Axiomatizácia výrokového počtu

Tvárime sa, že VF(P) sú vybudované z P pomocou logických spojok $\neg$ a $\Rightarrow$. Zápisom $A \equiv B$ skrátene značíme, že písmená A a B označujú tú istú výrokú formu. Znak $\equiv$, podobne ako znaky A, B, P, VF, I, J a pod., však nepatrí do jazyka výrokého počtu. Sú to znaky *metajazyka*, pomocou ktorého opisujeme výrokový počet.

Logické axiómy (3 schémy axióm)

(Ax 1) $A \Rightarrow (B \Rightarrow A)$
(Ax 2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
(Ax 3) $(\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)$

Odvodzovacie pravidlo MODUS PONENS

(MP) $\dfrac{A,\ A \Rightarrow B}{B}$ (z A a $A \Rightarrow B$ odvoď B)

Cvičenie. Ukážte, že nasledujúce VF sú dokázateľné len z logických axióm:

(a) $p \Rightarrow p$
(b) $\neg\neg p \Rightarrow p$
(c) $p \Rightarrow \neg\neg p$
(d) $\neg p \Rightarrow (p \Rightarrow q)$
(e) $(\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)$
(f) $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$
(g) $(p \Rightarrow (\neg q \Rightarrow \neg(p \Rightarrow q)))$
(h) $(p \Rightarrow q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow q)$
(i) $(\neg p \Rightarrow p) \Rightarrow p$

Ako (odstrašujúci) príklad urobíme len (a).

1. $(p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$
   (Ax 2) pre $A \equiv p$, $B \equiv (p \Rightarrow p)$, $C \equiv p$
2. $p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$
   (Ax 1) pre $A \equiv p$, $B \equiv (p \Rightarrow p)$
3. $(p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$
   vyplýva z 1. a 2. podľa (MP)
4. $p \Rightarrow (p \Rightarrow p)$
   (Ax 1) pre $A \equiv p$, $B \equiv p$
5. $p \Rightarrow p$
   vyplýva z 3. a 4. podľa (MP)

Veta o dedukcii. *Nech* $T \subseteq \mathrm{VF}(P)$ *a* $A, B \in \mathrm{VF}(P)$*. Potom* $T \vdash A \Rightarrow B$ *práve vtedy, keď* $T \cup \{A\} \vdash B$*.*

Dôkaz. Nech $T \vdash A \Rightarrow B$. Potom tým skôr $T \cup \{A\} \vdash A \Rightarrow B$. Zrejme $T \cup \{A\} \vdash A$, z čoho pomocou (MP) dostávame $T \cup \{A\} \vdash B$. Ak je totiž $C_0, C_1, \ldots, C_n$ dôkaz $A \Rightarrow B$ v $T \cup \{A\}$, tak $C_0, C_1, \ldots, C_n, A, B$ je dôkaz B v $T \cup \{A\}$.

Naopak, nech $T \cup \{A\} \vdash B$ a $B_0, B_1, \ldots, B_n$ je príslušný dôkaz. Budeme postupovať indukciou podľa n.

Ak $n = 0$, tak $B_0 \equiv B$. Potom sú len dve možnosti: $B \in T$ alebo $B \equiv A$. V prvom prípade B, $B \Rightarrow (A \Rightarrow B)$ (Ax 1), $A \Rightarrow B$ je dôkaz $A \Rightarrow B$ v T.

V druhom prípade si stačí uvedomiť, že $\vdash A \Rightarrow A$ (cvičenie (a)), teda tým skôr $T \vdash A \Rightarrow A$.

Nech ďalej $n > 0$ a náš záver platí pre všetky dôkazy $C_0, C_1, \ldots, C_m$, kde $m < n$. Rozlíšime dva prípady:

1. $B_n \in T$ alebo B_n je logická axióma. Potom B_n, $B_n \Rightarrow (A \Rightarrow B_n)$ (Ax 1), $A \Rightarrow B_n$ je dôkaz $A \Rightarrow B_n$ v T.

2. Existujú $j, k < n$ také, že $B_j \equiv (B_k \Rightarrow B_n)$. Potom $B_0, \ldots, B_j$ aj $B_0, \ldots, B_k$ sú dôkazy v $T \cup \{A\}$. Podľa indukčného predpokladu máme $T \vdash A \Rightarrow B_j$, t. j. $T \vdash A \Rightarrow (B_k \Rightarrow B_n)$, ako aj $T \vdash A \Rightarrow B_k$. Pomocou (Ax 2)

$$(A \Rightarrow (B_k \Rightarrow B_n)) \Rightarrow ((A \Rightarrow B_k) \Rightarrow (A \Rightarrow B_n))$$

a (MP) postupne dostávame

$$\begin{aligned} &T \vdash (A \Rightarrow B_k) \Rightarrow (A \Rightarrow B_n), \\ &T \vdash A \Rightarrow B_n, \end{aligned}$$

t. j. $T \vdash A \Rightarrow B$.

Dôsledok o dôkaze sporom. *Nech* $T \subseteq \mathrm{VF}(P)$ *a* $A \in \mathrm{VF}(P)$*. Potom* $T \vdash A$ *práve vtedy, keď teória* $T \cup \{\neg A\}$ *je sporná.*

Dôkaz. Nech $T \vdash A$. Tým skôr $T \cup \{\neg A\} \vdash A$. Keďže zrejme $T \cup \{\neg A\} \vdash \neg A$, teória $T \cup \{\neg A\}$ je sporná.

Nech naopak teória $T \cup \{\neg A\}$ je sporná. Potom je v nej dokázateľná každá VF; špeciálne $T \cup \{\neg A\} \vdash A$. Podľa vety o dedukcii potom $T \vdash \neg A \Rightarrow A$. Podľa cvičenia (i) je $\vdash (\neg A \Rightarrow A) \Rightarrow A$, a tým skôr $T \vdash (\neg A \Rightarrow A) \Rightarrow A$. Použitím (MP) dostávame $T \vdash A$.

Dôsledok o dôkaze rozborom možností. *Nech* $T \subseteq \mathrm{VF}(P)$ *a* $A, B \in \mathrm{VF}(P)$*. Potom* $T \cup \{A\} \vdash B$ *a* $T \cup \{\neg A\} \vdash B$ *platí práve vtedy, keď* $T \vdash B$*.*

Dôkaz. Nech platí $T \cup \{A\} \vdash B$ a $T \cup \{\neg A\} \vdash B$. Podľa vety o dedukcii z toho vyplýva $T \vdash A \Rightarrow B$ a $T \vdash \neg A \Rightarrow B$. Na základe cvičenia (h) máme

$$\vdash (A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow B),$$

a dvojnásobným použitím (MP) dostávame $T \vdash A$.

Nech naopak $T \vdash A$. Potom triviálne $T \cup \{A\} \vdash B$ aj $T \cup \{\neg A\} \vdash B$.

Lema o interpretácii. *Nech* $p_1, \dots, p_n \in P$ *a* $A \in \mathrm{VF}\{p_1, \dots, p_n\}$. *Potom pre ľubovoľnú interpretáciu* $I\colon \mathrm{VF}(P) \to \{0,1\}$ *platí*

$$\{p_1^I, \dots, p_n^I\} \vdash A^I.$$

Dôkaz. Indukciou podľa zložitosti formy A:

(a) Ak $A \equiv p \in P$, tak tvrdenie znamená, že $\{p\} \vdash p$ (ak $I(p) = 1$) alebo $\{\neg p\} \vdash \neg p$ (ak $I(p) = 0$). Jedno aj druhé je v poriadku.

(b) Nech $A \equiv \neg B$ a pre B náš záver platí. Potom tiež $B \in \mathrm{VF}\{p_1, \dots, p_n\}$.

Ak $I(A) = 1$, tak $I(B) = 0$ a $A^I \equiv A \equiv \neg B \equiv B^I$. Podľa predpokladu $\{p_1^I, \dots, p_n^I\} \vdash B^I$, t. j. $\{p_1^I, \dots, p_n^I\} \vdash A^I$.

Ak $I(A) = 0$, tak $I(B) = 1$, $B^I \equiv B$ a $A^I \equiv \neg A \equiv \neg\neg B$. Podľa predpokladu $\{p_1^I, \dots, p_n^I\} \vdash B^I$, t. j. $\{p_1^I, \dots, p_n^I\} \vdash B$. Podľa cvičenia (c) platí $\vdash B \Rightarrow \neg\neg B$, takže použitím (MP) dostávame $\{p_1^I, \dots, p_n^I\} \vdash \neg\neg B$, čiže $\{p_1^I, \dots, p_n^I\} \vdash A^I$.

(c) Nech $A \equiv (B \Rightarrow C)$ a pre B, C platí dokazovaný záver. Potom $B, C \in \mathrm{VF}\{p_1, \dots, p_n\}$. Rozlíšime tri prípady:

1. $I(B) = 0$. Potom $I(A) = I(B \Rightarrow C) = 1$, teda $A^I \equiv A$. Ďalej $B^I \equiv \neg B$, teda podľa indukčného predpokladu $\{p_1^I, \dots, p_n^I\} \vdash \neg B$. Podľa cvičenia (d) platí $\vdash \neg B \Rightarrow (B \Rightarrow C)$ a vďaka (MP) $\{p_1^I, \dots, p_n^I\} \vdash B \Rightarrow C$, t. j. $\{p_1^I, \dots, p_n^I\} \vdash A^I$.

2. $I(C) = 1$. Potom $C^I \equiv C$ a $I(A) = I(B \Rightarrow C) = 1$, teda $A^I \equiv A$. Podľa indukčného predpokladu $\{p_1^I, \dots, p_n^I\} \vdash C$. (Ax 1) dáva $\vdash C \Rightarrow (B \Rightarrow C)$ a pomocou (MP) dostávame $\{p_1^I, \dots, p_n^I\} \vdash B \Rightarrow C$, t. j. $\{p_1^I, \dots, p_n^I\} \vdash A^I$.

3. $I(B) = 1$, $I(C) = 0$. Potom $B^I \equiv B$, $C^I \equiv \neg C$ a $I(A) = I(B \Rightarrow C) = 0$, teda $A^I \equiv \neg A$. Podľa indukčného predpokladu $\{p_1^I, \dots, p_n^I\} \vdash B$, $\{p_1^I, \dots, p_n^I\} \vdash \neg C$. Cvičenie (g) dáva $\vdash B \Rightarrow (\neg C \Rightarrow \neg(B \Rightarrow C))$. Použijúc dvakrát (MP) dostávame $\{p_1^I, \dots, p_n^I\} \vdash \neg(B \Rightarrow C)$, t. j. $\{p_1^I, \dots, p_n^I\} \vdash A^I$.

Postova veta o úplnosti. *Pre ľubovoľnú výrokovú formu* $A \in \mathrm{VF}(P)$ *platí* $\vDash A$ *práve vtedy, keď* $\vdash A$.

Dôkaz. Dokážeme len, že každá tautológia je dokázateľná iba z logických axióm; opačný smer je veta o korektnosti.

Nech $A \in \mathrm{VF}\{p_1, \dots, p_n\}$. Keďže A je tautológia, $I(A) = 1$ a $A^I \equiv A$ pre každé pravdivostné ohodnotenie $I\colon \{p_1, \dots, p_n\} \to \{0,1\}$. Podľa lemy o interpretácii

$$\{p_1^I, \dots, p_n^I\} \vdash A.$$

Preto tiež pre ľubovoľné pravdivostné ohodnotenie $J\colon \{p_1, \dots, p_{n-1}\} \to \{0,1\}$ platí

$$\{p_1^J \dots, p_{n-1}^J, p_n\} \vdash A,$$
$$\{p_1^J \dots, p_{n-1}^J, \neg p_n\} \vdash A$$

Obe možnosti $I_1(p_n) = 1$, $I_2(p_n) = 0$ spolu s podmienkou $I_1(p_k) = I_2(p_k) = J(p_k)$ pre $k < n$ dávajú totiž pravdivostné ohodnotenia $I_1, I_2\colon \{p_1, \dots, p_n\} \to \{0,1\}$. Podľa dôsledku o dôkaze rozborom možností z toho vyplýva

$$\{p_1^J, \dots, p_{n-1}^J\} \vdash A.$$

Opakovaním uvedeného postupu dostaneme $\vdash A$.