Výroková logika

- teorie logických spojek chápaných jako pravdivostní funkce
- zabývá se způsoby tvoření výroků pomocí spojek a vztahy mezi pravdivostí různých výroků
- používá specifický jazyk složený z výrokových symbolů, logických spojek a závorek

Základní pojmy – výrok

- *výrok*: tvrzení nebo jazykový výraz, o jehož (ne)pravdivosti lze uvažovat
- syntaktická klasifikace výroků:
  - *jednoduchý výrok*: neobsahuje žádnou logickou spojku (žádná jeho vlastní část není výrokem);
    příklad: *prší*
  - *složený výrok*: obsahuje alespoň jednu logickou spojku;
    příklad: *není pravda, že prší* (vlastní část *prší* je jednoduchým výrokem, *není pravda, že* je logickou spojkou)

Výrok – příklady

- příklady výroků:
  - *je pět hodin*
  - $2 + 3 = 5$
  - *pokud nenapíšeš úkoly a neuklidíš, nepůjdeme do kina*
- příklady výrazů, které nejsou výroky:
  - *kolik je hodin?*
  - $2 + 3$
  - *napiš úkoly a ukliď*

Základní pojmy – pravdivostní funkce

- *(n-ární) pravdivostní funkce*: funkce přiřazující n-ticím pravdivostních hodnot některou pravdivostní hodnotu *pravda* (1, true apod.) nebo *nepravda* (0, false apod.)
- příklad: označme funkci dvou argumentů v přirozeném jazyce *a*; definujme ji tak, že její hodnota bude 1 (pravda) v případě, že oba argumenty (výroky) budou pravdivé. V ostatních případech (alespoň jeden argument bude nepravdivý) bude hodnota této funkce 0.
  Petr je doma a Pavel odjel na hory.
  Jsou-li výroky *Petr je doma* i *Pavel odjel na hory* pravdivé, pak hodnota funkce *a* je v tomto případě 1. Pokud je například výrok *Pavel odjel na hory* nepravdivý, je hodnota funkce 0.

Spojky výrokové logiky I

- pravdivostní hodnota složeného výroku je jednoznačně dána pravdivostními hodnotami jeho složek
- n-ární spojka je funkcí přiřazující uspořádané n-tici pravdivostních hodnot určitou pravdivostní hodnotu
- počet všech různých argumentů (uspořádaných n-tic) je vzhledem ke dvěma pravdivostním hodnotám roven 2^n

  Př.: možné argumenty pro unární funkce ($n = 1$) jsou uspořádané ”jednice” $(1), (0)$; jejich počet je $2^1 = 2$. Pro binární funkce ($n = 2$) existují čtyři ($2^2 = 4$) možné argumenty – uspořádané dvojice $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$. Pro ternární funkce existuje osm možných argumentů atd.

Spojky výrokové logiky II

- každou n-ární spojku jako totální pravdivostní funkci lze zadat *pravdivostní tabulkou* o 2^n řádcích – každému možnému argumentu (uspořádané n-tici) je přiřazena nějaká pravdivostní hodnota

  Př.: p, q – symboly reprezentující argumenty, F – definovaná spojka

p	q	F
1	1	0
1	0	1
0	1	1
0	0	0

- počet vzájemně různých n-árních spojek je 2^{2^n}; unární jsou čtyři, binárních je 16, ternárních 256 atd.

Nulární a unární výrokové spojky

- nulární pravdivostní funkce (nezávislé na žádném argumentu) jsou konstanty odpovídající pravdivostním hodnotám 0, 1
- unární (jednoargumentové) spojky:

p	F_1	F_2	F_3	F_4
1	1	1	0	0
0	1	0	1	0

Uvedené spojky nazýváme takto:

F_1 – unární verum,

F_2 – unární projekce p,

F_3 – negace p (ozn. $\neg p$); jediná netriviální unární funkce

F_4 – unární falsum.

Binární výrokové spojky $\vee, \wedge$

- $\vee$ – disjunkce (alternativa; a nebo, OR)
  $\wedge$ – konjunkce (a zároveň, AND)

p	q	$\vee$	$\wedge$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

- běžně se používá infixový zápis (např. $p \vee q$)
- spojky $\wedge, \vee$ jsou komutativní – hodnota funkce nezávisí na pořadí argumentů

Binární výrokové spojky $\Rightarrow, \Leftrightarrow$

- $\Rightarrow$ – implikace (jestliže p, pak q; předpoklad $\Rightarrow$ důsledek)
  $\Leftrightarrow$ – ekvivalence (právě tehdy, když; iff – if and only if)

p	q	$\Rightarrow$	$\Leftrightarrow$
1	1	1	1
1	0	0	0
0	1	1	0
0	0	1	1

- $\Leftrightarrow$ je komutativní, $\Rightarrow$ ne
- $p \Rightarrow q$: inverzní $\neg p \Rightarrow \neg q$, konverzní $q \Rightarrow p$, kontrapozitivní $\neg q \Rightarrow \neg p$

Další binární výrokové spojky

- spojky zajímavé z informatického hlediska:
  - XOR – nonekvivalence, negace ekvivalence (nebo ve vylučovacím smyslu; eXclusive OR)
  - negace konjunkce (Shefferova funkce, NAND)
  - negace disjunkce (Nicodova funkce, NOR)
- další spojky:
  - negace implikace (inhibice)
  - binární verum a falsum
  - binární projekce p, q a jejich negací
  - opačná (konverzní; $q \Rightarrow p$) implikace a její negace

Symbolický jazyk výrokové logiky

- *abeceda*
  1. výrokové symboly: $p, q, r, s, \ldots$, případně $p_1, p_2, p_3 \ldots$
  2. symboly pro spojky: $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$
  3. pomocné symboly: $($, $)$
- *správně utvořená formule* (dále jen formule)
  1. každý výrokový symbol je formule (tzv. *atomická formule*)
  2. je-li výraz A formule, pak $\neg(A)$ je formule
  3. jsou-li výrazy A, B formule, pak také $(A) \vee (B)$, $(A) \wedge (B)$, $(A) \Rightarrow (B)$, $(A) \Leftrightarrow (B)$ jsou formule
  4. nic jiného není formule
- závorková konvence: závorky lze vynechat, pokud to není na újmu jednoznačnosti formule

Jazyk výrokové logiky – příklady

Příklad 1:

- výrazy p, q, r jsou formulemi dle bodu 1 definice formule
- výrazy $\neg p, \neg\neg q$ jsou formulemi dle bodu 2 (a závorkové konvence)
- $p \wedge q, \neg\neg q \vee r, \neg p \Rightarrow r$ jsou formulemi dle bodu 3
- $(p \wedge q) \Rightarrow (\neg\neg q \vee r)$ je formulí dle bodu 3
- $((p \wedge q) \Rightarrow (\neg\neg q \vee r)) \Leftrightarrow (\neg p \Rightarrow r)$ je rovněž formulí dle bodu 3

Příklad 2:

- výrazy $pqr, \Leftrightarrow r, p\vee$ nejsou formulemi

Reprezentace výroků v přirozeném jazyce

Příklad:

- věta: *Pokud rychle napíšeš úkoly a venku bude hezky, půjdeme na procházku nebo pojedeme na koupaliště.*
- označení jednoduchých výroků výrokovými symboly:
  p – *rychle napíšeš úkoly*
  q – *venku bude hezky*
  r – *půjdeme na procházku*
  s – *pojedeme na koupaliště*
- reprezentace v symbolickém jazyce: $(p \wedge q) \Rightarrow (r \vee s)$
- poznámka: převod nemusí být vždy jednoznačný

Sémantika výrokové logiky

- *Pravdivostní ohodnocení (interpretace)* je funkce přiřazující všem atomickým formulím dané úvahy pravdivostní hodnoty (tj. každému výrokovému symbolu přiřadí 0 nebo 1). *Valuace* je rozšíření interpretace z atomických na všechny formule dle tabulky pro výrokové spojky (přiřadí 0 nebo 1 např. i $p \wedge \neg q$).
- Interpretace I *splňuje formuli* A (formule je *pravdivá* v I, resp. odpovídající valuace $I'(A) = 1$), pokud
  1. A je výrokový symbol a $I(A) = 1$
  2. A je $\neg B$ a I nesplňuje B, resp. $I'(B) = 0$
  3. A je tvaru $B \wedge C$ a I splňuje B i C, resp. $I'(B) = I'(C) = 1$
  4. A je $B \vee C$ a I splňuje B nebo C, resp. $I'(B) = 1$ nebo $I'(C) = 1$
  5. A je tvaru $B \Rightarrow C$ a I nesplňuje B nebo splňuje C, resp. $I'(B) = 0$ nebo $I'(C) = 1$
  6. A je $B \Leftrightarrow C$ a I splňuje B i C nebo I nesplňuje B i C, resp. $I'(B) = I'(C)$

Interpretace – příklady I

Příklad 1:

Mějme formuli $((p \wedge q) \Rightarrow (\neg\neg q \vee r)) \Leftrightarrow (\neg p \Rightarrow r)$ a následující interpretaci I: $I(p) = 1, I(q) = 0, I(r) = 1$

- dle bodu 1 I splňuje p a r, nesplňuje q
- dle bodu 2 I nesplňuje $\neg\neg q$ a $\neg p$
- dle bodu 3 I nesplňuje $p \wedge q$
- dle bodu 4 I splňuje $\neg\neg q \vee r$
- dle bodu 5 I splňuje $\neg p \Rightarrow r$ a $(p \wedge q) \Rightarrow (\neg\neg q \vee r)$
- dle bodu 6 I splňuje $((p \wedge q) \Rightarrow (\neg\neg q \vee r)) \Leftrightarrow (\neg p \Rightarrow r)$

Interpretace – příklady II

Příklad 2a:

Mějme formuli $(\neg p \wedge q) \Rightarrow p$ a interpretaci I: $I(p) = 0, I(q) = 1$

- dle bodu 1 I splňuje q a nesplňuje p
- dle bodu 2 I splňuje $\neg p$
- dle bodu 3 I splňuje $\neg p \wedge q$
- dle bodu 5 I nesplňuje $(\neg p \wedge q) \Rightarrow p$

Příklad 2b:

Mějme tutéž formuli a jinou interpretaci I_1: $I_1(p) = 1, I_1(q) = 0$

- dle bodu 1 I_1 splňuje p a nesplňuje q
- dle bodu 2 I_1 nesplňuje $\neg p$
- dle bodu 3 I_1 nesplňuje $\neg p \wedge q$
- dle bodu 5 I_1 splňuje $(\neg p \wedge q) \Rightarrow p$

Modely, logické vyplývání

- Mějme formuli $\neg p \vee p$; všechny možné interpretace (existují dvě: $I(p) = 1, I_1(p) = 0$) splňují tuto formuli.
  Formule, která je splňována každou interpretací, se nazývá *tautologie*.
- Formule $\neg p \wedge p$ není splňována žádnou z možných interpretací; takové formule nazýváme *kontradikce*.
- Formule A je *splnitelná*, je-li splňována alespoň jednou interpretací. Tuto interpretaci označujeme jako *model* formule A.
- Množina formulí $\mathbf{T}$ je splnitelná, pokud existuje interpretace splňující každou formuli z $\mathbf{T}$. Tuto interpretaci nazýváme *modelem množiny* $\mathbf{T}$.
- Formule A *logicky vyplývá* (na základě výrok. logiky) z množiny $\mathbf{T}$, pokud pro každý model I množiny $\mathbf{T}$ I splňuje A. Zapisujeme $\mathbf{T} \models A$.

Tautologie

- symbolický zápis $\models A$ (logicky vyplývají z prázdné množiny formulí)
- tautologií existuje nekonečně mnoho

Přehled vybraných tautologií I

- tautologie s jediným výrokovým symbolem:

  $p \Rightarrow p$ (zákon totožnosti)

  $p \vee \neg p$ (zákon vyloučení třetího)

  $\neg(p \wedge \neg p)$ (zákon sporu)

  $p \Leftrightarrow \neg\neg p$ (zákon dvojí negace)

- některé zobrazovací tautologie:

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

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

  $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$

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

Přehled vybraných tautologií II

- algebraicko-logické zákony:

  komutativní:

  $(p \wedge q) \Leftrightarrow (q \wedge p)$

  $(p \vee q) \Leftrightarrow (q \vee p)$

  $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$

  asociativní:

  $((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$

  $((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$

  $((p \Leftrightarrow q) \Leftrightarrow r) \Leftrightarrow (p \Leftrightarrow (q \Leftrightarrow r))$

  distributivní:

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

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

Přehled vybraných tautologií III

- charakteristiky implikace:

  $p \Rightarrow (q \Rightarrow p)$ (z. simplifikace)

  $(p \wedge \neg p) \Rightarrow q$

  $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ (z. kontrapozice)

  $(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow ((p \wedge q) \Rightarrow r)$ (slučování premis)

  $(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow (q \Rightarrow (p \Rightarrow r))$ (záměna premis)

  $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Leftrightarrow (p \Rightarrow r)$ (tranzitivita)

- transformační tautologie:

  idempotence:

  $(p \wedge p) \Leftrightarrow p$; $(p \vee p) \Leftrightarrow p$

  absorbce:

  $(p \wedge (p \vee q)) \Leftrightarrow p$; $(p \vee (p \wedge q)) \Leftrightarrow p$

  de Morganovy zákony:

  $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q);\ \neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$

Některé vlastnosti tautologií I

- **Věta o implikaci** (sémantický modus ponens): jsou-li formule A a $A \Rightarrow B$ tautologie, pak i B je tautologie.
  Důkaz: sporem. Nechť platí $\models A$ a $\models A \Rightarrow B$. Nechť existuje interpretace I (pro výr. symboly z A a B) nesplňující B (tj. B není tautologie). I splňuje A (protože A je tautologie). Tedy I nesplňuje $A \Rightarrow B$, neboť splňuje A a nesplňuje B. Dostáváme spor s předpokladem, že $A \Rightarrow B$ je tautologie.
  Pozn.: věta umožňuje získat z tautologií daného tvaru další tautologie.

- aplikace věty o implikaci:
  Víme, že $p \Rightarrow p$ a $(p \Rightarrow p) \Rightarrow (q \Rightarrow (p \Rightarrow p))$ jsou tautologie. Pak také $q \Rightarrow (p \Rightarrow p)$ je tautologie.

Některé vlastnosti tautologií II

- **Věta o dedukci** (sémantická varianta): mějme formule $A_1, A_2, \ldots A_n, B$, kde $n \geq 1$. Pak platí, že $A_1, A_2, \ldots A_{n-1}, A_n \models B$ právě když $A_1, A_2, \ldots A_{n-1} \models A_n \Rightarrow B$.

  Důkaz: oba směry ekvivalence sporem.

  Pozn.: věta umožňuje (opakovaným použitím) převádět platné úsudky na tautologie a naopak.

- aplikace věty o dedukci:

  Víme, že platí $p \vee q, p \wedge \neg q \models \neg q$. Pak dvojí aplikací věty o dedukci dostaneme tautologii $\models (p \vee q) \Rightarrow ((p \wedge \neg q) \Rightarrow \neg q)$.

  Ověřte, že jde skutečně o tautologii.

Klasifikace formulí výrokové logiky I

- *tabulková metoda* – zjištění pravdivosti formulí pro všechny možné interpretace

Příklad 1: formule $(p \vee q) \Leftrightarrow (p \wedge q)$

p	q	$(p$	$\vee$	$q)$	$\Leftrightarrow$	$(p$	$\wedge$	$q)$
1	1	1	1	1	**1**	1	1	1
1	0	1	1	0	**0**	1	0	0
0	1	0	1	1	**0**	0	0	1
0	0	0	0	0	**1**	0	0	0

- vyhodnocení: po složkách (podformulích) dané formule (výrok. symboly, negace,. . . ,celá formule)
- zápis pravdivostní hodnoty: v řádku s příslušnou interpretací pod vyhodnocovanou spojku (výr. symbol)

Klasifikace formulí výrokové logiky II

Příklad 2: formule $(p \wedge \neg p)$

p	p	$\wedge$	$\neg p$
1	1	**0**	0
0	0	**0**	1

- dle výsledných pravdivostních hodnot celé formule (tučně vyznačený sloupec v předchozích tabulkách) rozlišujeme
  - kontradikce: všechny výsledné pravdivostní hodnoty rovny nule
  - splnitelné formule: alespoň jedna výsledná pravdivostní hodnota rovna jedné; modely jsou interpretace uvedené v řádcích, kde je výsledná pravdivostní hodnota formule rovna jedné
  - tautologie: všechny výsledné pravdivostní hodnoty rovny jedné

Další typy úloh I

- Zjistěte, zda je množina formulí $\mathbf{T} = \{p \vee q, p \wedge \neg q\}$ splnitelná.

p	q	$p \vee q$	$p \wedge \neg q$
1	1	1	0
1	0	**1**	**1**
0	1	1	0
0	0	0	0

  $\mathbf{T}$ je splnitelná, jediným modelem je interpretace uvedená na vyznačeném řádku tabulky.

- Vyplývá formule $\neg q$ logicky z množiny $\mathbf{T}$?
  (+ stejné typy úloh formulovaných v přirozeném jazyce)
  Ano, pro všechny modely $\mathbf{T}$ (viz předch. tab.) je $\neg q$ pravdivá. Píšeme $p \vee q, p \wedge \neg q \models \neg q$ (schéma úsudku platného na základě výrokové logiky).

Další typy úloh II

- ověření tautologií tvaru implikace metodou protipříkladu: $\Rightarrow$ je nepravdivá pouze pro pravdivý předpoklad a nepravdivý důsledek. Pro tuto variantu – za předpokladu nepravdivosti důsledku – pro příslušné interpretace ověříme (ne)pravdivost předpokladu.
- příklad: $p \Rightarrow (q \Rightarrow p)$
  - předpoklad: p pravdivá, $q \Rightarrow p$ ne
  - jediná možnost nepravdivosti $q \Rightarrow p$: q pravdivá, p ne
  - spor s předpokladem pravdivosti p

Úplný systém spojek výrokové logiky

- prostřednictvím systému spojek $\{\neg, \wedge, \vee\}$ jsme dokázali vyjádřit libovolnou pravdivostní funkci (spojku); lib. množinu spojek s touto vlastností nazýváme *úplným systémem spojek*
- úplnými systémy spojek jsou například $\{\neg, \wedge\}, \{\neg, \vee\}, \{\neg, \Rightarrow\}$
- existují i jednoprvkové úplné systémy: lib. pravdivostní funkci lze vyjádřit pouze pomocí Shefferovy funkce (negace konjunkce, ozn. $|$), stejnou vlastnost má i Nicodova funkce (negace disjunkce, ozn. .$|$.)
  Př. $(p \vee q) \Leftrightarrow ((p \,|\, p) \,|\, (q \,|\, q))$

Dualita konjunkce a disjunkce I

- vztah mezi $\wedge$ a $\vee$ nazýváme *dualita*, tyto spojky jsou vzájemně komplementární
- **Věta o dualitě I**: nechť A, B obsahují pouze spojky $\neg, \wedge, \vee$. Nechť A', B' vzniknou z A, B záměnou spojek $\wedge$ a $\vee$ (formuli A' nazýváme duální formou k A). Pak platí:
  1. $\models A$ právě když $\models \neg A'$ (resp. $\models \neg A$ právě když $\models A'$)
  2. pokud $\models A \Rightarrow B$, pak $\models B' \Rightarrow A'$
  3. pokud $\models A \Leftrightarrow B$, pak $\models B' \Leftrightarrow A'$
- příklad využití věty (bod 3):
  $A = p \wedge (q \vee r), B = (p \wedge q) \vee (p \wedge r)$
  $A' = p \vee (q \wedge r), B' = (p \vee q) \wedge (p \vee r)$
  víme, že $\models (p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$;
  pak také $\models (p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$

Dualita konjunkce a disjunkce II

- **Věta o dualitě II**: nechť A, B obsahují pouze spojky $\neg, \wedge, \vee$. Nechť A^*, B^* vzniknou z A, B záměnou spojek $\wedge$ a $\vee$ a nahrazením všech atomických formulí jejich negacemi (se zjednodušením $\neg\neg$). Pak platí:
  1. $\models \neg A \Leftrightarrow A^*$
  2. pokud $\models A \Rightarrow B$, pak $\models B^* \Rightarrow A^*$
  3. pokud $\models A \Leftrightarrow B$, pak $\models A^* \Leftrightarrow B^*$
- příklad konstrukce A^*:
  $A = (p \wedge q) \vee (p \wedge \neg r)$
  $A^* = (\neg p \vee \neg q) \wedge (\neg p \vee r)$
  ověřme, že A^* je ekvivalentní $\neg A$:
  $\neg A = \neg((p \wedge q) \vee (p \wedge \neg r))$
  $\Leftrightarrow \neg(p \wedge q) \wedge \neg(p \wedge \neg r)$
  $\Leftrightarrow (\neg p \vee \neg q) \wedge (\neg p \vee r) = A^*$