Logika pro pedagogy

(P. Hájek)

Logika studuje pojem *důsledku* mezi výrazy (množinami výroků)
Výroky pravdivé, nepravdivé (záleží na významu složek)
Kalkuly: výrokový počet, predikátový počet.
Symboly výrokového počtu: výrokové proměnné $p, q, \ldots$

logické spojky $\&, \vee, \rightarrow, \equiv, \neg$ (a závorky).

Pravdivostní tabulky spojek.

Formule. Ohodnocení výrokových proměnných, jednoznačnost rozšíření na ohodnocení všech formulí respektující pravdivostní tabulky spojek.

Tautologie (př. $\varphi \rightarrow \varphi$); sémanticky ekvivalentní fle.

Lemma: φ, ψ jsou sém. ekvivalentní, právě když $(\varphi \equiv \psi)$ je tautologie.

Důležité tautologie (ověřit)

$(\varphi \& \psi) \equiv (\psi \& \varphi), (\varphi \& (\psi \& \chi)) \equiv ((\varphi \& \psi) \& \chi)$
– komutativita a asociativita konjunkce; podobně disjunkce.
$(\varphi \& (\psi \vee \chi) \equiv ((\varphi \& \psi) \vee (\varphi \& \chi)), (\varphi \vee (\psi \& \chi)) \equiv ((\varphi \vee \psi) \& (\varphi \vee \chi))$
– distributivita
$\neg(\varphi \& \psi) \equiv (\neg\varphi \vee \neg\psi), \neg(\varphi \vee \psi) \equiv (\neg\varphi \& \neg\psi)$
– de Morgan
$(\varphi \& \neg\varphi) \rightarrow \psi$ (ex falso quodlibet)
$\varphi \vee \neg\varphi$ (tertium non datur)
$(\varphi \& \psi) \equiv \neg(\varphi \rightarrow \neg\psi)$
$(\varphi \vee \psi) \equiv (\neg\varphi \rightarrow \psi)$
$(\varphi \equiv \psi) \equiv \neg((\varphi \rightarrow \psi) \rightarrow \neg(\psi \rightarrow \varphi))$

Důsledek: každá fle je sémanticky ekvivalentní fli neobsahující spojky $\&, \vee, \equiv$

Další tautologie:

(A1) $\quad \varphi \rightarrow (\psi \rightarrow \varphi)$
(A2) $\quad (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$
(A3) $\quad (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$

(A1)–(A3) jsou *axiomy výr. počtu.*

Dedukční pravidlo *modus ponens* (odloučení): z φ a $\varphi \rightarrow \psi$ odvoď ψ.

Fakt: Pro libovolné ohodnocení e, jestliže $e(\varphi) = e(\varphi \rightarrow \psi) = 1$, pak $e(\psi) = 1$.
Tedy: Jsou-li $\varphi, \varphi \rightarrow \psi$ tautologie, je i ψ tautologií.

Pojem *důkazu* (ve výr. počtu) a *dokazatelné formule.* Značení: $\vdash \varphi$.

Příklad: důkaz formule $\varphi \rightarrow \varphi$ (má 5 členů).

Korektnost výr. počtu: každá dokazatelná fle je tautologií. *Problém úplnosti:* je každá tautologie dokazatelná? (ANO)
Teorie ve výr. počtu; důkaz v teorii, $T \vdash \varphi$.
Příklad: $\varphi, \varphi \rightarrow \psi, \psi \rightarrow \chi \vdash \chi$.

Model teorie T je ohodnocení e takové, že $e(\psi) = 1$ pro každé $\psi \in T$.

Silná korektnost: Je-li $T \vdash \varphi$, pak $e(\varphi) = 1$ pro každý model e teorie T. *Problém silné úplnosti:* lze obrátit? (ANO, bude).

Věta o dedukci: T teorie, φ, ψ fle. $T \cup \{\varphi\} \vdash \psi$, právě když $T \vdash (\varphi \to \psi)$. (Důkaz.)

Věta: Následující fle jsou dokazatelné ve výrokovém počtu: (důkaz užitím věty o dedukci)

(1) $(\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi))$

(2) $\varphi \to ((\varphi \to \psi) \to \psi)$

(3) $(\varphi \to (\psi \to \chi)) \to (\psi \to (\varphi \to \chi))$

(4) $\neg\varphi \to (\varphi \to \psi)$
(neboť $\vdash \neg\varphi \vdash \neg\psi \to \neg\varphi$)

(5) $\neg\neg\varphi \to \varphi$
(neboť $\vdash \neg\neg\varphi \to (\neg\varphi \to \neg\neg\neg\varphi))$

(6) $\varphi \to \neg\neg\varphi$
(neboť $\vdash \neg\neg\neg\varphi \to \neg\varphi$)

(7) $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$
(neboť $\varphi \to \psi \vdash \neg\neg\varphi \to \neg\neg\psi$)
podobně $(\varphi \to \neg\psi) \to (\psi \to \neg\varphi)$ atd.)

(8) $\varphi \vdash \neg\neg\varphi$ (z(6))

(9) $\psi \vdash \varphi \to \psi$ (z ax. (1))

(10) $\neg\varphi \vdash \varphi \to \psi$ (viz. (4))

(11) $\varphi, \neg\psi \vdash \neg(\varphi \to \psi)$
(neboť $\vdash \varphi \to ((\varphi \to \psi) \to \psi)$,
tedy $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$)

(12) $(\neg\psi \to \psi) \to \psi$
(neboť $\vdash \neg\psi \to (\psi \to \neg\chi)$ (viz (4)),
$\vdash (\neg\psi \to \psi) \to (\neg\psi \to \neg\chi)$
$\vdash (\neg\psi \to \psi) \to (\chi \to \psi)$
$\vdash (\chi \to ((\neg\psi \to \psi) \to \psi)$, zvol za χ axiom)

Věta: (rozbor případů) Když $T, \varphi \vdash \psi$ a $T, \neg\varphi \vdash \psi$, pak $T \vdash \psi$.
$(T \vdash \varphi \to \psi, T \vdash \neg\varphi \to \psi, T \vdash \neg\psi \to \varphi, T \vdash \neg\psi \to \psi, T \vdash \psi)$

Def.: $(0)\varphi$ je $\neg\varphi$, $(1)\varphi$ je φ.

Lemma. Buď e ohodnocení proměnných $p_1, \ldots, p_n$, buď φ fle vybudovaná z těchto proměnných. Pak

$$(e(p_1))p_1, \ldots, (e(p_n)) \vdash (e(\varphi))\varphi.$$

D. indukcí: užij (8) – (11).

Příklad: $e(p) = e(r) = 1, e(q) = 0$.
$p, \neg q, r \vdash (p \to q), \neg(r \to (p \to q)$.

Věta o *úplnosti výrokového počtu.* Je-li φ tautologie, pak $\vdash \varphi$.

Dle lemmatu:

$p_1, p_2, \dots p_{n-1}, p_n \vdash \varphi$
$p_1, p_2, \dots p_{n-1}, \neg p_n \vdash \varphi$, tedy
$p_1, \dots, p_{n-1} \vdash \varphi$
...
$\neg p_1, \neg p_2, \dots \neg p_{n-1}, p_n \vdash \varphi$
$\neg p_1, \neg p_2, \dots \neg p_{n-1}, \neg p_n \vdash \varphi$
tedy $\neg p_1, \dots \neg p_{n-1} \vdash \varphi$
atd.

Důsledek: Silná úplnost (zatím) pro konečné teorie.

(následuje: konjunktivní a disjunktivní norm. formy)

Silná věta o úplnosti: Pro každou teorii T a formuli φ výrokového počtu platí: $T \vdash \varphi$, právě když $e(\varphi) = 1$ pro každý model e teorie T.

Stačí dokázat: Když T nedokazuje φ, pak existuje model e teorie T, pro nějž $e(\varphi) = 0$. K tomu

Definice. T je *sporná*, jestliže existuje formule φ taková, že $T \vdash \varphi$ a $T \vdash \neg\varphi$. Je *bezesporná*, jestliže není sporná. T je *(deduktivně) úplná*, jestliže pro každou formuli φ platí $T \vdash \varphi$ nebo $T \vdash \neg\varphi$.

Poznámka. T je sporná, právě když každá formule je dokazatelná v T.

Lemma: $T \nvdash \varphi$, právě když $T \cup \{\neg\varphi\}$ je bezesporná (Důkaz.)

Tedy stačí dokázat, že každá bezesporná teorie T^* má model. Nechť $T = \{\varphi_0, \varphi_1, \varphi_2, \dots\}$, buď $T_0 = T$. Je-li definována (bezesporná) teorie $T_n \supseteq T$ a $T_n \vdash \varphi_n$, pak $T_{n+1} = T_n$; je-li $T_n \nvdash \varphi_n$, pak $T_{n+1} = T_n \cup \{\neg\varphi_n\}$. Buď $T^* = \bigcup_n T_n$. T^* je úplná a bezesporná teorie. Položme $e(p_i) = 1$, když $T^* \vdash p_i$; jinak $e(p_i) = 0$. Užitím (8)-(11) plyne, že pro libovolnou fli φ je $e(\varphi) = 1$, právě když $T^* \vdash \varphi$. Tedy e je model teorie T^*, a tedy i model teorie T. Tím je silná věta o (sémantické) úplnosti dokázána.

Další užitečná fakta

(14) "Modus tollens": $\varphi \to \psi, \neg\psi \vdash \neg\varphi$ (viz. (7))

Pozn. Ukažte, že $p \to q \nvdash q \to p$ (pomoci vlastního ohodnocení)

(16) $\chi \vdash \psi$, právě když $\neg\psi \vdash \neg\chi$
$\chi \vdash \neg\psi$, právě když $\psi \vdash \neg\chi$
$\neg\chi \vdash \psi$, právě když $\neg\psi \vdash \chi$

V dalším považujeme $\varphi \& \psi$ za zkratku za $\neg(\varphi \to \neg\psi)$; formuli $\varphi \vee \psi$ považujeme za zkratku za $\neg\varphi \to \psi$. (Proč můžeme?)

(17) $\varphi\&\psi \vdash \varphi$, $\varphi\&\psi \vdash \psi$, $\varphi, \psi \vdash \varphi\&\psi$.

(Víme $\neg\varphi \vdash \varphi \to \neg\psi$ a $\neg\psi \vdash \varphi \to \neg\psi$, tedy $\neg(\varphi \to \neg\psi) \vdash \varphi$, a $\neg(\varphi \to \psi) \vdash \psi$, neboli $(\varphi\&\psi) \vdash \varphi, (\varphi\&\psi) \vdash \psi$. Dále víme $\varphi, \varphi \to \neg\psi \vdash \neg\psi$, tedy $\varphi, \psi \vdash \neg(\varphi \to \psi)$, čili $\varphi, \psi \vdash \varphi\&\psi$.)

(18) $\varphi \vdash \varphi \vee \psi$, $\psi \vdash \varphi \vee \psi$

(Víme $\vdash \varphi \to (\neg\varphi \to \psi)$ a také $\vdash \psi \to (\neg\varphi \to \psi)$.)

(19) $\varphi \to \chi, \psi \to \chi \vdash (\varphi \vee \psi) \to \chi$

Chceme $\varphi \to \chi, \psi \to \chi, (\neg\varphi \to \psi) \vdash \chi$ (stále užíváme větu o dedukci). Buď $T = \{\varphi \to \chi, \psi \to \chi, \neg\varphi \to \psi\}$, Zřejmě $T, \varphi \vdash \chi$ a také $T, \neg\varphi \vdash \chi$, tedy $T \vdash \chi$ (rozbor případů).

(20) $\varphi \vee \psi, \neg\varphi \vdash \psi,\ \varphi \vee \psi, \neg\psi \vdash \varphi$

$\neg\varphi \to \psi, \neg\varphi \vdash \psi$ je zřejmé; $\neg\varphi \to \psi \vdash \neg\psi \to \varphi$, tedy $\neg\varphi \to \psi, \neg\psi \vdash \varphi$.

Cvičení.

(1) Ukažte, že následující formule jsou tautologie (bez užití dokazatelností (17)–(20)):
$(\varphi\&\psi) \to \varphi; \varphi \to (\psi \to (\varphi\&\psi)); \varphi \to (\varphi \vee \psi); \psi \to (\varphi \vee \psi)$;
$(\varphi \to \chi) \to ((\psi \to \chi) \to ((\varphi \vee \psi) \to \chi))$.

(2) Rozhodněte, zda následující tvrzení jsou správně:

(i) $\neg\neg p, r \to s, p \to q, \neg q \vee \neg s, (t\&u) \to r \vdash \neg(t\&u)$

(ii) $(\neg p \vee \neg r \vee \neg t) \to z, r \to z, t \to q, p \to s \vdash z$

(iii) $\neg\neg p, r \to s, q \to p, \neg q \vee \neg s, (t\&u) \to r \vdash \neg(t\&u)$

(3) Ukažte, že $\varphi \vee \psi, \neg\psi \vee \chi \vdash \varphi \vee \chi$. (Tzv. princip resoluce) (Např. ukažte, že když $e(\varphi \vee \psi) = e(\neg\psi \vee \chi) = 1$, pak $e(\varphi \vee \chi) = 1$, což stačí díky silné úplnosti)

(4) Ukažte, že existují φ, ψ, χ taková, že $\varphi \vee \psi, \psi \vee \chi \nvdash \varphi \vee \chi$.

Predikátový počet

Nejprve studujme *monadický* predikátový počet.

Jazyk: predikáty $P, Q, \ldots$, konstanty $c, d, \ldots$, proměnná x (jen jedna); logické *spojky* a *kvantifikátory* $\forall$ (velký, universální), $\exists$ (malý, existenční).

Otevřené formule: atomické – tvaru $P(x)$, kde P je predikát. Neatomické otevřené formule se tvoří z otevřených atomických pomocí logických spojek (např. $P(x) \to (Q(x)\&R(x))$.

Uzavřené formule: atomické – tvaru $P(c)$, kde P je predikát a c je konstanta. Je-li $\varphi(x)$ otevřená formule, pak $(\forall x)\varphi(x)$, $(\exists x)\varphi(x)$ jsou uzavřené formule. Další uzavřené formule vznikají z právě popsaných pomocí logických spojek. Např.

$$(\forall x)(P(x) \to Q(x)),\ (\exists x)(P(x)\&\neg Q(x)),\ \text{apod.}$$

Interpretace jazyka je struktura

$$\mathbf{M} = (M, (X_P)_{P\,predikt}, (m_c)_{c\,konstanta}),$$

kde $M \neq 0, X_P \subseteq M$ pro každé P a $m_c \in M$ pro každé c.

Splňování otevřených formulí: značení $\mathbf{M} \models \varphi[m]$, kde $m \in M$ (čti "v M je formule φ splněna prvkem m").

$$\mathbf{M} \models P(x)[m], \text{ jestliže } m \in X_P;$$

$\mathbf{M} \models (\varphi \to \psi)[m]$, jestliže $\mathbf{M} \models \psi[m]$ nebo $\mathbf{M} \not\models \varphi[m]$;

$$M \models \neg\varphi[m], \text{ jestliže } \mathbf{M} \not\models \varphi[m].$$

Pravdivost uzavřených flí: (znač $\mathbf{M} \models \varphi$, φ je pravdivé v $\mathbf{M}$)

$$\mathbf{M} \models P(c), \text{ jestliže } m_c \in X_P$$

$$\mathbf{M} \models (\forall x)\varphi \text{ jestliže pro každé } m \in M \text{ je } \mathbf{M} \models \varphi[m]$$

$$\mathbf{M} \models (\exists x)\varphi \text{ jestliže existuje } m \in M \text{ tak, že } \mathbf{M} \models \varphi[m].$$

Indukční krok pro logické spojky zřejmý.

Příklad

	P	Q
m_1	1	1
m_2	0	1
m_3	0	0
m_4	1	1

$\mathbf{M} \models P[m_1], \mathbf{M} \models \neg P[m_2], \ldots$
$\mathbf{M} \models (P(x) \to Q(x))[m_i], i = 1, \ldots, 4,$
$\mathbf{M} \models (\forall x)(P(x) \to Q(x))$
$\mathbf{M} \models \neg(\forall x)(Q(x) \to P(x))$ apod.

Označení. Buď $(M, (X_P)_{P\ pred.}, (m_c)_{c\ konst.})$ interpretace. Každé otevřené formuli φ přiřadíme množinu X_φ všech prvků, které je splňují. Pro atomické je to dáno přímo interpretací; dále definujeme $X_{\neg\varphi} = M - X_\varphi, X_{\varphi\&\psi} = X_\varphi \cap X_\psi, X_{\varphi\to\psi} = X_{\neg\varphi} \cup X_\psi$ atd.

Tautologie jsou fle pravdivé ve všech interpretacích.

Lemma. Následující fle jsou tautologie:

(1) $\neg(\forall x)\varphi(x) \equiv (\exists x)\neg\varphi(x)$
(2) $\neg(\forall x)(\varphi(x) \to \psi(x)) \equiv (\exists x)(\varphi(x) \& \neg\psi(x))$
(3) $(\forall x)\varphi(x) \to \varphi(c)$ (c konstanta)
(4) $(\forall x)(\varphi(x) \to \psi(x)) \to (\forall x)(\neg\psi(x) \to \neg\varphi(x))$
(5) $\varphi(c) \to (\exists x)\varphi(x)$
(6) $(\forall x)(\varphi(x) \to \psi(x)) \to ((\forall x)\varphi(x) \to (\forall x)\psi(x))$
(7) $(\forall x)(\varphi(x) \to \psi(x)) \to ((\exists x)\varphi(x) \to (\exists x)\psi(x))$

Důkazy: pomocí definice pravdivosti a splňování, např. (1) říká, že $X_\varphi \neq M$, právě když $X_{\neg\varphi} \neq \emptyset$; (2) říká, že X_φ není částí X_ψ, právě když $X_\varphi \cup (M - X_\psi) \neq \emptyset$ atd. (proveďte).

Dedukční pravidlo: má *předpoklady* (fle) a *závěr.* Je *korektní,* když platí: kdykoli jsou pravdivé předpoklady, je pravdivý závěr.

Příklady:

$$\frac{(\forall x)(\varphi(x) \to \psi(x)), (\forall x)(\psi(x) \to \chi(x))}{(\forall x)(\varphi(x) \to \chi(x))} \qquad \frac{(\forall x)(\varphi(x) \to \psi(x))}{(\forall x)(\neg\psi(x) \to \neg\varphi(x))}$$

apod.

Aristotelovy sylogismy

– korektní dedukční pravidla jistého tvaru, vyjádřitelná v monadické logice.

Buďte P, Q predikáty. Aristoteles má čtyři výroky (uzavřené formule) z nich vytvořené:

A	$(\forall x)(P(x) \to Q(x))$, stručně APQ (všechna P jsou Q)
I	$(\exists x)(P(x) \& Q(x))$, stručně IPQ (některá P jsou Q)
E	$(\forall x)(P(x) \to \neg Q(x))$, stručně EPQ (žádné P není Q)
O	$(\exists x)(P(x) \& \neg Q(x))$, stručně OPQ (některá P nejsou Q)

A, I jsou ze slova "affirmo"; E, O jsou ze slova "nego".
A říká: $X_P \subseteq X_Q$;
I říká: X_P protne X_Q ($X_P \cap X_Q \neq \emptyset$);
E říká: X_P je disjunktní s X_Q;
O říká: X_P není částí X_Q.

Sylogismy obsahují tři predikáty: M, S, V (čti: malý, střední, velký – pozor: neplést s označením struktury). Čtyři *typy:*

$$\begin{array}{cccc} SV & VS & SV & VS \\ MS & MS & SM & SM \\ \hline MV & MV & MV & MV \end{array}$$

Konkrétní sylogismus vznikne tak, že každému řádku připíšeme A, I, E nebo O, např. sylogismus "Barbara" – první typ, AAA :

$$\begin{array}{c} ASV \\ AMS \\ \hline AMV \end{array}$$

neboli

$$\begin{array}{c} (\forall x)(S(x) \to V(x)) \\ (\forall x)(M(x) \to S(x)) \\ \hline (\forall x)(M(x) \to V(x)) \end{array}$$

Zřejmě je korektní; pochopitelně můžete dostat nekorektní sylogismus. Aristotelská logika má "básničku", která vypočítává všecky korektní sylogismy (přesněji viz níže) všech čtyř typů a dává jim jména; samohlásky každého jména dávají příslušnou trojici z A, I, E, O.

Barbara, Celarent primae, *Darii, Ferioque;*
Cesare, Camestres, Festino, Baroco secundae;
Tertia grande sonans recitat: (*Darapti, Felapton*),
Disamis, Datisi, Bocardo, Ferison. Quartae
sunt: *(Bamalip), Calemes, Dimatis,* (Fesapo), Fresison.

Tedy např. Fresison je
$$\begin{array}{ll} EVS & (\forall x)(V \rightarrow \neg S) \\ ISM & (\exists x)(S \& M) \\ \hline OMV & (\exists x)(M \& \neg V) \end{array}$$
(ověřte korektnost)

Sylogismy v závorce jsou korektní pouze za předpokladu *neprázdnosti* interpretace některého predikátu; např. Fesapo je korektní, jen když k předpokladům přidáme $(\exists x)S$ (což není formule Aristotelova typu). Říká:

Když disj $(X_V, X_S), X_S \subseteq X_M[$ a $X_S \neq \emptyset]$, pak $X_M \nsubseteq X_V$.

Cvičení: Napište každý korektni sylogismus (z "básničky") ve stručné formě i v jazyce monadické logiky a ověřte korektnost. (Jako pomůcku uveďte význam některých z nich; pišme místo X_M, X_S, X_V prostě M, S, V.)

Typ I:
Barbara: Když $S \subseteq V$ a $M \subseteq S$ pak $M \subseteq V$.
Celarent: Když disj(S, V) a $M \subseteq S$, pak disj(M, V)
Darii: Když $S \subseteq V$ a protne (M, S), pak protne (M, V)
Ferio: Když disj(S, V) a protne (M, S), pak $M \nsubseteq V$.

Typ II:
Cesare: Když disj(V, S) a $M \subseteq S$, pak disj(M, V)

Typ III:
Ferison: Když disj(V, S) a protne (M, S), pak $M \nsubseteq V$ atd.

Klasický predikátový počet

Jazyk: predikáty $P, Q, \ldots$, každý má *četnost* – přirozené čislo (kladné) *konstanty* $c, d, \ldots$, *proměnné* $x, y, \ldots$, dále logické spojky a kvantifikátory.

Termy jsou konstanty a proměnné.

Atomické formule mají tvar $P(t_1, \ldots, t_n)$, kde P je predikát četnosti n a $t_1, \ldots, t_n$ jsou termy. Jsou-li φ, ψ fle, jsou i $\neg\varphi, \varphi \to \psi$ (atd.) fle. Je-li φ fle a x proměnná, pak $(\forall x)\varphi, (\exists x)\varphi$ jsou fle.

Interpretace jazyk je struktura

$$\mathbf{M} = (M, (r_P)_{P\ predikt}, (m_c)_{c\ konstanta}),$$

kde $M \neq \emptyset$, pro každý predikát P četnosti n je $r_P \subseteq M^n$, a pro každou konstantu c je $m_c \in M$.

Ohodnocení proměnných v M, je zobrazení v přiřazující každé proměnné x prvek $v(x) \in M$.

Tarského definice splňování a pravdivosti. Význam termu: $|x|_{\mathbf{M},v} = v(x)$, $|c|_{\mathbf{M},v} = m_c$.

$\mathbf{M} \models P(t_1, \ldots, t_n)[v]$ jestliže n-tice významů termů $t_1, \ldots, t_n$ je v relaci r_P; tj. $(|t_1|_{\mathbf{M},v}, \ldots |t_n|_{\mathbf{M},v}) \in r_P$.

$\mathbf{M} \models \neg\varphi[v]$, jestliže $\mathbf{M} \not\models \varphi[v]$.

$\mathbf{M} \models (\varphi \to \psi)[v]$, jestliže $\mathbf{M} \not\models \varphi[v]$ nebo $\mathbf{M} \models \psi[v]$.

$\mathbf{M} \models (\forall x)\varphi[v]$, jestliže pro každé $v' \equiv_x v$ je $\mathbf{M} \models \varphi[v']$ (kde $v' \equiv_x v$ znamená, že pro všecky proměnné y různé od x je $v'(y) = v(y)$).

$\mathbf{M} \models (\exists x)\varphi[v]$, jestliže existuje $v' \equiv_x v$ tak, že $\mathbf{M} \models \varphi[v']$.

Volné a vázané proměnné. x je volné v atomické formuli, když se v ní vyskytuje. Žádná proměnná není vázaná v atomické formuli.

x je volné/vázané v $\neg\varphi$, právě když je volné/vázané v φ

x je volné/vázané v $\varphi \to \psi$, právě když je volné/vázané v φ nebo v ψ.

x je vázaná ve fli $(\forall x)\varphi$ a není v ní volná. Je-li y proměnná různá od x, pak y je volná/vázaná v $(\forall x)\varphi$, právě když je volná/vázaná ve fli φ. Podobně pro $(\exists x)\varphi$.

Lemma. Když $\mathbf{M} \models \varphi[v]$, x není volné v φ a $v' \equiv_x v$, pak $\mathbf{M} \models \varphi[v']$. (Důkaz indukcí.)

Indukční krok pro $\forall$: ať x není volné v $(\forall y)\varphi, v' \equiv_x v, v' = v(x/a)$. Nechť x je různé od y; pak následující podmínky jsou ekvivalentní:

$\mathbf{M} \models (\forall y)\varphi[v]$,

pro každé $b \in M$: $\mathbf{M} \models \varphi[v(y/b)]$,

pro každé $b \in M$: $\mathbf{M} \models \varphi[v(y/b, x/a)]$ (indukční předpoklad)

pro každé $b \in M$: $\mathbf{M} \models \varphi[v(x/a, y/b)]$,

pro každé $b \in M$: $\mathbf{M} \models \varphi[v'(y/b)]$

a tedy $\mathbf{M} \models (\forall y)\varphi[v']$.

Pro případ, že x je y, je důkaz evidentní:

φ je *pravdivá* v $\mathbf{M}$ jestliže $\mathbf{M} \models \varphi[v]$ pro každé ohodnocení v. *Teorie* je množina formulí (speciálních axiomů). $\mathbf{M}$ je *model* teorie T, jestliže $\mathbf{M} \models \varphi$ pro každé $\varphi \in T$.

Příklad Teorie lineárního kvasiuspořádání.

φ je *tautologie* (predikátového počtu), je-li pravdivá v každé interpretaci.

Lemma. Buď $\psi(p_1, \dots, p_n)$ tautologie výrokového počtu, nechť φ vzniká z ψ substitucí formulí $\varphi_1, \dots \varphi_n$ pred. počtu za výrokové proměnné $p_1, \dots, p_n$. Pak je tautologie predikátového počtu.

Příklad $(\forall x)(\exists y)P(x,y) \to (\forall x)(\exists y)P(x,y)$

Substituce. $\varphi(x/c)$ značí výsledek substituce konstanty c za volné výskyty proměnné x v φ. Podobně $\varphi(x/y)$ pro proměnnou y. (Pedantická definice indukcí podle složitosti formule.)

Př.φ je $(\forall z)(x < z), \varphi(x/c)$ je $(\forall z)(c < z), \varphi(x/y)$ je $(\forall z)(y < z), \varphi(z/y)$ je $(\forall z)(x < y)$.

Lemma. $M \models \varphi(x/c)[v]$, právě když $M \models \varphi[v(x/m_c)]$, kde $v(x/m_c)$ je ohodnocení $v' \equiv_x v$ takové, že $v'(x) = m_c$.

Důkaz: Zřejmé pro φ atomické; indukční krok pro log. spojky sřejmý. Nechť φ je $(\forall z)\psi(x,y)$. Pak následující řádky jsou ekvivalentní:

$M \models (\forall z)\psi(x,z)(x/c)[v]$
$M \models (\forall z)\psi(c,z)[v]$
pro lib. $v' \equiv_z v \quad M \models \psi(c,z)[v']$
pro lib. $v' \equiv_z v \quad M \models \psi(x,z)[v'(x/m_c)]$
pro lib. $v'' \equiv_z v(x/m_c) \quad M \models \psi(x,z)[v'']$
$M \models (\forall z)\psi(x,z)[v(x/m_c)]$

Podobně pro $\varphi(x/y)$, ale *pozor:*

Def. y je *substituovatelné* za x do φ, jestliže φ neobsahuje žádnou podformuli tvaru $(\forall y)\psi$ nebo $(\exists y)\psi$, v níž je x volné.

Lemma Je-li y substituovatelné za x do φ, pak

$$M \models \varphi(x/y)[v], \text{ právě když } \mathbf{M} \models \varphi[v(x/v(y))].$$

Př. y není subst. za x do $(\exists y)(x < y)$. V přirozených číslech je $(\exists y)(x < y)$ splněna každým ohodnocením, ale $(\exists y)(y < y)$ žádným.

Důsledek:

(1) Formule $(\forall x)\varphi \to \varphi(x/c)$ je tautologie.
(2) Pokud je y substituovatelné za x do φ, pak formule $(\forall x)\varphi \to \varphi(x/y)$ je tautologie.
(3) Podobně $\varphi(x/c) \to (\exists x)\varphi, \varphi(x/y) \to (\exists x)\varphi$.

Neboť když $\mathbf{M} \models (\forall x)\varphi[v]$, pak pro libovolné $v' \equiv_x v$ je $\mathbf{M} \models \varphi[v']$, speciálně $\mathbf{M} \models \varphi[v(x/v(y)]$, tedy $\mathbf{M} \models \varphi(x/y)[v]$.

Lemma. Nechť x není volné v ν. Pak fle $(\forall x)(\nu \to \varphi) \to (\nu \to (\forall x)\varphi)$ je tautologie.

Důkaz. Ať $\mathbf{M} \models (\forall x)(\nu \to \varphi)[v]$, tj. pro každé $v' \equiv_x v, \mathbf{M} \models (\nu \to \varphi)[v']$, tedy $[M \not\models \nu[v']$ nebo $\mathbf{M} \models \varphi[v']]$, tedy (pro každé $v' \equiv_x v)[\mathbf{M} \not\models \nu[v]$ nebo $M \models \varphi[v']]$, tedy $[\mathbf{M} \not\models \nu[v]$ nebo pro každé $v' \equiv_x v$ $\mathbf{M} \models \varphi[v']]$, tedy $(\mathbf{M} \not\models \nu[v]$ nebo $M \models (\forall x)\varphi(x))$, tedy $\mathbf{M} \models (\nu \to (\forall x)\varphi[v]$.

Axiomy predikátového počtu pro libovolné fle φ, ψ, χ pred. počtu

$$\varphi \to (\psi \to \varphi),$$

$$(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)),$$

$$(\neg\varphi \to \neg\psi) \to (\psi \to \varphi),$$

(axiomy výrokového počtu) a dále

($\forall$1) $(\forall x)\varphi \to \varphi(x/c)$,

($\forall$1) $(\forall x)\varphi \to \varphi(x/y)$,

pokud y je substituovatelné za x do φ,

($\forall$2) $(\forall x)(\nu \to \varphi) \to (\nu \to (\forall x)\varphi)$, kde x není volné v φ.

Dedukční pravidla: modus ponens a *generalizace:* z φ odvoď $(\forall x)\varphi$. Důkaz, dokazatelnost.

Pozor: $\varphi\&\psi, \varphi \vee \psi, \varphi \equiv \psi$ jsou *zkratky;* $(\exists x)\varphi$ je zkratka za $\neg(\forall x)\neg\varphi$.

Lemma. Následující fle jsou dokazatelné v predikátovém počtu:

(1) $\varphi(x/c) \to (\exists x)\varphi; \varphi(x/y) \to (\exists x)\varphi$ pokud y je substituovatelné za x do φ.

(2) $(\forall x)(\varphi \to \psi) \to ((\forall x)\varphi \to (\forall x)\psi)$

(3) $(\forall x)(\varphi \to \psi) \to ((\exists x)\varphi \to (\exists x)\psi)$

(4) $\nu \equiv (\forall x)\nu, \nu \equiv (\exists x)\nu$, pokud x není volné v ν.

Návod:

(1) Postupně dokažte:
$(\forall x)\neg\varphi \to \neg\varphi(x/c)$
$\varphi(x/c) \to \neg(\forall x)\neg\varphi$.

(2) Postupně dokažte:
$(\forall x)(\varphi \to \psi) \to (\varphi \to \psi)$
$(\forall x)(\varphi \to \psi) \to ((\forall x)\varphi \to \psi)$
$(\forall x)[(\forall x)(\varphi \to \psi) \to ((\forall x)\varphi \to \psi)]$
$(\forall x)(\varphi \to \psi) \to (\forall x)((\forall x)\varphi \to \psi)$
$(\forall x)(\varphi \to \psi) \to ((\forall x)\varphi \to (\forall x)\psi)$

(3) $(\forall x)(\varphi \to \psi) \to (\forall x)(\neg\psi \to \neg\varphi)$ (výrokový počet, generalizace a (2))
$(\forall x)(\neg\psi \to \neg\varphi) \to ((\forall x)\neg\psi \to (\forall x)\neg\varphi)$
$((\forall x)\neg\psi \to (\forall x)\neg\varphi) \to (\neg(\forall x)\neg\varphi \to \neg(\forall x)\neg\psi)$

(4) $(\forall x)\nu \to \nu, (\forall x)(\nu \to \nu), \nu \to (\forall x)\nu$. Podobně $\exists$.

Lemma. Další dokazatelné formule: nechť x není volné v ν.

(5) $(\forall x)(\nu \to \varphi) \equiv (\nu \to (\forall x)\varphi)$

(6) $(\exists x)(\nu \to \varphi) \equiv (\nu \to (\exists x)\varphi)$

(7) $(\forall x)(\varphi \to \nu) \equiv ((\exists x)\varphi \to \nu)$

(8) $(\exists x)(\varphi \to \nu) \equiv ((\forall x)\varphi \to \nu)$

Návod: (5) $\to$ je axiom $(\forall 2)$; dokažte $\leftarrow$ tím, že dokážete $(\nu \to (\forall x)\varphi) \to (\nu \to \varphi)$, generalizujte a užijte axiom $(\forall 2)$.

(6) $(\nu \to \varphi) \to (\nu \to (\exists x)\varphi)$
$\neg(\nu \to (\exists x)\varphi) \to \neg(\nu \to \varphi)$
$\neg(\nu \to (\exists x)\varphi) \to (\forall x)\neg(\nu \to \varphi)$
$(\exists x)(\nu \to \varphi) \to (\nu \to (\exists x)\varphi)$. Obráceně:
$\neg\nu \to (\nu \to \varphi), (\exists x)\neg\nu \to (\exists x)(\nu \to \varphi), \neg\nu \to (\exists x)(\nu \to \varphi)$;
$\varphi \to (\nu \to \varphi), (\exists x)\varphi \to (\exists x)(\nu \to \varphi)$;
$(\neg\nu \vee (\exists x)\varphi) \to (\exists x)(\nu \to \varphi)$;
$(\nu \to (\exists x)\varphi) \to (\exists x)(\nu \to \varphi)$.

(7) Dokažte sérii ekvivalencí: $(\forall x)(\varphi \to \nu) \equiv (\forall x)(\neg\nu \to \neg\varphi) \equiv (\neg\nu \to (\forall x)\neg\varphi) \equiv (\neg(\forall x)\neg\varphi \to \nu) \equiv ((\exists x)\varphi \to \nu)$

(8) Podobně.

Lemma. (přejmenování proměnných). Když y se nevyskytuje v φ, pak $(\forall x)\varphi \equiv (\forall y)\varphi(x/y)$ je dokazatelné.

Návod: Dokažte postupně $(\forall x)\varphi \to \varphi(x/y), (\forall y)((\forall x)\varphi \to \varphi(x/y)), (\forall x)\varphi \to (\forall y)\varphi(x/y)$ a podobně zpět.

Formule v prenexní normální formě (PNF). Otevřené fle jsou v PNF; je-li a v PNF a x je proměnná, pak $(\forall x)\varphi, (\exists x)\varphi$ jsou v PNF. Jiné nejsou.

Věta o PNF. Ke každé fli φ existuje fle φ' v PNF taková, že $\varphi \equiv \varphi'$ je dokazatelná.

Důkaz užitím (5)–(8) a přejmenování vázaných proměnných.

Teorie (jako výše:) množina formulí (spec. axiomů). Důkaz v teorii; $T \vdash \varphi$.

Věta o dedukci pro predikátový počet. Buď T teorie, φ, ψ fle, φ uzavřená. Pak $T \cup \{\varphi\} \vdash \psi$, právě když $T \vdash \varphi \to \psi$.

Důkaz jako ve výrok. počtu, přibude indukční krok pro generalizaci.

Teorie T je *sporná,* jestliže existuje formule φ taková, že $T \vdash \varphi$ a $T \vdash \neg\varphi$. Jinak je bezesporná. (Stejně jako ve výrokovém počtu.)

Lemma. T je sporná, právě když každá fle je dokazatelná.

Gödelova věta o (sémantické) *úplnosti* predikátového počtu. (1) Pro každou fli φ platí: $\vdash \varphi$ (φ je dokazatelné v predikátovém počtu), právě když φ je tautologií pred. počtu (tj. je pravdivá v každé interpretaci).

(2) *Silná věta o (sémantické) úplnosti:* Buď T teorie, φ fle. Pak $T \vdash \varphi$, právě když $\mathbf{M} \models \varphi$ pro každý model $\mathbf{M}$ teorie T.

(Pozn. (1) je speciální případ silné věty.)

Implikace $\Rightarrow$ je (silná) korektnost – viz výše. K obrácení implikace stačí dokázat:

Lemma o modelu. Každá bezesporná teorie T má model.

Proč stačí: Ať platí lemma a ať $T \not\vdash \varphi$. Lze předpokládat φ *uzavřené.* Pak $T' = T \cup \{\neg\varphi\}$ je bezesporná teorie (proč? – užijte dokazatelnost (12) vy výrokovém počtu), tedy existuje její model $\mathbf{M}$. Tedy $\mathbf{M}$ je model teorie T, v němž φ není pravdivé.

V dalším pracujeme na důkazu lemmatu.

T je *rozšíření* teorie T, jestliže jazyk teorie T je podjazykem teorie T' a každý axiom teorie T je dokazatelný v T'. Rozšíření T' teorie T je *konservativní,* protože každá fle jazyka teorie T dokazatelná v teorii T' je dokazatelná v T.

Lemma. Buď T teorie, $\varphi(x)$ fle jejího jazyka s jedinou volnou proměnnou x, buď c konstanta, která není v jazyku teorie T. Pak teorie $T \cup \{(\exists x)\varphi(x) \rightarrow \varphi(c)\}$ je konservativní rozšíření teorie T. (Pozn. přidaný axiom lze pedanticky psát $(\exists x)\varphi \rightarrow \varphi(x/c)$.)

Důkaz. Ať $T' \vdash \psi$, kde ψ je uzavřená fle neobsahující konstantu c. Pak
$T \vdash ((\exists x)\varphi(x) \rightarrow \varphi(c)) \rightarrow \psi$ (věta o dedukci),
$T \vdash ((\exists x)\varphi(x) \rightarrow \varphi(y)) \rightarrow \psi$, kde y je proměnná nepoužitá v předcházejícím důkazu,
$T \vdash (\forall y)[((\exists x)\varphi(x) \rightarrow \varphi(y)) \rightarrow \psi]$,
$T \vdash (\exists y)((\exists x)\varphi(x) \rightarrow \varphi(y)) \rightarrow \psi$,
$T \vdash [(\exists y)\varphi(x) \rightarrow (\exists y)\varphi(y)] \rightarrow \psi$,
$T \vdash \psi$.

Poznámka. Mlčky předpokládejme, že pracujeme s teoriemi, jejichž jazyk je nejvýše spočetný, tudíž i množina všech flí je spočetná.

Teorie T je *Henkinovská,* jestliže pro každou uzavřenou fli $(\exists x)\varphi(x)$ jejího jazyka existuje konstanta c taková, že $T \vdash (\exists x)\varphi(x) \rightarrow \varphi(c)$.

Iterací předchozího lemmatu dostáváme:

Lemma. Každá teorie má konservativní henkinovské rozšíření.

Teorie T je (deduktivně) úplná, jestliže pro každou uzavřenou fli φ je $T \vdash \varphi$ nebo $T \vdash \neg\varphi$. (Pozor na rozdíl proti výrokovému počtu.)

Lemma. Každá bezesporná teorie T má bezesporné úplné rozšíření.

Důkaz (jako ve výr. počtu). Buď $\varphi_0, \varphi_1, \varphi_2, \ldots$ posloupnost všech uzavřených flí, buď $T_0 = T$. Je-li T_n sestrojeno a $T_n \vdash \varphi_n$, buď $T_{n+1} = T_n$, jinak buď $T_{n+1} = T_n \cup \{\neg\varphi_n\}$. Buď $\hat{T} = \bigcup_{n=0}^{\infty} T_n$; $\hat{T}$ je hledaná teorie.

Lemma. Každá bezesporná úplná henkinovská teorie má model $\mathbf{M}$.

Důkaz. Buď M množina všech konstant teorie T. Pro libovolné konstanty $c_1, \ldots c_n, c$ z M buď $(c_1, \ldots, c_n) \in r_P$, právě když $T \vdash P(c_1, \ldots, c_n)$; buď $m_c = c$. Tím je $\mathbf{M}$ dáno; ověřte indukcí dle složitosti formulí, že pro každou uzavřenou fli φ platí

$$M \models \varphi, \text{ právě když } T \vdash \varphi.$$

(Důkaz pro negaci užívá bezespornost a úplnost, pro kvantifikátory henkinovskost.)

Důsledek. Tedy každá bezesporná teorie má model. Tím je dokázáno lemma o modelu a tedy: (silná) Gödelova věta o úplnosti.

Věta o kompaktnosti. Buď T libovolná teorie. T má model, právě když každá její konečná podteorie má model. (Neboť nemá-li T model, pak je sporná, tedy nějaká její konečná podteorie T_0 je sporná a tedy nemá model.)

Definice.
(1) Teorie daného modelu $\mathbf{M}$ je množina $Th(\mathbf{M}) = \{\varphi | \mathbf{M} \models \varphi\}$ (množina všech formulí pravdivých v $\mathbf{M}$).
(2) Buďte $\mathbf{M}, \mathbf{M}'$ dva modely. $\mathbf{M}$ je *elementárně ekvivalentní* s $\mathbf{M}'$ (značení $\mathbf{M} \equiv \mathbf{M}'$, jestliže $Th(\mathbf{M}) = Th(\mathbf{M}')$.
(3) Buď $\mathbf{M}$ model jazyka $L, \mathbf{M}'$ model jazyka $L' \supseteq L$. $\mathbf{M}'$ je *expanze* modelu $\mathbf{M}$, mají-li oba modely týž nosič (universum) a tytéž interpretace predikátů a konstant z L.

Věta. Buď T teorie v jazyce L, T' teorie v jazyce $L' \supseteq L$. T' je konservativní rozšíření teorie T, právě když ke každému modelu $\mathbf{M}$ teorie T existuje elementárně ekvivalentní model $\mathbf{M}'$ a expanze $\mathbf{M}''$ modelu $\mathbf{M}'$ taková, že $\mathbf{M}''$ je model teorie T'.

Důkaz – návod. Když T' není konservativní rozšíření T, pak buď φ uzavřená formule jazyka T dokazatelná v T', ale ne v T; buď $\mathbf{M}$ model teorie $T \cup \{\neg\varphi\}$. K němu neexistují $\mathbf{M}'$ a $\mathbf{M}''$ splňující podmínky věty. Když T' je konservativní rozšíření T a $\mathbf{M}$ je model T, pak $Th(\mathbf{M}) \cup T'$ je bezesporná (proč?) a má model $\mathbf{M}''$ který (se svou restrikcí $\mathbf{M}'$ na jazyk L) splňuje podmínky věty.

Klasický predikátový počet s funkcemi a rovností

Symboly: predikáty, proměnné, konstanty, logické spojky a kvantifikátory – jako dříve. K tomu: speciální binární predikát = (rovnítko); funkční symboly $F_1, F_2, \ldots$, každý se svou *četností* (kladné přirozené číslo).

Termy: Proměnné a konstanty jsou atomické termy. Je-li F n-ární funkční symbol a jsou-li $t_1, \ldots, t_n$ termy, pak $F(t_1, \ldots t_n)$ je term.

Interpretace:
$\mathbf{M} = (M, (r_P)_{P \text{ predikát}}, (m_c)_{c \text{ konstanta}}, (f_F)_{F \text{ fční symbol}})$ kde vše je jako dříve, a pro každý n-ární funkční symbol F je $f : M^n \to M$ n-ární operace na m; dále $r_= = \{(a,a) | a \in M\}$.

Hodnota termu $|t|_{\mathbf{M},v}$. Pro atomické termy jako dříve;
$|F(t_1, \ldots, t_n)|_{\mathbf{M},v} = f_F(|t_1|_{\mathbf{M},v}, \ldots, |t_n|_{\mathbf{M},v})$.
$\|\varphi\|_{\mathbf{M},v}$ jako dříve.

Axiomy logiky: jako dříve, jen $(\forall 1)$ se změní na

$$(\forall x)\varphi \to \varphi(x/t)$$

kde t je term substituovatelný za x do φ, tj. žádná proměnná y termu t se nevyskytuje v žádné podformuli formule φ tvaru $(\forall y)\psi$ (nebo $(\exists y)\psi$) takové, že x je volné v ψ.

Dalšími axiomy logiky jsou *axiomy rovnosti,*

$x = x$ (reflexivita)

$x = y \to y = x$ (symetrie)

$(x = y \& y = z) \to x = z$ (transitivita)

$$(x_1 = y_1 \& \ldots \& x_n = y_n) \to (P(x_1, \ldots x_n) \equiv P(y_1 \ldots y_n))$$

pro každý n-ární predikát P,

$$x_1 = y_1 \& \ldots \& x_n \ldots y_n) \to (F(x_1, \ldots, x_n) = F(y_1, \ldots, y_n)$$

pro každý n-ární funkční symbol F.

Pojem důkazu v logice, teorie důkazu v teorii, dokazatelnosti, modelu teorie – zřejmé.

Lemma (1) Buď $\varphi(x_1, \ldots, x_n)$ formule s volnými proměnnými $x_1, \ldots x_n$.
Pak

$$\vdash (x_1 = y_1 \& \ldots \& x_n = y_n) \to (\varphi(x_1 \ldots x_n) \equiv \varphi(y_1, \ldots, y_n))$$

(2) Buď $t(x_1, \ldots, x_n)$ term s proměnnými $x_1, \ldots x_n$.
Pak

$$\vdash (x_1 = y_1 \& \ldots \& x_n = y_n) \to (t(x_1 \ldots x_n) = t(y_1, \ldots, y_n))$$

Gödelova věta o úplnosti platí ve stejném znění. Při sestrojování modelu k bezesporné henkinovské teorii T vezměte za M množinu všech *uzavřených termů* (vybudovaných z konstant a funkčních symbolů); definujte $f_F(t_1, \ldots t_n) = F(t_1, \ldots t_n)$. Jinak vše stejné. Tím dostanete model s *neabsolutní rovností;*

Zbývá faktorizovat: $[t]_{\mathbf{M}} = \{s | \mathbf{M} \models t = s\}$, $\hat{M} = \{[t]_{\mathbf{M}} | t$ uzavřený term$\}$,
$\hat{r}_P = \{([t_1]_{\mathbf{M}} \ldots [t_n]_{\mathbf{M}}) | (t_1, \ldots, t_n| \in r_P\}$
$\hat{f}_F([f_1]_{\mathbf{M}}, \ldots, [t_n]_{\hat{\mathbf{M}}}) = [F(t_1, \ldots, t_n)]_{\mathbf{M}}$.

Pak ukažte $\hat{M} \models \varphi(t_1, \ldots t_n)$ právě když $M \models \varphi(t_1, \ldots t_n)$; nadto $\hat{r}_= = \{([t]_{\mathbf{M}}, [t]_{\mathbf{M}}) |\ t$ uzavřený term$\}$.

Příklad: Axiomatická aritmetika

Jazyk: predikáty $=, \leq$ (binární), konstanta $\bar{0}$, funkční symboly S (unární), dále $+$ a $*$ (binární).

Standardní interpretace: množina přirozených čísel s rovností, relací menší–rovno, nulou, následníkem (přičítání jedničky), sčítáním a násobením.

Metamatematika aritmetiky (přehled)

Axiomy Robinsonovy aritmetiky Q :

$(Q1)$ $S(x) \neq \bar{0}$
$(Q2)$ $S(x) = S(y) \rightarrow x = y$
$(Q3)$ $x \neq 0 \rightarrow (\exists y)(x = S(y))$
$(Q4)$ $x + \bar{0} = x$
$(Q5)$ $x + S(y) = S(x + y)$
$(Q6)$ $x * \bar{0} = \bar{0}$
$(Q7)$ $x * S(y) = (x * y) + x$
$(Q8)$ $x \leq y \equiv (\exists z)(z + x = y)$

(Všechny jsou pravdivé ve standardním modelu $\mathbf{N}$.)

Peanova aritmetika PA : axiomy $(Q1) - (Q8)$ a pro každou formuli φ (jazyka aritmetiky) axiom indukce

$$(\varphi(\bar{0})\&(\forall x)(\varphi(x) \rightarrow \varphi(S(x))) \rightarrow (\forall x)\varphi(x).$$

Dokažte: $Q \vdash \bar{0} + \bar{0} = \bar{0}$;
$Q \vdash \bar{0} + x = x \rightarrow \bar{0} + S(x) = S(x)$;
$PA \vdash (\forall x)(\bar{0} + x = x)$
$PA \vdash (\forall y)(S(x) + y = S(x + y))$
$PA \vdash x + y = y + x$

$Tr(\mathbf{N}) = \{\varphi | \mathbf{N} \models \varphi\}$. *Korektnost:* Když $PA \models \varphi$ pak $\varphi \in Tr(\mathbf{N})$.

(Formule dokazatelné v PA jsou pravdivé ve standardním modelu $\mathbf{N}$ aritmetiky.)

Lze obrátit?

Uvažujme teorie $T \supseteq Q$. T je *rekursivně axiomatizovaná,* jestliže existuje algoritmus, který pro každou fli φ rozhodne, zda je nebo není axiomem teorie T.

Numerály: $\bar{n}$ je $S(\ldots S(\bar{0})\ldots)$ (n symbolů S). Zřejmě $\bar{n}$ znamená v $\mathbf{N}$ číslo n. Formule jsou jisté konečné posloupnosti symbolů, lze je kódovat přirozenými čísly. Také důkazy lze kódovat čísly (jsou to jisté posloupnosti formulí). Má tedy smysl $\bar{\varphi}$ pro formuli φ, $\bar{d}$ pro důkaz d. Při vhodném kódování je množina všech formulí rekursivní; pokud je T rekursivně axiomatizovaná, je množina všech důkazů v teorii T rekursivní. (*Pozor:* množina všech formulí dokazatelných v T nemusí být rekursivní!)

Gödelovo diagonální lemma: Pro každou fli $\psi(x)$ jazyka aritmetiky s jedinou volnou proměnnou x existuje uzavřená fle φ taková, že

$$Q \vdash \varphi \equiv \psi(\bar{\varphi})$$

(autoreferenční fle: říká "já mám vlastnost ψ").

Omezené kvantifikátory: $(\forall x \leq y)\varphi$ je $(\forall x)(x \leq y \rightarrow \varphi)$. Podobně $(\exists x \leq y)\varphi$ je $(\exists x)(x \leq y \& \varphi)$. *Omezená formule:* všechny kvantifikátory v ní jsou omezené. φ je Σ_1-formule, jestliže má tvar $(\exists x)\varphi$, kde φ je omezená.

Σ_1-*úplnost aritmetiky:* Je-li φ uzavřená Σ_1-formule pravdivá v $\mathbf{N}$, pak $Q \vdash \varphi$.

Fakt: Je-li T rekursivně axiomatizované, pak existuje Σ_1-formule $D(x)$ definující v $\mathbf{N}$ formule dokazatelné v T : pro každou fli φ,

$$T \vdash \varphi, \text{ právě když } \mathbf{N} \models D(\bar{\varphi}).$$

Gödelova fle G : splňuje $Q \vdash G \equiv \neg D(\bar{G})$ (říká: "já nejsem dokazatelná").

První Gödelova věta o (deduktivní) neúplnosti. Buď T teorie v jazyce aritmetiky, $T \supseteq Q$, T rekursivně axiomatizovaná, buď $\mathbf{N}$ model T. Pak Gödelova fle G není v T ani dokazatelná ani vyvratitelná (T nedokazuje G, T nedokazuje $\neg G$).

Důkaz: Když $T \vdash G$, pak $N \models D(G)$, tedy $T \vdash D(G)$, tedy $T \vdash \neg G$ a T je sporná. Když $T \vdash \neg G$, pak $T \vdash D(G)$, tedy $\mathbf{N} \models D(G)$, tedy $T \vdash G$ a T je sporná.

Tedy každá bezesporná rekursivně axiomatizovaná teorie T obsahující Q je (deduktivně) neúplná.

Důsledek (nerozhodnutelnost aritmetiky). Každá taková teorie T je *nerozhodnutelná,* tj. neexistuje algoritmus, který by pro každou fli φ rozhodoval, zda je či není dokazatelná v T. (Kdyby T byla rozhodnutelná, šlo by sestrojit její bezesporné rekursivní deduktivně úplné rozšíření.)

Další důsledek. Existují nestandardní modely aritmetiky PA. (Buď φ uzavřená taková, že $PA \not\vdash \varphi$, $PA \not\vdash \neg\varphi$, nechť např. $\mathbf{N} \models \varphi$. Pak $PA \cup \{\neg\varphi\}$ má model $\mathbf{M}$ neisomorfní s $\mathbf{N}$.)

Buď φ fle $\bar{0} = \bar{1}$ (tj. $\bar{0} = S\bar{0}$)), buď Con_T fle $\neg D(\bar{\varphi})$ (vyjadřuje bezespornost: říká, že fle $\bar{0} = \bar{1}$ není dokazatelná.

Fakt. Za dalších rozumných podmínek na T (splněných např. teorií PA) platí $T \vdash Con_T \equiv G$, tedy $T \not\vdash Con_T$ a $T \not\vdash \neg Con_T$. (Nedokazatelnost bezespornosti: žádná "rozumná" matematická teorie nemůže dokázat svou vlastní bezespornost.)

To je tzv. Druhá Gödelova věta o (deduktivní) neúplnosti.