizace, vidíme, že tvrzení *(1)* se od ostatních odlišuje svojí formou. Nevyskytují se v něm proměnné ani kvantifikátory, předpokládáme, že tvrzení vypovídá o (jednoznačně určených) konkrétních osobách. *Atomickými formulemi* (tedy podformulemi, uvnitř nichž se nevyskytují žádné logické spojky) jsou v případě tvrzení *(1)* již dále nedělitelné elementární výroky *M , P, L*, jimž lze přiřadit pravdivostní hodnoty. Tvrzení *(1)* je formulí *výrokové logiky (výrokového počtu)*.

V tvrzeních *(2)* a *(3)* jsou již atomické formule obecnější, například $x \geqq n_0$, $V(x)$, $V(n_0)$, ve formulích se vyskytují kvantifikátory. Tvrzení vypovídají o vlastnostech obecných prvků nějakých množin, nikoli jen o konkrétních objektech.

U výše uvedených formalizovaných výroků *(2)* a *(3)* jsme čtenáři nabídli jejich konkrétní *interpretaci* (tedy přiřazení významu použitým symbolům), v našem případě určení množin, z nichž vybíráme prvky, o nichž formule vypovídá. Obecně platí, že konkrétní formuli lze interpretovat různými způsoby a lze tak získat třídu výroků, z nichž každý je buď pravdivý nebo nepravdivý. Se zapojením znalostí z vysokoškolské matematiky to můžeme ukázat na dalších příkladech:

(4) Existuje nejmenší prvek.

Formalizováno: $\exists x \, \forall \, y \;\; x \leq y$

Ve speciálním případě uvedeném výše, kdy jsme prvky x a y vybírali z množiny přirozených čísel, je tvrzení pravdivé, nejmenším přirozeným číslem je 1.

Pokud bychom ovšem prvky x a y vybírali z množiny reálných čísel, tvrzení pravdivé není, protože množina reálných čísel nemá nejmenší (ani největší) prvek.

Pokud bychom prvky x a y vybírali z nějaké částečně uspořádané množiny, závisela by pravdivost tvrzení na této konkrétní množině. Pokud by touto částečně uspořádanou množinou byl například svaz, bylo by tvrzení pravdivé, protože každý svaz má nejmenší (i největší) prvek.

(5) Formuli $(\exists F)\,\{(F(a) = b) \wedge (\forall x)\,[p(x) \rightarrow (F(x) = g(x, F(f(x))))]\}$

čteme „existuje funkce F taková, že $F(a) = b$ a pro všechna x, která splňují podmínku $p(x)$, platí $F(x) = g(x, F(f(x)))$.“

Interpretace této formule spočívá v následujícím:

ve volbě nějaké neprázdné množiny (označíme ji D),
v přiřazení některých konkrétních prvků z D symbolům a a b,
v přiřazení nějaké funkce zobrazující D do D symbolu f; $f: D \rightarrow D$, např. $y = f(x)$,
v přiřazení nějaké funkce zobrazující $D \times D$ do D symbolu g; $g: D \times D \rightarrow D$, např. $z = g(x, y)$,
v přiřazení nějaké funkce (*predikátu*) zobrazující D do množiny {PRAVDA, NEPRAVDA} symbolu p ; $p: D \rightarrow$ {PRAVDA, NEPRAVDA}.

Interpretace 1 („číselná“):

Zvolíme:

$D = N_0$ (tj. množina přirozených čísel N rozšířená o nulu),
$a = 0$, $b = 1$,
$f(x) = x - 1$ pro $x \epsilon N$ a $f(0) = 0$ (tj. $f(x)$ je funkce „předchůdce (x)“ s „ne zcela standardním“ dodefinováním „předchůdce nuly“),
$g(x, y) = x \cdot y$,
$p(x) = (x > 0)$.

Zkonkretizujme tvrzení *(5)* ve smyslu této interpretace: „existuje funkce F taková, že $F(0) = 1$ a pro všechna přirozená čísla $x > 0$ platí $F(x) = x \cdot F(x - 1)$.“

Toto tvrzení je zřejmě pravdivé, protože takovou funkcí F je například faktoriál $F(x) = x!$ Z rekurzivní definice faktoriálu víme, že $x! = x \cdot (x - 1)!$ a $0! = 1$.

Interpretace 2 („řetězcová“):

Zvolíme:

$D = \Sigma^*$ (tj. množina všech řetězců nad nějakou abecedou Σ),
$a = e$, $b = e$ (tj. a i b jsou prázdné řetězce),
$f(x) = zbytek(x)$ (tj. f je funkce „zbytek řetězce po odstranění prvního písmene zleva“ s dodefinováním $f(e) = e$),
$g(x, y) = y \cdot začátek(x)$ (operátor $\cdot$ zde představuje zřetězení řetězců, tj. g je zřetězením řetězce y s prvním písmenem řetězce x),
$p(x) = (x \neq e)$.

Zkonkretizujeme tvrzení *(5)* ve smyslu této interpretace: „existuje funkce F taková, že $F(e) = e$ a pro všechny neprázdné řetězce x platí $F(x) = F(zbytek(x)) \cdot začátek(x)$.“

Toto tvrzení je zřejmě pravdivé, protože takovou funkcí F je reverze (obrácení) řetězce $F(x) = reverze(x) = x^R$ (viz V. Vais: Teoretická informatika – 1. část Konečné automaty a regulární jazyky, kapitola 2.3). Názorně: Jak rekurzivním postupem „obrátíme“ řetězec? První písmeno dáme na konec, před něj pak „přilepíme“ převrácený zbytek.

Interpretace 3 („číselná“):

Zvolíme:

$D = N$ (tj. množina přirozených čísel N),
$a = 0$, $b = 1$,
$f(x) = x$,
$g(x, y) = y + 1$,
$p(x) = (x > 0)$.

Zkonkretizujme tvrzení *(5)* ve smyslu této interpretace: „existuje funkce F taková, že $F(0) = 1$ a pro všechna $x > 0$ platí $F(x) = F(x) + 1$“.

Toto tvrzení je ovšem evidentně nepravdivé.

Tvrzení *(2)* až *(5)* byla reprezentována formulemi *predikátového počtu*. Predikátový počet má bohatší vyjadřovací schopnosti než počet výrokový. K výrokové logice přidává kvantifikátory a vypovídá o vlastnostech *individuí*, tj. prvků z nějaké množiny (*univerza*), prostřednictvím *predikátů* (tj. funkcí zobrazujících do množiny $\{\text{PRAVDA}, \text{NEPRAVDA}\}$). V predikátové logice platí všechny vztahy výrokové logiky.

V souvislosti s predikátovou logikou hovoříme o jejím *řádu*. *Predikátová logika prvního řádu* obsahuje pouze jeden druh proměnných pro individua. Mohou jimi být přirozená čísla, množiny, prvky, apod. *Predikátová logika druhého řádu* má dva druhy proměnných. Jedny pro individua, jedny pro *množiny individuí*. Dále predikátová logika (bez ohledu na její řád) pracuje se symboly pro funkční a predikátové konstanty a funkční a predikátové proměnné (obecně *n*-ární, tj. s *n* argumenty). Analogicky existují i logiky vyšších řádů.

Ve výrokové logice i v predikátové logice prvního řádu existují dokazovací systémy, které jsou korektní a zároveň úplné (viz 1.1). Pro logiky vyšších řádů to už ale neplatí.

V dalším textu se budeme zabývat pouze výrokovou logikou, kterou ovšem informatici vnímají nejen jako nástroj pro logické odvozování a dokazování, ale v její algebraické reprezentaci i jako nenahraditelnou pomůcku při návrzích hardware číslicových systémů. Predikátovému počtu se budou věnovat jiné předměty ve studijním plánu vyšších ročníků.

1.2.2. Výroková logika

Výroková logika je formální odvozovací systém, ve kterém jsou atomickými formulemi *výrokové proměnné*.

Abeceda jazyka výrokové logiky

P označuje neprázdnou množinu symbolů, reprezentujících *výrokové proměnné* (jinak též *atomické výrokové formule, prvoformule, elementární výroky,….*).
Výrokovými spojkami jsou nazývány symboly $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.
Abecedou jazyka výrokové logiky jsou pak prvky množiny P, výrokové spojky a závorky (,).

Syntaxe formulí výrokové logiky

(*Dobře utvořené*) výrokové formule lze definovat rekurzivně:

1. Každá výroková proměnná je výroková formule.
2. Jestliže *A* a *B* jsou (libovolné dobře utvořené) výrokové formule, jsou výrokovými formulemi i formule *(A)* a *(B)* a *složené formule* $\neg A$, $\neg B$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$.
3. Neexistují žádné jiné výrokové formule

Je tedy zřejmé, že každou výrokovou formuli lze vytvořit jen konečným počtem užití pravidel 1 a 2.

Poznámka 1: Při zápisu složených formulí se obvykle dvojice vnějších závorek vynechává, např. místo $((A \wedge B) \rightarrow (B \vee C))$ pak píšeme $(A \wedge B) \rightarrow (B \vee C)$.

Poznámka 2: Od počátku svého vývoje logika zkoumala soudy ve formě implikací. Symboly výrokových spojek začaly být používány až v průběhu 19. století. Kromě symbolů $\neg$ a $\rightarrow$ byly zavedeny i ostatní spojky, a to jako zkratky:

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

Proto jsou axiomy, s nimiž pracují „klasické“ odvozovací systémy, ve tvaru implikací, zatímco ostatní výrokové spojky se při logickém odvozování spíše nepoužívají. Mají ovšem velký vý-

znam při algebraickém popisu a následné hardwarové implementaci logických funkcí (viz kapitola 1.3).

Sémantika jazyka výrokové logiky

Každé výrokové proměnné lze přiřadit pravdivostní hodnotu PRAVDA nebo NEPRAVDA (obvykle reprezentované symboly 1 a 0 nebo T - **true** a F - **false**). Výrokové proměnné obvykle interpretujeme jako elementární (tedy dále nedělitelné) výroky, tedy tvrzení, kterým lze (respektive má smysl) přiřadit pravdivostní hodnotu.

Přiřazení pravdivostních hodnot složeným formulím je jednoznačně určeno *pravdivostním ohodnocením* výrokových proměnných (a samozřejmě také významem výrokových spojek). Přiřazením konkrétního pravdivostního ohodnocení výrokovým proměnným se formule stává konkrétním výrokem s jednoznačně určenou pravdivostní hodnotou (analogie – dosadíme-li do reálné funkce *n* reálných proměnných za argumenty konkrétní reálná čísla, získáme funkční hodnotu, tedy konkrétní reálné číslo; dosadíme-li do formule za *n* výrokových proměnných konkrétní logické hodnoty (PRAVDA nebo NEPRAVDA) získáme výrok s konkrétní pravdivostní hodnotou (PRAVDA nebo NEPRAVDA)).

Poznámka: Vystupuje-li ve formuli *k* různých výrokových proměnných, bude pro tuto formuli existovat 2^k různých pravdivostních ohodnocení.

Význam výrokových spojek je definován takto:

$\neg X$ - *negace formule X* je formule, která má opačnou pravdivostní hodnotu než formule *X.* Čteme „non *X*“ , „není pravda, že *X*“.

$X \wedge Y$ - *konjunkce (logický součin) formulí X* a *Y* je formule, která je pravdivá pouze v případě, že obě formule *X* a *Y* jsou pravdivé. Ve všech ostatních případech je konjunkce nepravdivá. Čteme „*X et Y*“, „*X a zároveň Y*“.

$X \vee Y$ - *disjunkce (logický součet) formulí X* a *Y* je formule, která je pravdivá, je-li pravdivá alespoň jedna z formulí *X* , *Y*. Jsou-li obě formule *X* , *Y* nepravdivé, je nepravdivá i disjunkce. Čteme „*X vel Y*“, „*X nebo Y*“ (POZOR! Slovo *nebo* zde není chápáno ve vylučovacím smyslu!! Disjunkce je pravdivá i v případě, že jsou současně pravdivé oba operandy).

$X \rightarrow Y$ - *implikace X implikuje Y* je formule, která je nepravdivá pouze v případě, že je první formule (*předpoklad*) *X* pravdivá a druhá formule (*tvrzení*) *Y* nepravdivá. Ve všech ostatních případech je implikace pravdivá (tedy i když je nepravdivý předpoklad!!). Čteme „*z X vyplývá Y*“, „*X implikuje Y*“.

$X \leftrightarrow Y$ - *ekvivalence formulí X* a *Y* je formule, která je pravdivá pouze v případě, že obě formule *X* a *Y* jsou současně pravdivé nebo současně nepravdivé. Mají-li formule *X* a *Y* různé pravdivostní hodnoty, je ekvivalence nepravdivá. Čteme „*X právě tehdy, když Y*“.

Přehledně významy logických spojek shrnuje tabulka, která definuje pravdivostní hodnoty formulí svázaných logickými spojkami:

A	B	Negace $\neg A$	Konjunkce $A \wedge B$	Disjunkce $A \vee B$	Implikace $A \rightarrow B$	Ekvivalence $A \leftrightarrow B$
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

Klasifikace formulí výrokového počtu

Formule, která je pravdivá alespoň v jednom pravdivostním ohodnocení, se nazývá *splnitelná formule.* Pravdivostní ohodnocení, v němž je splnitelná formule pravdivá, se nazývá *model formule*. Značení: $\mathcal{M} \models A$, čteme „ohodnocení $\mathcal{M}$ je modelem formule A".

Formule, která je pravdivá ve všech pravdivostních ohodnoceních, se nazývá *tautologie* neboli *logicky pravdivá formule.* Modelem tautologie je libovolné pravdivostní ohodnocení.

Formule, která není pravdivá pro žádné pravdivostní ohodnocení, se nazývá *kontradikce* neboli *nesplnitelná formule.* Model kontradikce neexistuje.

Některé důležité tautologie:

zákon dvojí negace	$(\neg(\neg A)) \leftrightarrow A$,
obměna implikace	$(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$,
princip sporu	$\neg((\neg A) \wedge A)$,
zákon vyloučení třetího	$A \vee \neg A$,
tranzitivita implikace	$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$,
antisymetrie implikace	$((A \rightarrow B) \wedge (B \rightarrow A)) \rightarrow (A \leftrightarrow B)$,
de Morganova pravidla	$(\neg(A \wedge B)) \leftrightarrow (\neg A \vee \neg B)$,
	$(\neg(A \vee B)) \leftrightarrow (\neg A \wedge \neg B)$,
negace implikace	$(\neg (A \rightarrow B)) \leftrightarrow (A \wedge (\neg B))$.

Věta o nahrazení: Nahradíme-li v tautologii všechny výskyty některé výrokové proměnné libovolnou (ale pro všechny výskyty stejnou) formulí, vznikne tak opět tautologie.

Je zřejmé, že negací tautologie je kontradikce a naopak.

Logické vyplývání (sémantický důsledek)

Vzájemné vztahy mezi výrokovými formulemi lze zkoumat na základě jejich pravdivosti v různých pravdivostních ohodnoceních. Specifickým vztahem je důsledkový vztah, kdy platnost jedné formule „automaticky" vyplývá z platnosti formule druhé. V textu výše bylo zmíněno, že ekvivalence $A \leftrightarrow B$ je zkratka za formuli $(A \rightarrow B) \wedge (B \rightarrow A)$. Je tedy zřejmé, že ve všech ohodnoceních, kde je pravdivá ekvivalence $A \leftrightarrow B$, je pravdivá i implikace $A \rightarrow B$. Proto říkáme, že formule $A \rightarrow B$ *logicky vyplývá* z formule $A \leftrightarrow B$. Jiná terminologie: formule $A \rightarrow B$: je *sémantickým důsledkem* (alternativně *tautologickým důsledkem, konsekventem*)

formule $A \leftrightarrow B$. Obráceně tento vztah ovšem neplatí. NELZE říci „formule $A \leftrightarrow B$ logicky vyplývá z formule $A \rightarrow B$“, protože pro ohodnocení A = NEPRAVDA, B = PRAVDA je implikace $A \rightarrow B$ pravdivá, ovšem ekvivalence $A \leftrightarrow B$ pravdivá není.

Obecně: Formule K logicky vyplývá (je sémantickým důsledkem, je tautologickým důsledkem, je konsekventem) formule A právě tehdy, je-li K pravdivá ve všech modelech formule A. Značení: $A \vdash K$. Terminologie: formuli A nazýváme *antecedent,* formuli K *konsekvent*.

Je zřejmé, že tautologie T je sémantickým důsledkem libovolné formule (respektive libovolné množiny formulí včetně prázdné množiny), což značíme $\vdash T$.

Je zřejmé, že pokud platí $A \vdash B$ i $B \vdash A$, jsou formule A a B ekvivalentní, tedy $A \leftrightarrow B$.

Hilbertův odvozovací systém

Hilbertovský výrokový kalkulus je tvořen třemi logickými axiomy a odvozovacím pravidlem *modus ponens*.

Soubor logických axiomů *(soubor axiomů výrokové logiky)*:

axiom *A1*: $A \rightarrow (B \rightarrow A)$,
axiom *A2*: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$,
axiom *A3*: $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$.

kde *A, B, C* jsou libovolné výrokové formule.

Odvozovací pravidlo *modus ponens:*

z platnosti formulí A a $A \rightarrow B$ lze odvodit platnost formule B, formálně $A, A \rightarrow B \vdash B$.

Poznámky k axiomům:

Axiom A1 vyjadřuje, že je-li výrok A pravdivý, je pravdivá i libovolná implikace, jejímž je (pravdivý) výrok A důsledkem.
Axiom A2 vyjadřuje distributivnost implikace.
Axiom A3 vyjadřuje pricip nepřímého důkazu – máme-li dokázat, že z předpokladu A plyne tvrzení B, lze to učinit důkazem, že z nepravdivosti tvrzení B plyne nepravdivost předpokladu A.

Neexistuje žádná tautologie výrokového počtu, kterou by z výše uvedeného souboru axiomů nebylo možné dokázat. Systém axiomů je tedy úplný.

Uvedené logické axiomy i odvozovací pravidlo lze chápat jako vyjádření jakýchsi „principů správného uvažování“. Snadno lze ukázat, že všechny tři axiomy jsou tautologie, stejně tak i formule, vyjadřující princip odvození pomocí *modus ponens* $(A \wedge (A \rightarrow B)) \rightarrow B$.

Poznámka: Pravidlo *modus ponens* je třeba chápat takto: pro všechna ohodnocení, kde jsou současně pravdivé formule A a $A \rightarrow B$ je pravdivá i formule B. Jsou-li tedy formule A a $A \rightarrow B$ tautologie, je i formule B tautologií; obecněji - jsou-li formule A a $A \rightarrow B$ současně pravdivé na nějaké množině ohodnocení M (M je množina modelů formulí A a $A \rightarrow B$),

je pro všechna ohodnocení z množiny M pravdivá i formule *B.* Takže (bez ohledu na to, jaká je množina modelů formulí A a $A \to B$) „všude, kde jsou současně pravdivé A a $A \to B$, je pravdivá i B“ čili z (platnosti) A a $A \to B$ lze odvodit (platnost) *B.*

Omezíme-li se jen na axiomy výrokového počtu A1, A2, A3, umožňuje pravidlo *modus ponens* odvozovat tautologie (viz předchozí poznámka).

Formálním důkazem formule A nazveme takovou konečnou posloupnost formulí $A_1, A_2, A_3, \ldots, A_n$, kde je dokazovaná formule posledním členem, tedy $A = A_n$, a pro každé $i \le n$ je A_i axiom nebo je A_i odvozeno pravidlem *modus ponens* z formulí A_j, A_k, kde $j < i$, $k < i$ (obě antecedentní formule se tedy v posloupnosti musí vyskytnout před konsekventní formulí).

Ilustrační příklad (formální důkaz formule $A \to A$ deduktivním postupem):

Posloupnost formulí A_i vytvoříme takto:

$A_1 : A \to ((A \to A) \to A)$	(axiom *A1*; za *B* dosazeno $A \to A$)
$A_2 : (A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	(axiom *A2*; za *B* dosazeno $A \to A$; za *C* dosazeno *A*)
$A_3 : (A \to (A \to A)) \to (A \to A)$	(aplikace *modus ponens* na A_1, A_2)
$A_4 : A \to (A \to A)$	(axiom *A1*; za *B* dosazeno *A*)
$A_5 : A \to A$	(aplikace *modus ponens* na A_3, A_4)

Je zřejmé, že takto zkonstruovaná posloupnost formulí je (ve výše uvedeném smyslu) důkazem toho, že je formule $A \to A$ tautologií, nicméně obraty použité při vytváření této posloupnosti budou čtenářům připadat „umělé“; jen obtížně lze vysvětlit, proč byl v konkrétním kroku zvolen ten který axiom a s jakou substitucí. Dokazování složitějších formulí si lze představit jen těžko. V kapitole 1.3 poznáme, že pro dokazování formulí existují efektivnější (a „technicky uvažujícím“ jedincům bližší) metody.

(Konec ilustračního příkladu).

Tautologie jsou formule, které jsou pravdivé nikoli díky konkrétnímu pravdivostnímu ohodnocení výrokových proměnných, ale díky své struktuře. Jako takové tedy samy o sobě nic nevypovídají o realitě, kterou se nástroji logiky snažíme zkoumat. Jak tedy využít princip deduktivního odvozování při zkoumání reality?

Zkoumanou realitu popíšeme k elementárními výroky (tj. k výrokovými proměnnými). Celkem tedy bude existovat $n_0 = 2^k$ různých pravdivostních ohodnocení. Některá z těchto pravdivostních ohodnocení vyloučíme (na základě pozorování nebo experimentu např. zjistíme, že takové kombinace reálných jevů nemohou nastat). Zbyde tedy $n < n_0$ různých pravdivostních ohodnocení. Empirické poznatky pak budeme vyjadřovat množinou formulí, jež budou pravdivé ve všech n pravdivostních ohodnoceních, které jsme nevyloučili. Množinu těchto formulí budeme nazývat *teorie*, její prvky pak budeme nazývat *vlastní axiomy teorie*. Z těchto vlastních axiomů a (již dříve uvedených) tří axiomů výrokového počtu pak lze dedukcí odvozovat další platná tvrzení, tedy formule, jež budou pravdivé ve všech n uvažovaných pravdivostních ohodnoceních. Tautologická platnost, již zaručuje odvozování (výhradně) s použitím

„tautologických“ axiomů A1, A2, A3, je v tomto případě „pošpiněna“ použitím vlastních axiomů, které tautologiemi nejsou. Platnost odvozených formulí je ale zachována v tom smyslu, že jsou odvozené formule pravdivé ve všech ohodnoceních, v nichž jsou pravdivé všechny formule výchozí teorie.

Formálním důkazem formule F z teorie T nazveme takovou konečnou posloupnost formulí $A_1, A_2, A_3, \dots, A_n$, kde je dokazovaná formule posledním členem, tedy $F = A_n$, a pro každé $i \le n$ je A_i axiomem výrokového počtu nebo je vlastním axiomem teorie T nebo je A_i odvozeno pravidlem *modus ponens* z formulí A_j, A_k, kde $j < i$, $k < i$.

V dalším textu nejdříve zobecníme některé dříve uvedené pojmy a poznatky ve vztahu k množinám formulí - teoriím.

Množina formulí T je *splnitelná*, jestliže existuje pravdivostní ohodnocení $\mathcal{M}$, které je modelem všech formulí teorie T, tedy když $\exists \mathcal{M} \ \forall A \in \mathrm{T} : \ \mathcal{M} \vDash A$. Pravdivostní ohodnocení $\mathcal{M}$ pak nazýváme *modelem množiny* T. Značení: $\mathcal{M} \vDash \mathrm{T}$. Množina formulí obvykle představuje množinu vlastních axiomů, proto se často nazývá teorie.

Formule F *logicky vyplývá z množiny formulí* T právě tehdy, je-li F pravdivá ve všech modelech množiny T, tedy když $\forall \mathcal{M} : \ \mathcal{M} \vDash \mathrm{T} \rightarrow \mathcal{M} \vDash F$. Značení: $\mathrm{T} \vdash F$. Alternativní terminologie: Formule F je *tautologickým důsledkem množiny formulí* T, formule F je *sémantickým důsledkem množiny formulí* T.

Jiná (ekvivalentní) formulace pravidla *modus ponens*: Je-li T množina formulí a formule A a B takové, že $\mathrm{T} \vdash A$ a $\mathrm{T} \vdash (A \rightarrow B)$, pak $\mathrm{T} \vdash B$.

Množina formulí T je *bezesporná (konzistentní)*, jestliže neexistuje žádná formule A taková, že $\mathrm{T} \vdash A$ a současně $\mathrm{T} \vdash \neg A$. V opačném případě je množina formulí T *sporná*.

Poznámka: Jestliže existuje formule A taková, že $\mathrm{T} \vdash A$ a současně $\mathrm{T} \vdash \neg A$, znamená to dokonce, že lze z množiny formulí T dokázat LIBOVOLNOU formuli. Obecná vlastnost výrokové logiky – z nepravdivých (sporných) předpokladů lze dokázat COKOLI, elementárně to ukazuje pravdivostní tabulka implikace.

Ilustrační příklad (formální důkaz formule z množiny jiných formulí):

Dokažte, že z formulí T1 : $A \rightarrow B$ a T2 : $B \rightarrow C$ logicky vyplývá formule $A \rightarrow C$

Posloupnost formulí A_i vytvoříme takto:

$A_1 : (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$	(axiom A2)
$A_2 : (B \rightarrow C) \rightarrow (A \rightarrow (B \rightarrow C))$	(axiom A1; za A dosazeno $B \rightarrow C$; za B dosazeno A)
$A_3 : B \rightarrow C$	(vlastní axiom T2)
$A_4 : A \rightarrow (B \rightarrow C)$	(aplikace *modus ponens* na A_3, A_2)
$A_5 : (A \rightarrow B) \rightarrow (A \rightarrow C)$	(aplikace *modus ponens* na A_4, A_1)
$A_6 : A \rightarrow B$	(vlastní axiom T1)
$A_7 : A \rightarrow C$	(aplikace *modus ponens* na A_6, A_5)

Opět nezbývá než konstatovat, že tato posloupnost formulí je důkazem toho, že z formulí $A \to B$ a $B \to C$ logicky vyplývá formule $A \to C$, ovšem postup konstrukce posloupnosti formulí lze stejně jako v předchozím ilustračním příkladu označit za „nepříliš komfortní".

(Konec ilustračního příkladu).

Věta o dedukci: Jsou-li A a B výrokové formule a T množina výrokových formulí, pak $T \vdash (A \to B)$ právě tehdy, když $T \cup \{A\} \vdash B$.

Jak interpretovat větu o dedukci? Rozšíříme-li množinu formulí o předpoklad implikace, která z této množiny logicky vyplývá, pak z této (rozšířené) množiny logicky vyplývá i tvrzení té implikace. Existuje-li důkaz tvrzení $A \to B$, tak existuje i důkaz tvrzení B a naopak.

Věta o důkazu sporem: Je-li A výroková formule a T množina výrokových formulí, pak $T \vdash A$ právě, tehdy když $T \cup \{\neg A\}$ je nesplnitelná množina.

Jak interpretovat větu o důkazu sporem? Tvrzení lze dokázat tak, že vyvrátíme jeho negaci tím, že dojdeme ke sporu negace tvrzení s předpoklady.

Věta o rozboru případů: Jsou-li A a B výrokové formule a T množina výrokových formulí, pak $T \cup \{A, B\} \vdash C$ právě tehdy, když $T \cup \{A\} \vdash C$ a zároveň $T \cup \{B\} \vdash C$.

Jak interpretovat větu o rozboru případů? Je-li v předpokladech disjunkce, je třeba prověřit obě alternativy a z obou musí vyplývat závěr.

Věta o bezespornosti výrokového počtu: Je-li T množina výrokových formulí, pak T je bezesporná právě když T je splnitelná.

Logický kalkul je *rozhodnutelný*, jestliže existuje algoritmus, který o každé formuli jednoznačně rozhodne, zda je či není tautologií. Výrokový počet je rozhodnutelný, na rozdíl od predikátového počtu, který rozhodnutelný není. Pomocí nástrojů, jež přesahují rozsah tohoto textu (teorie vyčislitelnosti, Turingův stroj), lze ovšem zavést slabší pojem *parciální rozhodnutelnost* a ukázat, že predikátový počet prvního řádu je pak alespoň *parciálně rozhodnutelný*, zatímco predikátové počty vyšších řádů nejsou rozhodnutelné ani parciálně.

1.3. Algebraický přístup k výrokovému počtu

1.3.1. Logické funkce

Britský matematik George Boole (1815 – 1864) aplikoval při formalizaci procesu odvozování algebraické techniky. Booleova „algebra logiky" (*Booelova algebra*) má podobné vlastnosti jako algebraické systémy nad čísly. Zavádí logické operátory, elementárními objekty nejsou čísla, ale logické proměnné. Připomenutí z diskrétní matematiky - Booleova algebra není nic jiného než distributivní a komplementární svaz.

V dalším uvidíme, že algebraický přístup k výrokovému počtu otevírá cesty k pohodlnějšímu způsobu dokazování formulí.

Výroková formule, v níž vystupuje *k* výrokových proměnných, má pro každé z 2^k ohodnocení jednoznačně definovanou pravdivostní hodnotu. Představuje tedy (logickou) funkci o *k* (logických) proměnných. Přívlastek *logický* zde vyjadřuje fakt, že jak nezávislé proměnné, tak i hodnota funkce mohou nabývat poze dvou hodnot – NEPRAVDA nebo PRAVDA (pro zjednodušení zápisu dále už jen 0 nebo 1). Konzistentně s terminologií algebry se místo pojmu logická spojka používá pojem *logický operátor*.

Každá výroková formule *F* tedy reprezentuje funkci z množiny všech *k*-tic tvořených z prvků množiny {0,1} do množiny {0,1}, formálně tedy

$$F\colon \{0,1\}^k \to \{0,1\}, \quad \text{resp. } y = F(x_1, x_2, \ldots\ldots, x_k) \text{ nebo } \langle x_1, x_2, \ldots\ldots, x_k \rangle \mapsto y \ .$$

kde symbol $\{0,1\}^k$ představuje množinu všech pravdivostních ohodnocení nezávislých (výrokových) proměnných. Protože je definiční obor této funkce konečný (má 2^k prvků), můžeme formuli *F* reprezentovat (konečnou) tabulkou. *Pravdivostní tabulka* je jednou ze standardních reprezentací logických funkcí (a tedy i formulí výrokového počtu). Každý řádek pravdivostní tabulky odpovídá jednomu pravdivostnímu ohodnocení nezávislých proměnných. Ve sloupci jsou pak zapsány hodnoty funkce pro jednotlivá ohodnocení.

Již jsme konstatovali, že počet různých pravdivostních ohodnocení formule, tedy funkce *k* výrokových proměnných, je 2^k. Protože je konečný i obor hodnot (má 2 prvky), lze nad *k* výrokovými proměnnými zkonstruovat jen $2^{(2^k)}$ navzájem různých logických funkcí. Pro malé hodnoty *k* není obtížné všechny tyto funkce ukázat v jedné tabulce.

Všechny logické funkce jedné proměnné

A	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

Je zřejmé následující:

$f_0 = 0$ (konstantní funkce 0) $\qquad f_2 = \neg A$ (negace *A*)
$f_1 = A$ (aserce *A*) $\qquad f_3 = 1$ (konstantní funkce 1)

Všechny logické funkce dvou proměnných

A	*B*	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

Je zřejmé, že sloupce, u nichž je součet indexů roven 15, jsou „vzájemnými doplňky“ (jeden je negací druhého):

$f_0 = 0$	(konstanta 0)	$f_{15} = 1$	(konstanta 1)
$f_1 = A \wedge B$	(konjunkce)	$f_{14} = \neg(A \wedge B)$	(negace konjunkce, Shefferova fce)
$f_2 = \neg(A \rightarrow B)$	(negace implikace)	$f_{13} = A \rightarrow B$	(implikace)
$f_3 = A$	(A; *aserce A*)	$f_{12} = \neg A$	(negace A)
$f_4 = \neg(B \rightarrow A)$	(negace implikace)	$f_{11} = B \rightarrow A$	(implikace)
$f_5 = B$	(B; aserce B)	$f_{10} = \neg B$	(negace B)
$f_6 = \neg(A \leftrightarrow B)$	(nonekvivalence)	$f_9 = A \leftrightarrow B$	(ekvivalence)
$f_7 = A \vee B$	(disjunkce)	$f_8 = \neg(A \vee B)$	(negace disjunkce, Peirceova fce)

Pravdivostní tabulky se používají nejen k definici funkcí, ale i k vyhodnocování výrokových formulí. V tom případě má tabulka více sloupců, do kterých pro usnadnění výpočtu postupně vyhodnocujeme jednotlivé podformule.

Ilustrační příklad (vyhodnocení formule $F = ((A \wedge (\neg B)) \rightarrow C) \leftrightarrow (A \vee C)$ pravdivostní tabulkou):

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

Ve žlutě podbarvené části tabulky jsou zapsána všechna možná pravdivostní ohodnocení výrokových proměnných. Řádky v této části jsou vytvořeny jako binární rozvoje čísel od 0 do $2^k - 1$. Ve sloupcích v bílé části tabulky jsou pravdivostní hodnoty podformulí vyhodnocované formule. Jsou výsledkem logických operací reprezentovaných výrokovými spojkami (viz kapitola 1.2.2 , strana 10). V posledním sloupci tabulky jsou pak hodnoty formule F pro všechna pravdivostní ohodnocení. Je vidět, že formule F je splnitelná formule (ve sloupci je alespoň jedna jednička), ale není to tautologie (nejsou tam samé jedničky).

(Konec ilustračního příkladu).

1.3.2. Normální formy logických funkcí

Pro použití v aplikacích je vhodné reprezentovat logické funkce nějakým standardním způsobem. Princip takové reprezentace ukážeme na výsledku předchozího ilustračního příkladu s tím, že pro nezávislé proměnné logických funkcí budeme v následujícím textu místo velkých písmen A, B, C, …. používat v algebře běžné označení x_1, x_2, …., x_k.

Ilustrační příklad (reprezentace funkce $F(x_1, x_2, x_3)$ normálními formami):

číslo řádku	x_1	x_2	x_3	$F(x_1, x_2, x_3)$	Popis funkční hodnoty 1 pomocí konjunkce	Popis funkční hodnoty 0 pomocí disjunkce
0	0	0	0	0		$x_1 \vee x_2 \vee x_3$
1	0	0	1	1	$\neg x_1 \wedge \neg x_2 \wedge x_3$	
2	0	1	0	0		$x_1 \vee \neg x_2 \vee x_3$
3	0	1	1	1	$\neg x_1 \wedge x_2 \wedge x_3$	
4	1	0	0	0		$\neg x_1 \vee x_2 \vee x_3$
5	1	0	1	1	$x_1 \wedge \neg x_2 \wedge x_3$	
6	1	1	0	1	$x_1 \wedge x_2 \wedge \neg x_3$	
7	1	1	1	1	$x_1 \wedge x_2 \wedge x_3$	

Budeme se snažit vyjádřit formuli F z předchozího ilustračního příkladu ve formě disjunkce několika podformulí. Je zřejmé, že v tom případě formule F nabude hodnoty 1 právě tehdy, když hodnotu 1 bude mít alespoň jedna z podformulí. Podformule vytvoříme tak, že každá z nich bude popisovat právě jednu jedničku ve sloupci hodnot formule F. Například jedničku v řádku 3 popíšeme konjunktivní podformulí $F_3 = \neg x_1 \wedge x_2 \wedge x_3$ (unární operátor $\neg$ má vyšší prioritu než binární operátor $\wedge$). Tato podformule nabude hodnoty 1 právě tehdy, když mají všechny členy v konjunkci hodnotu 1, tedy při hodnotách $x_1 = 0$, $x_2 = 1$, $x_3 = 1$. Formuli F pak zapíšeme jako

$$F = F_1 \vee F_3 \vee F_5 \vee F_6 \vee F_7 =$$
$$= (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge x_3)$$

Tato forma reprezentace formule se nazývá *úplná disjunktivní normální formule (ÚDNF)*.

Analogicky vyjádříme formuli F ve formě konjunkce podformulí. V tom případě formule F nabude hodnoty 0 právě tehdy, když hodnotu 0 bude mít alespoň jedna z podformulí. Podformule vytvoříme tak, že každá z nich bude popisovat právě jednu nulu ve sloupci hodnot formule F. Například nulu v řádku 4 popíšeme disjunktivní podformulí $F_4 = \neg x_1 \vee x_2 \vee x_3$. Tato podformule nabude hodnoty 0 právě tehdy, když mají všechny členy v disjunkci hodnotu 0, tedy při hodnotách $x_1 = 1$, $x_2 = 0$, $x_3 = 0$. Formuli F pak zapíšeme jako

$$F = F_0 \wedge F_2 \wedge F_4 = (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3)$$

Tato forma reprezentace formule se nazývá *úplná konjunktivní normální formule (ÚKNF)*.

Přívlastek *úplná* vyjadřuje fakt, že se v každé podformuli vyskytují všechny proměnné x_i , a to buď „přímo" (*v* aserci) x_i nebo v negaci $\neg x_i$, tedy že každá podformule ÚDNF reprezentuje právě jednu jedničku ve sloupci funkčních hodnot v pravdivostní tabulce (respektive každá podformule ÚKNF reprezentuje právě jednu nulu).

(Přerušení ilustračního příkladu).

Poznámka 1: Pro úplné normální formy formulí někteří autoři používají termín *kanonické formy*.

Poznámka 2: Podobně jako u operátoru násobení je zvykem operátor konjunkce $\wedge$ nahrazovat tečkou nebo dokonce vynechávat, takže např. místo $(\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3)$ lze psát $\neg x_1\ x_2\ x_3 \vee x_1\ \neg x_2\ x_3$.

V dalším textu budeme používat symbol ~. Jeho význam je takový, že zápis $\sim x_i$ znamená, že se na uvedeném místě může vyskytnout buď x_i nebo $\neg x_i$.

Formule tvaru $(\sim x_1 \wedge \sim x_2 \ldots\ldots \wedge \sim x_k)$ budeme nazývat *mintermy.*
Obecnější pojem (když se v konjunkci nevyskytují všechny proměnné $\sim x_i$) – *součinový term*.

Formule tvaru $(\sim x_1 \vee \sim x_2 \ldots\ldots \vee \sim x_k)$ budeme nazývat *maxtermy*.
Obecnější pojem (když se v disjunkci nevyskytují všechny proměnné $\sim x_i$) – *součtový term*.

Je zřejmé, že formule v úplné disjunktivní normální formě je disjunkcí mintermů, zatímco formule v úplné konjunktivní normální formě je konjunkcí maxtermů.

Návrat k Ilustračnímu příkladu

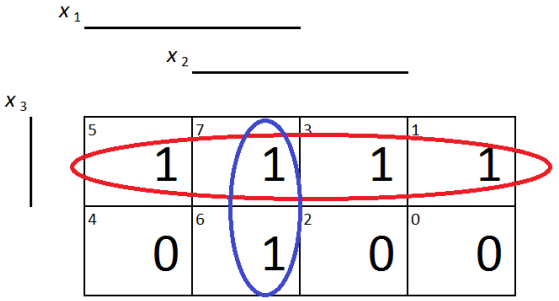
Uvažujme funkci *G* definovanou jako $G = x_3 \vee (x_1 \wedge x_2)$ a reprezentujme ji pravdivostní tabulkou:

číslo řádku	x_1	x_2	x_3	$G_1 = x_3$	$G_2 = x_1 \wedge x_2$	$G = G_1 \vee G_2$		F
0	0	0	0	0	0	0		0
1	0	0	1	1	0	1		1
2	0	1	0	0	0	0		0
3	0	1	1	1	0	1		1
4	1	0	0	0	0	0		0
5	1	0	1	1	0	1		1
6	1	1	0	0	1	1		1
7	1	1	1	1	1	1		1

Funkční hodnoty funkce *G* jsou v levém zeleném sloupci. Porovnáním s pravým zeleným sloupcem, do něhož jsme přenesli funkční hodnoty funkce *F* z předchozího příkladu, vidíme, že funkce *F* a *G* jsou ekvivalentní, jinak řečeno – formule *G* je jen jinou reprezentací funkce *F*, v našem případě dokonce v tzv. *minimální disjunktivní formě*.

Přestože mají obě formule ve sloupci hodnot pět jedniček, formule *F* (vyjádřena v ÚDNF) je disjunkcí pěti mintermů, zatímco formule *G* je disjunkcí pouze dvou součinových termů.

Smyslem *minimalizace logických funkcí* je získat podklad pro hardwarovou realizaci s co nejmenším počtem logických členů (tudíž realizaci „nejméně náročnou na finanční zdroje“). S detailnějším popisem minimalizačních metod i s různými způsoby hardwarové realizace logických funkcí budou studenti seznámeni v jiných předmětech, zvídavějšímu čtenáři ale může v tuto chvíli mnohé naznačit následující obrázek. Znázorňuje funkci *G* zapsanou v tzv. *Karnaughově mapě,* která názorně ukazuje souvislost členů disjunkce a „pokrytých jedniček“ z finálního sloupce pravdivostní tabulky funkce *G* .



$G = x_3 \vee (x_1 \wedge x_2)$

Jiný způsob reprezentace logických funkcí je pomocí seznamu indexů, pro něž funkce nabývá hodnoty 1, respektive seznamem indexů, v nichž nabývá hodnoty 0. Funkci *G* pak vyjádříme ve tvaru $G(x_1, x_2, x_2) = \Sigma\,(1,3,5,6,7)$, respektive $G(x_1, x_2, x_2) = \Pi\,(0,2,4)$.

Praktické aplikace přinášejí i to, že pro některé kombinace vstupních logických proměnných nemusí být funkční hodnota určena (nezáleží na ní – viz např. V. Vais: Teoretická informatika – 1. část Konečné automaty a regulární jazyky, kapitola 1.7). V takových případech říkáme, že je funkce *neúplná*. Je-li neúplná funkce reprezentována seznamem indexů, je výčet indexů, pro něž funkce není definována, uvozen symbolem Ø. Při minimalizaci lze pak funkci vhodně dodefinovat tak, aby měl minimalizovaný tvar co nejmenší počet termů.

1.3.3. Dokazování výrokových formulí algebraickými nástroji

V kapitole 1.2.2 jsme ukázali, že formální dokazování formulí (tedy jejich odvozování z axiomů) není jednoduché a pro většinu technicky zaměřených čtenářů to není cesta, která by je naplňovala potěšením.

V dalším si ukážeme, že formule můžeme dokazovat i algebraickými nástroji. Musíme si ovšem uvědomit jeden zásadní rozdíl: odvozováním z axiomů můžeme dostávat nové pravdivé formule, jejichž interpretací získáváme z výchozí teorie nové platné závěry. Algebraickou cestou můžeme pouze dokázat, zda nějaká formule je, či není platná (tj. zda logicky vyplývá z výchozí teorie), nejsme ovšem schopni tuto formuli odvodit (tedy „vymyslet“). Proto je odvozování z axiomů nezastupitelné, ovšem dnes má význam už jen ve formě automatických odvozovacích systémů, které jsou schopny z axiomů formalizovaných teorií odvozovat nové poznatky metodami založenými na backtrackingu.

Ilustrační příklad (důkaz, že formule $A \to B$ je sémantickým důsledkem formule $A \leftrightarrow B$):

Připomeňme, že pro to, abychom mohli konstatovat, že implikace $A \to B$ logicky vyplývá z ekvivalence $A \leftrightarrow B$, musí platit, že je implikace $A \to B$ pravdivá ve všech modelech ekvivalence $A \leftrightarrow B$. To znamená, že v pravdivostních ohodnoceních (tedy řádcích pravdivostní tabulky), kde má ekvivalence $A \leftrightarrow B$ jedničku, musí mít jedničku také implikace $A \to B$. Hodnoty obou formulí zapíšeme do společné pravdivostní tabulky:

A	B	$A \leftrightarrow B$	$A \to B$
0	0	**1**	**1**
0	1	0	1
1	0	0	0
1	1	**1**	**1**

Vidíme, že všechny (červené) jedničky ve sloupečku ekvivalence jsou „pokryty“ (modrými) jedničkami ve sloupečku implikace. Na zbývající jedničce ve sloupci implikace nezáleží. Výše uvedená tabulka tedy dokazuje, že formule $A \to B$ logicky vyplývá z formule $A \leftrightarrow B$.

(Přerušení ilustračního příkladu)

V těch pravdivostních ohodnoceních, kde je antecedent nepravdivý, na hodnotách konsekventu nezáleží. Uvědomíme-li si, že implikace je při nepravdivém předpokladu vždy pravdivá, nabízí se nám následující formulace:

Formule Y je sémantickým důsledkem formule X právě tehdy, je-li implikace $X \to Y$ tautologií, tedy její negace $X \wedge (\neg Y)$ kontradikcí.

Návrat k ilustračnímu příkladu

V následující pravdivostní tabulce je vyhodnocena implikace $X \to Y$ i její negace $X \wedge (\neg Y)$,

A	B	$A \leftrightarrow B$	$A \to B$	$\neg(A \to B)$	$(A \leftrightarrow B) \to (A \to B)$	$(A \leftrightarrow B) \wedge \neg (A \to B)$
0	0	1	1	0	1	0
0	1	0	1	0	1	0
1	0	0	0	1	1	0
1	1	1	1	0	1	0

K důkazu logického vyplývání by (samozřejmě) postačilo vyhodnocení poze jedné z formulí v zeleně podbarvených sloupcích.

Konec ilustračního příkladu

Obecněji - jak zjistit, zda formule Y logicky vyplývá z teorie $T = \{T_1, T_2, \ldots, T_n\}$? Sestrojíme formuli $(T_1 \wedge T_2 \wedge \ldots \wedge T_n) \rightarrow Y$. Je-li tato formule tautologií, je formule Y sémantickým důsledkem teorie T. Analogicky – je-li negace této formule, tedy formule $T_1 \wedge T_2 \wedge \ldots \wedge T_n \wedge (\neg Y)$ kontradikcí, je formule Y sémantickým důsledkem teorie T.

Ilustrační příklad (důkaz logického vyplývání pravdivostní tabulkou):

Dokažte, že z formulí $T_1 : A \rightarrow B$ a $T_2 : B \rightarrow C$ logicky vyplývá formule $A \rightarrow C$.

Vytvoříme formuli $F = (A \rightarrow B) \wedge (B \rightarrow C) \wedge (\neg(A \rightarrow C))$ a pravdivostní tabulkou dokážeme, že je kontradikcí (modře jsou podbarveny podformule, které se vyskytují ve výše uvedené konjunkci):

			F_1	F_2	F_3	F_4	
A	B	C	$A \rightarrow B$	$B \rightarrow C$	$A \rightarrow C$	$\neg(A \rightarrow C)$	$F = F_1 \wedge F_2 \wedge F_4$
0	0	0	1	1	1	0	0
0	0	1	1	1	1	0	0
0	1	0	1	0	1	0	0
0	1	1	1	1	1	0	0
1	0	0	0	1	0	1	0
1	0	1	0	1	1	0	0
1	1	0	1	0	0	1	0
1	1	1	1	1	1	0	0

Stejně korektním důkazem je vytvoření formule $F = ((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$ a ověření, že je tautologií:

			F_1	F_2	F_3	F_4	
A	B	C	$A \rightarrow B$	$B \rightarrow C$	$A \rightarrow C$	$F_1 \wedge F_2$	$F = F_4 \rightarrow F_3$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	1	0	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	1	0	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

Ověřování kontradikce ovšem může být pokládáno za výpočetně jednodušší, protože v řádcích, kde se nám u těch podformulí, jež se uplatňují ve výsledné konjunkci (modře podbarvené sloupce) objeví nula, nemusíme dál pokračovat ve výpočtu (jedna nula nuluje celou konjunkci), takže výsledná tabulka může vypadat takto:

			F_1	F_2	F_3	F_4	
A	B	C	$A \to B$	$B \to C$	$A \to C$	$\neg(A \to C)$	$F = F_1 \wedge F_2 \wedge F_4$
0	0	0	1	1	1	0	0
0	0	1	1	1	1	0	0
0	1	0	1	0			0
0	1	1	1	1	1	0	0
1	0	0	0				0
1	0	1	0				0
1	1	0	1	0			0
1	1	1	1	1	1	0	0

Ještě efektivnější cestou k tomu, jak dokázat, že je formule kontradikcí, může být *důkaz sporem*. Upravíme formuli F z předchozí tabulky tak, že vyjádříme negaci implikace $\neg(A \to C)$ jako $A \wedge \neg C$. Formule F tedy bude mít tvar $F = (A \to B) \wedge (B \to C) \wedge A \wedge \neg C$. Budeme předpokládat, že formule F NENÍ kontradikcí a dojdeme ke sporu s tímto předpokladem:

F NENÍ kontradikcí, existuje tedy alespoň jedno pravděpodobnostní ohodnocení, ve kterém F nabývá hodnoty 1. Všechny čtyři členy konjunkce $(A \to B)$, $(B \to C)$, A, $\neg C$ tedy v tomto pravděpodobnostním ohodnocení musí mít hodnotu 1. Tedy

4. člen $\neg C = 1$, proto $C = 0$,
3. člen $A = 1$,
1. člen $A \to B = 1$, proto (vzhledem k tomu, že $A = 1$) $B = 1$,
2. člen $B \to C = 1$, proto (vzhledem k tomu, že $B = 1$) $C = 1$ = spor s prvním řádkem

Závěr: neexistuje pravděpodobnostní ohodnocení, ve kterém by F nabyla hodnoty 1, JE to tedy kontradikce.

Konec Ilustračního příkladu

Použitá literatura

Janák, Vl.: Základy formální logiky, SPN 1976.

Gregor, P.: Výroková a predikátová logika – I
http://ktiml.mff.cuni.cz/~gregor/logika/VPL01.pdf

Kučera, A.: Matematická logika
https://www.fi.muni.cz/usr/kucera/teaching/logic/log.pdf

Manna, Z.: Matematická teorie programů. SNTL 1981.

Pajas, P.: Základy logiky a teorie množin
http://pajas.matfyz.cz/vyuka