

Matematická logika

Lekce 1: Motivace a seznámení s klasickou výrokovou logikou

Petr Cintula¹ Tomáš Lávička² **Igor Sedlár**¹

¹Ústav informatiky ²Ústav teorie informace a automatizace



Akademie věd
České republiky

`cs.cas.cz/sedlar/mal.html`

Příklad

$(G, \cdot)$ je grupa právě tehdy, když $\cdot$ je asociativní operace na G s neutrálním prvkem 1 a pro všechny $x \in G$ existuje $y \in G$ takový, že $x \cdot y = 1 = y \cdot x$.

Tvrzení

Pro všechny prvky x grupy G existuje **právě jeden** $y \in G$ takový, že $x \cdot y = 1 = y \cdot x$ (označení x^{-1}).

Důkaz. $xa = 1 = ax$ a $xb = 1 = bx$

$$b(xa) = b1 = b$$

$$b(xa) = (bx)a = 1a = a$$

Tedy $a = b$



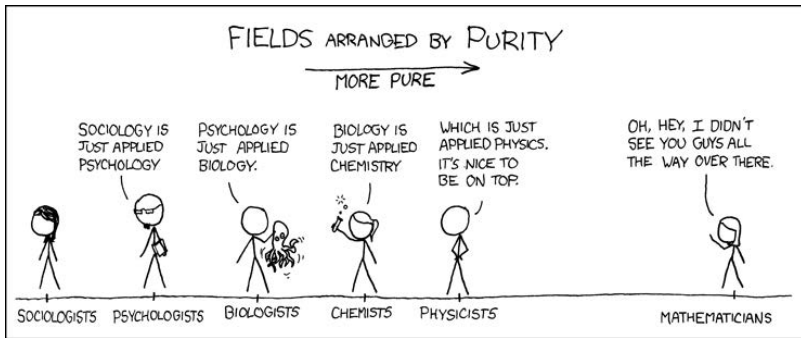
Důkaz „pořádně“

Předpoklady: $xa = 1, ax = 1, xb = 1, bx = 1.$

(G1) $\forall xyz((xy)z = x(yz))$	1. $xa = 1 \rightarrow ((b(xa) = b1) \wedge ((xa)b = 1b))$
(G2) $\forall x(x1 = x \wedge 1x = x)$	(E3)
(E1) $\forall xy(x = y \rightarrow y = x)$	2. $(b(xa) = b1) \wedge ((xa)b = 1b)$
(E2) $\forall xyz((x = y \wedge y = z) \rightarrow x = z)$	(Př1, 1, MP)
(E3)	3. $b(xa) = b1$
$\forall xyz(x = y \rightarrow (zx = zy \wedge xz = xy))$	(2, $\wedge 1$, MP)
($\wedge 1$) $(\varphi \wedge \psi) \rightarrow \varphi$	4. $b1 = b$
($\wedge 2$) $\varphi \rightarrow (\psi \rightarrow (\varphi \wedge \psi))$	(G2, $\wedge 1$, MP)
(MP) $\frac{\varphi \quad \varphi \rightarrow \psi}{\psi}$	5. $b(xa) = b$
($\forall E$) $\frac{\forall x\varphi}{\varphi(x/t)}$	(E2, $\wedge 2$, 3, 4, MP)
	6. $(bx)a = b(xa)$
	(G1)
	7. $(bx)a = b$
	(6, 7, $\wedge 2$, MP, E2, MP)
	8. $(bx)a = 1a$
	(Př4, E3, MP, $\wedge 1$, MP)
	9. $1a = (bx)a$
	(E1, MP)
	10. $1a = b$
	(8, 9, $\wedge 2$, MP, E2, MP)
	11. $a = b$
	(G2, $\wedge 1$, E1, $\wedge 2$, E2, MP)

Logika jakožto obecná teorie $\forall, \rightarrow$ atd.

- V matematických důkazech používáme axiomy jednotlivých matematických teorií...
- ...ale také se opíráme o „logické výrazy“ jako „pro všechny“ ($\forall$), „a“ ($\wedge$), „jestliže, pak“ ($\rightarrow$) atd.
- Logiku můžeme chápat jako matematickou teorii těchto výrazů
- Logika je tedy disciplína, která je v pozadí veškerého matematického usuzování (dokazování)
- Jak uvidíme, logika je také „metamatematikou“, tedy teorií matematických teorií



<http://www.xkcd.com/435/>

Proč důkazy „pořádně“?

Epistemické důvody: Porozumění / vysvětlení důkazů „do detailů“; Vypracování jistých (pevných) základů matematických teorií (G. Frege a aritmetika)

Hygiena matematiky: Paradoxy a krize základů matematiky jakožto logické problémy (B. Russell)

Automatické dokazování: algoritmy potřebují přesne formulované pravidla odvozování včetně základních logických pravidel

Formalizace: formalizace teorií v matematice (a Gödelovy věty), ale také v př. vědách (R. Carnap a logičtí pozitivisti), dnes časté využití v informatice (AI, KR, verifikace sw/hw)

Logika a správné usuzování

Logika jako disciplína vznikla jako součást filozofie v antickém Řecku, jejím cílem bylo studovat **principy správného usuzování**.

Příklad („Úroveň 1“)

- Pokud by Bůh existoval, tak by byl dobrý a všemocný.
- Pokud by Bůh byl dobrý a všemocný, tak by lidé netrpěli.
- Ale, lidé trpí.
- Tudíž Bůh neexistuje.

Příklad („Úroveň 2“)

- $\overbrace{\text{Bůh existuje}}^p \rightarrow \overbrace{\text{Bůh je dobrý}}^q \wedge \overbrace{\text{Bůh je všemocný}}^r$

- $(q \wedge r) \rightarrow \neg(\overbrace{\text{Lidé trpí}}^s)$

- s

- Tedy $\neg p$

$$\begin{aligned} p &\rightarrow (q \wedge r) \\ (q \wedge r) &\rightarrow \neg s \end{aligned}$$

$$\begin{array}{c} s \\ \hline \neg p \end{array}$$

Příklad („Úroveň 3“)

Teorie

$$(\rightarrow 1) \quad (\varphi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \chi))$$

$$(\rightarrow 2) \quad (\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \neg\varphi)$$

$$(MP) \quad \frac{\varphi \quad \varphi \rightarrow \psi}{\psi}$$

Odvození v teorii

1. $p \rightarrow (q \wedge r)$ Př.1
2. $p \rightarrow (q \wedge r) \rightarrow (((q \wedge r) \rightarrow \neg s) \rightarrow (p \rightarrow \neg s))$ ($\rightarrow 1$)
3. $((q \wedge r) \rightarrow \neg s) \rightarrow (p \rightarrow \neg s)$ (1,2,MP)
4. $(q \wedge r) \rightarrow \neg s$ Př.2
5. $p \rightarrow \neg s$ (3,4,MP)
6. $(p \rightarrow \neg s) \rightarrow (s \rightarrow \neg p)$ ($\rightarrow 2$)
7. $s \rightarrow \neg p$ (5,6,MP)
8. s Př.3
9. $\neg p$ (7,8,MP)

Každý úsudek má předpoklady a závěr.

Ty mohou být v daném kontextu buď pravdivé nebo nepravdivé.

Úsudek je správný iff není žádný kontext, v němž by byly všechny jeho předpoklady pravdivé a závěr nepravdivý.

Atomické formule (výrokové atomy): spočetná nekonečná množina Var primitivních výroků (t.j. výroků bez další vnitřní struktury)

Formule: nejmenší množina For obsahující Var , tž. pro každé $\varphi, \psi \in \text{For}$ platí:

$$\varphi \rightarrow \psi \in \text{For} \quad \text{a} \quad \neg\varphi \in \text{For}$$

	atomické formule:	$p, q, r, s, t, \dots$
Obvyklé symboly pro:	formule:	$\varphi, \psi, \chi, \dots$
	množiny formulí:	$\Gamma, \Delta, \Psi, \Phi, \dots$

Příklady neformulí: $p \rightarrow$ $pp \rightarrow q$ $p \rightarrow \rightarrow p$ $p \rightarrow q \rightarrow p$

Příklady formulí: $p \rightarrow q$ $\neg p \rightarrow p$ $p \rightarrow (\neg q \rightarrow p)$ $(p \rightarrow q) \rightarrow q$

Negace má větší prioritu než implikace!

Klasická výroková logika: Syntax

Primitivní spojky: (binární) implikace $\rightarrow$ a (unární) negace $\neg$

Definované (binární) spojky: disjunkce $\vee$, konjunkce $\wedge$, ekvivalence $\leftrightarrow$:

$$\varphi \vee \psi = \neg\varphi \rightarrow \psi \quad \varphi \wedge \psi = \neg(\varphi \rightarrow \neg\psi) \quad \varphi \leftrightarrow \psi = (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$$

Priorita spojek:	0	$\neg$	
	1	$\vee$	$\wedge$
	2	$\rightarrow$	$\leftrightarrow$

Příklady formulí (bez konvence o prioritě spojek):

$$p \rightarrow (p \wedge q) \qquad p \rightarrow ((\neg q) \wedge p)$$

Příklady formulí (s konvencí o prioritě spojek):

$$p \rightarrow p \wedge q \qquad p \rightarrow \neg q \wedge p$$

Klasická výroková logika: Sémantika

Základní princip: v daném kontextu má každá formule právě jednu z pravdivostních hodnot: **pravda**, **nepravda**

Definice

Ohodnocení je každé zobrazení $e: \text{For} \rightarrow \{0, 1\}$ tž.:

$$e(\neg\varphi) = 1 - e(\varphi) \qquad e(\varphi \rightarrow \psi) = \begin{cases} 1 & \text{pokud } e(\varphi) \leq e(\psi) \\ 0 & \text{pokud } e(\varphi) > e(\psi) \end{cases}$$

Tvrzení

$$e(\varphi \wedge \psi) = \min\{e(\varphi), e(\psi)\} \qquad e(\varphi \vee \psi) = \max\{e(\varphi), e(\psi)\}$$

$$e(\varphi \leftrightarrow \psi) = \begin{cases} 1 & \text{pokud } e(\varphi) = e(\psi) \\ 0 & \text{pokud } e(\varphi) \neq e(\psi) \end{cases}$$

Správné usuzování (v klasické výrokové logice)

Definice

Formule φ je **logickým důsledkem** množiny formulí Γ , $\Gamma \models \varphi$, pokud pro každé ohodnocení e platí:

pokud $e(\gamma) = 1$ pro každou fli $\gamma \in \Gamma$, pak $e(\varphi) = 1$.

Správný úsudek = logický důsledek

Úsudek je správný iff **není žádný kontext, v němž by byly všechny jeho předpoklady pravdivé a závěr nepravdivý**

Příklady (ne)správných úsudků

Příklad (Modus ponens)

$$\frac{p \rightarrow q \quad p}{q}$$

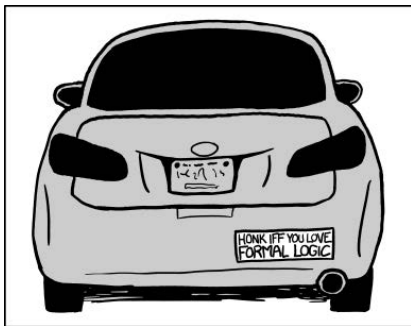
Toto je správný úsudek (pokud $e(p \rightarrow q) = e(p) = 1$, pak $e(q) = 1$).

Příklad (Abdukce)

$$\frac{p \rightarrow q \quad q}{p}$$

Toto **není** správný úsudek (vezměme: $e(p) = 0$ a $e(q) = 1$).

Ještě jeden příklad



Title text: Note that this implies you should NOT honk solely because I stopped for a pedestrian and you're behind me

<http://www.xkcd.com/1033/>

Ještě jeden příklad

Note that this implies you should NOT honk solely because I stopped for a pedestrian and you're behind me

Příklad

$$h \leftrightarrow l$$

$$\neg l$$

$$\varphi$$

$$\neg h$$

Toto **je** správný úsudek bez ohledu na φ .

Zpět k našemu původnímu příkladu

Příklad

$$\begin{array}{l} p \rightarrow q \wedge r \\ q \wedge r \rightarrow \neg s \\ s \\ \hline \neg p \end{array}$$

Toto je správný úsudek: pokud

$e(p \rightarrow q \wedge r) = e(q \wedge r \rightarrow \neg s) = e(s) = 1$, pak $e(\neg s) = 0$ a tak $e(q \wedge r) = 0$. Tudíž $e(p) = 0$ a tak $e(\neg p) = 1$.

ALE, opravdu jsme dokázali, že Bůh není?

Jistěže ne! Jen víme, že tento závěr je pravdivý pokud (!) jsou pravdivé předpoklady tohoto úsudku.

A navíc! Víme to pouze pokud souhlasíme se správností formalizaci původního úsudku **a** věříme, že (klasická výroková) logika je **správná**.

Strukturalita 'logického' usuzování

Pokud by **Bůh existoval**,

tak **by** byl dobrý a všemocný

Pokud by **Bůh** byl dobrý a všemocný,

tak **by** lidé netrpěli.

Ale, **lidé trpí**.

Tudíž **Bůh neexistuje**.

$$p \rightarrow q \wedge r$$

$$q \wedge r \rightarrow \neg s$$

$$s$$

$$\neg p$$

Strukturalita 'logického' usuzování

Pokud by politici byli ideální, tak by byli schopní a čestní.

Pokud by politici byli schopní a čestní, tak by neexistovala korupce.

Ale, korupce existuje.

Tudíž politici nejsou ideální.

$$p \rightarrow q \wedge r$$

$$q \wedge r \rightarrow \neg s$$

$$s$$

$$\neg p$$

Strukturalita 'logického' usuzování

Pokud by X byla množina racionálních čísel, tak by byla nekonečná a hustá.

Pokud by X byla nekonečná a hustá, tak existuje prosté $f: \mathbb{N} \rightarrow X$

Ale žádné takové f neexistuje.

Tudíž X není množina racionálních čísel.

$$p \rightarrow q \wedge r$$

$$q \wedge r \rightarrow \neg s$$

$$s$$

$$\neg p$$

Připomeňme si sémantickou definici správného úsudku

Ohodnocení je každé zobrazení $e: \text{For} \rightarrow \{0, 1\}$ tž.:

$$e(\neg\varphi) = 1 - e(\varphi) \qquad e(\varphi \rightarrow \psi) = \begin{cases} 1 & \text{pokud } e(\varphi) \leq e(\psi) \\ 0 & \text{pokud } e(\varphi) > e(\psi) \end{cases}$$

Formule φ je **logickým důsledkem** množiny formulí Γ , $\Gamma \models \varphi$, pokud pro každé ohodnocení e platí:

pokud $e(\gamma) = 1$ pro každou fli $\gamma \in \Gamma$, pak $e(\varphi) = 1$.

Formule φ je **tautologie** iff $\emptyset \models \varphi$.

Příklad

Všechny formule těchto tvarů jsou tautologie:

- $(\varphi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \chi))$
- $(\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \neg\varphi)$
- $(\varphi \wedge \psi) \rightarrow \varphi$
- $\varphi \rightarrow (\psi \rightarrow (\varphi \wedge \psi))$

Ted' to zkusme syntakticky

Axiomy (pro každou $\varphi, \psi, \chi \in \text{For}$):

$$\text{A1 } \varphi \rightarrow (\psi \rightarrow \varphi)$$

$$\text{A2 } (\chi \rightarrow (\varphi \rightarrow \psi)) \rightarrow ((\chi \rightarrow \varphi) \rightarrow (\chi \rightarrow \psi))$$

$$\text{A3 } (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$$

Dedukční pravidlo *Modus Ponens* (pro každou $\varphi, \psi \in \text{For}$):
$$\frac{\varphi \quad \varphi \rightarrow \psi}{\psi}$$

Důkaz formule φ z množiny předpokladů Γ je konečná posloupnost formulí $\langle \psi_1, \dots, \psi_n \rangle$ tž. $\psi_n = \varphi$ a pro každé $i \leq n$, buď

- ψ_i je instance axiomu nebo prvek Γ , nebo
- existují $j, k < i$ tž. $\psi_k = \psi_j \rightarrow \psi_i$.

Píšeme $\Gamma \vdash \varphi$ pokud existuje důkaz φ z množiny předpokladů Γ .

Věta u úplnosti

Věta (Věta u úplnosti)

Pro každou množinu formulí $\Gamma \cup \{\varphi\}$ platí:

$$\Gamma \vdash \varphi \iff \Gamma \models \varphi$$