Výroková a predikátová logika - X

Petr Gregor

KTIML MFF UK

ZS 2018/2019

Rozšiřování teorií

Ukážeme, že zavádění nových pojmů má "pomocný charakter".

Tvrzení *Nechť T je teorie jazyka L, T' je teorie jazyka L' a $L \subseteq L'$.*

(i) *T' je extenze T, právě když redukt $\mathcal{A}$ každého modelu $\mathcal{A}'$ teorie T' na jazyk L je modelem teorie T,*

(ii) *T' je konzervativní extenze T, je-li T' extenze T a každý model $\mathcal{A}$ teorie T lze expandovat do jazyka L' na model $\mathcal{A}'$ teorie T'.*

Důkaz

$(i)a)$ Je-li T' extenze T a φ libovolný axiom T, pak $T' \models \varphi$. Tedy $\mathcal{A}' \models \varphi$ a rovněž $\mathcal{A} \models \varphi$, z čehož plyne, že $\mathcal{A}$ je modelem T.

$(i)b)$ Je-li $\mathcal{A}$ modelem T a $T \models \varphi$, kde φ je jazyka L, pak $\mathcal{A} \models \varphi$ a rovněž $\mathcal{A}' \models \varphi$. Z toho plyne, že $T' \models \varphi$ a tedy T' je extenze T.

(ii) Je-li $T' \models \varphi$, kde φ je nad L, a $\mathcal{A}$ je model T, pak v nějaké jeho expanzi $\mathcal{A}' \models \varphi$ a tedy $\mathcal{A} \models \varphi$. Z čehož $T \models \varphi$, tj. T' je konzervativní. $\square$

Extenze o definovaný relační symbol

Nechť T je teorie jazyka L, $\psi(x_1, \ldots, x_n)$ je formule jazyka L ve volných proměnných $x_1, \ldots, x_n$ a L' je rozšíření L o nový n-ární relační symbol R.

Extenze teorie T *o definici* R formulí ψ je teorie T' vzniklá přidáním axiomu

$$R(x_1, \ldots, x_n) \;\leftrightarrow\; \psi(x_1, \ldots, x_n)$$

Pozorování *Každý model teorie T lze jednoznačně expandovat na model T'.*

Důsledek *T' je konzervativní extenze T.*

Tvrzení *Pro každou formuli φ' nad L' existuje φ nad L, t.ž. $T' \models \varphi' \leftrightarrow \varphi$.*

Důkaz Každou podformuli $R(t_1, \ldots, t_n)$ nahradíme za $\psi'(x_1/t_1, \ldots, x_n/t_n)$, kde ψ' je vhodná varianta ψ zaručující substituovatelnost všech termů. □

Např. symbol $\leq$ lze zavést v jazyce aritmetiky pomocí axiomu

$$x_1 \leq x_2 \;\leftrightarrow\; (\exists y)(x_1 + y = x_2)$$

Extenze o definovaný funkční symbol

Nechť T je teorie jazyka L a pro formuli $\psi(x_1, \ldots, x_n, y)$ jazyka L ve volných proměnných $x_1, \ldots, x_n, y$ platí

$T \models (\exists y)\psi(x_1, \ldots, x_n, y)$ (existence)

$T \models \psi(x_1, \ldots, x_n, y) \ \wedge \ \psi(x_1, \ldots, x_n, z) \ \rightarrow \ y = z$ (jednoznačnost)

Označme L' rozšíření L o nový n-ární funkční symbol f.

Extenze teorie T *o definici f* formulí ψ je teorie T' vzniklá přidáním axiomu

$$f(x_1, \ldots, x_n) = y \ \leftrightarrow \ \psi(x_1, \ldots, x_n, y)$$

Poznámka *Je-li ψ tvaru $t(x_1, \ldots, x_n) = y$, kde $x_1, \ldots, x_n$ jsou proměnné termu t, podmínky existence a jednoznačnosti platí.*

Např. binární funkční symbol $-$ lze zavést pomocí $+$ a unárního $-$ axiomem

$$x_1 - x_2 = y \ \leftrightarrow \ x_1 + (-x_2) = y$$

Extenze o definovaný funkční symbol (pokr.)

Pozorování *Každý model teorie T lze jednoznačně expandovat na model T'.*

Důsledek *T' je konzervativní extenze T.*

Tvrzení *Pro každou formuli φ' nad L' existuje φ nad L, t.ž. $T' \models \varphi' \leftrightarrow \varphi$.*

Důkaz Stačí uvážit φ' s jediným výskytem f. Má-li φ' více výskytů f, lze postup aplikovat induktivně (v případě vnořených výskytů jdeme od vnitřních k vnějším). Označme φ^* formuli vzniklou z φ' nahrazením termu $f(t_1, \ldots, t_n)$ za novou proměnnou z. Za φ vezmeme formuli

$$(\exists z)(\varphi^* \ \wedge \ \psi'(x_1/t_1, \ldots, x_n/t_n, y/z)),$$

kde ψ' je vhodná varianta ψ zaručující substituovatelnost všech termů.

Nechť $\mathcal{A}$ je model T', e je ohodnocení, $a = f^A(t_1, \ldots, t_n)[e]$. Díky oběma podmínkám platí $\mathcal{A} \models \psi'(x_1/t_1, \ldots, x_n/t_n, y/z)[e]$ právě když $e(z) = a$. Tedy

$$\mathcal{A} \models \varphi[e] \quad \Leftrightarrow \quad \mathcal{A} \models \varphi^*[e(z/a)] \quad \Leftrightarrow \quad \mathcal{A} \models \varphi'[e]$$

pro každé ohodnocení e, tj. $\mathcal{A} \models \varphi' \leftrightarrow \varphi$ a tedy $T' \models \varphi' \leftrightarrow \varphi$. $\square$

Extenze o definice

Teorie T' jazyka L' je *extenze* teorie T jazyka L *o definice*, pokud vznikla z T postupnou extenzí o definici relačního či funkčního symbolu.

Důsledek *Nechť T' je extenze teorie T o definice. Pak*

- *každý model teorie T lze jednoznačně expandovat na model T',*
- *T' je konzervativní extenze T,*
- *pro každou formuli φ' nad L' existuje φ nad L taková, že $T' \models \varphi' \leftrightarrow \varphi$.*

Např. v teorii $T = \{(\exists y)(x + y = 0), (x + y = 0) \wedge (x + z = 0) \rightarrow y = z\}$ nad $L = \langle +, 0, \leq \rangle$ s rovností lze zavést $<$ a unární funkční symbol $-$ axiomy

$$-x = y \quad \leftrightarrow \quad x + y = 0$$
$$x < y \quad \leftrightarrow \quad x \leq y \ \wedge \ \neg(x = y)$$

Pak formule $-x < y$ je v této extenzi o definice ekvivalentní formuli

$$(\exists z)((z \leq y \ \wedge \ \neg(z = y)) \ \wedge \ x + z = 0).$$

Ekvisplnitelnost

Ukážeme, že problém splnitelnosti lze redukovat na otevřené teorie.

- Teorie T, T' jsou *ekvisplnitelné*, jestliže T má model $\Leftrightarrow$ T' má model.
- Formule φ je v *prenexním (normálním) tvaru (PNF)*, má-li tvar
$$(Q_1x_1)\dots(Q_nx_n)\varphi',$$
kde Q_i značí $\forall$ nebo $\exists$, proměnné $x_1,\dots,x_n$ jsou navzájem různé a φ' je otevřená formule, zvaná *otevřené jádro*. $(Q_1x_1)\dots(Q_nx_n)$ je tzv. *prefix*.
- Speciálně, jsou-li všechny kvantifikátory $\forall$, je φ *univerzální* formule.

K teorii T nalezneme ekvisplnitelnou otevřenou teorii následujícím postupem.

(1) Axiomy teorie T nahradíme za ekvivalentní formule v prenexním tvaru.

(2) Pomocí nových funkčních symbolů je převedeme na univerzální formule, tzv. Skolemovy varianty, čímž dostaneme ekvisplnitelnou teorii.

(3) Jejich otevřená jádra budou tvořit hledanou teorii.

Vytýkání kvantifikátorů

Nechť Q značí kvantifikátor $\forall$ nebo $\exists$ a $\overline{Q}$ značí opačný kvantifikátor.
Pro každé formule φ, ψ takové, že x není volná ve formuli ψ,

$$\begin{array}{lrcl}
\models & \neg(Qx)\varphi & \leftrightarrow & (\overline{Q}x)\neg\varphi \\
\models & ((Qx)\varphi \wedge \psi) & \leftrightarrow & (Qx)(\varphi \wedge \psi) \\
\models & ((Qx)\varphi \vee \psi) & \leftrightarrow & (Qx)(\varphi \vee \psi) \\
\models & ((Qx)\varphi \rightarrow \psi) & \leftrightarrow & (\overline{Q}x)(\varphi \rightarrow \psi) \\
\models & (\psi \rightarrow (Qx)\varphi) & \leftrightarrow & (Qx)(\psi \rightarrow \varphi)
\end{array}$$

Uvedené ekvivalence lze ověřit sémanticky nebo dokázat tablo metodou (*přes generální uzávěr, není-li to sentence*).

Poznámka *Předpoklad, že x není volná ve formuli ψ je v každé ekvivalenci (kromě té první) nutný pro nějaký kvantifikátor Q. Např.*

$$\not\models \ ((\exists x)P(x) \wedge P(x)) \ \leftrightarrow \ (\exists x)(P(x) \wedge P(x))$$

Převod na prenexní tvar

Tvrzení *Nechť φ' je formule vzniklá z formule φ nahrazením některých výskytů podformule ψ za formuli ψ'. Jestliže $T \models \psi \leftrightarrow \psi'$, pak $T \models \varphi \leftrightarrow \varphi'$.*

Důkaz Snadno indukcí dle struktury formule φ. □

Tvrzení *Ke každé formuli φ existuje ekvivalentní formule φ' v prenexním normálním tvaru, tj. $\models \varphi \leftrightarrow \varphi'$.*

Důkaz Indukcí dle struktury φ pomocí vytýkání kvantifikátorů, náhradou podformulí za jejich varianty a využitím předchozího tvrzení o ekvivalenci. □

Např.

$$\begin{aligned}
((\forall z)P(x,z) \wedge P(y,z)) &\rightarrow \neg(\exists x)P(x,y)\\
((\forall u)P(x,u) \wedge P(y,z)) &\rightarrow (\forall x)\neg P(x,y)\\
(\forall u)(P(x,u) \wedge P(y,z)) &\rightarrow (\forall v)\neg P(v,y)\\
(\exists u)((P(x,u) \wedge P(y,z)) &\rightarrow (\forall v)\neg P(v,y))\\
(\exists u)(\forall v)((P(x,u) \wedge P(y,z)) &\rightarrow \neg P(v,y))
\end{aligned}$$

Skolemova varianta

Nechť φ je sentence jazyka L v prenexním normálním tvaru, $y_1, \ldots, y_n$ jsou existenčně kvantifikované proměnné ve φ (v tomto pořadí) a pro každé $i \leq n$ nechť $x_1, \ldots, x_{n_i}$ jsou univerzálně kvantifikované proměnné před y_i. Označme L' rozšíření L o nové n_i-ární funkční symboly f_i pro každé $i \leq n$.

Nechť φ_S je formule jazyka L', jež vznikne z formule φ odstraněním $(\exists y_i)$ z jejího prefixu a nahrazením každého výskytu proměnné y_i za term $f_i(x_1, \ldots, x_{n_i})$. Pak formule φ_S se nazývá *Skolemova varianta* formule φ.

Např. pro formuli φ

$$(\exists y_1)(\forall x_1)(\forall x_2)(\exists y_2)(\forall x_3)R(y_1, x_1, x_2, y_2, x_3)$$

je následují formule φ_S její Skolemovou variantou

$$(\forall x_1)(\forall x_2)(\forall x_3)R(f_1, x_1, x_2, f_2(x_1, x_2), x_3),$$

kde f_1 je nový konstantní symbol a f_2 je nový binární funkční symbol.

Vlastnosti Skolemovy varianty

Lemma *Nechť* φ *je sentence* $(\forall x_1)\dots(\forall x_n)(\exists y)\psi$ *jazyka* L *a* φ' *je sentence* $(\forall x_1)\dots(\forall x_n)\psi(y/f(x_1,\dots,x_n))$*, kde* f *je nový funkční symbol. Pak*

(1) *redukt* $\mathcal{A}$ *každého modelu* $\mathcal{A}'$ *formule* φ' *na jazyk* L *je modelem* φ*,*

(2) *každý model* $\mathcal{A}$ *formule* φ *lze expandovat na model* $\mathcal{A}'$ *formule* φ'*.*

Poznámka Na rozdíl od extenze o definici funkčního symbolu, expanze v tvrzení (2) *tentokrát nemusí být jednoznačná.*

Důkaz (1) Nechť $\mathcal{A}' \models \varphi'$ a $\mathcal{A}$ je redukt $\mathcal{A}'$ na jazyk L. Jelikož pro každé ohodnocení e je $\mathcal{A} \models \psi[e(y/a)]$, kde $a = (f(x_1,\dots,x_n))^{A'}[e]$, platí $\mathcal{A} \models \varphi$.
(2) Nechť $\mathcal{A} \models \varphi$. Pak existuje funkce $f^A\colon A^n \to A$ taková, že pro každé ohodnocení e platí $\mathcal{A} \models \psi[e(y/a)]$, kde $a = f^A(e(x_1),\dots,e(x_n))$, a tedy expanze $\mathcal{A}'$ struktury $\mathcal{A}$ o funkci f^A je modelem φ'. $\square$

Důsledek *Je-li* φ' *Skolemova varianta formule* φ*, obě tvrzení* (1) *a* (2) *pro* φ*,* φ' *rovněž platí. Tedy* φ*,* φ' *jsou ekvisplnitelné.*

Skolemova věta

Věta *Každá teorie T má otevřenou konzervativní extenzi T^*.*

Důkaz Lze předpokládat, že T je v uzavřeném tvaru. Nechť L je její jazyk.

- Nahrazením každého axiomu teorie T za ekvivalentní formuli v prenexním tvaru získáme ekvivalentní teorii T°.
- Nahrazením každého axiomu teorie T° za jeho Skolemovu variantu získáme teorii T' rozšířeného jazyka L'.
- Jelikož je redukt každého modelu teorie T' na jazyk L modelem teorie T, je T' extenze T.
- Jelikož i každý model teorie T lze expandovat na model teorie T', je to extenze konzervativní.
- Jelikož každý axiom teorie T' je univerzální sentence, jejich nahrazením za otevřená jádra získáme otevřenou teorii T^* ekvivalentní s T'. $\square$

Důsledek *Ke každé teorii existuje ekvisplnitelná otevřená teorie.*

Redukce nesplnitelnosti na úroveň VL

Je-li otevřená teorie nesplnitelná, lze to “doložit na konkrétních prvcích”.

Např. teorie

$$T = \{P(x,y) \vee R(x,y),\ \neg P(c,y),\ \neg R(x,f(x))\}$$

jazyka $L = \langle P, R, f, c\rangle$ nemá model, což lze doložit nesplnitelnou konjunkcí konečně mnoha instancí (některých) axiomů teorie T v konstantních termech

$$(P(c,f(c)) \vee R(c,f(c)))\ \wedge\ \neg P(c,f(c))\ \wedge\ \neg R(c,f(c)),$$

což je lživá formule ve tvaru výroku

$$(p \vee r)\ \wedge\ \neg p\ \wedge\ \neg r.$$

Instance $\varphi(x_1/t_1, \ldots, x_n/t_n)$ otevřené formule φ ve volných proměnných $x_1, \ldots, x_n$ je *základní (ground) instance*, jsou-li všechny termy $t_1, \ldots, t_n$ konstantní. Konstantní termy nazýváme také *základní (ground) termy*.

Herbrandův model

Nechť $L = \langle \mathcal{R}, \mathcal{F} \rangle$ je jazyk s alespoň jedním konstantním symbolem.
(Je-li třeba, do L přidáme nový konstantní symbol.)

- *Herbrandovo univerzum* pro L je množina všech konstantních termů z L.
  Např. pro $L = \langle P, f, c \rangle$, kde P je relační, f je binární funkční, c konstantní
  $$A = \{c, f(c,c), f(f(c,c),c), f(c, f(c,c)), f(f(c,c), f(c,c)), \dots\}$$
- Struktura $\mathcal{A}$ pro L je *Herbrandova struktura*, je-li doména A Herbrandovo univerzum pro L a pro každý n-ární funkční symbol $f \in \mathcal{F}$ a $t_1, \dots, t_n \in A$,
  $$f^A(t_1, \dots, t_n) = f(t_1, \dots, t_n)$$
  (včetně $n = 0$, tj. $c^A = c$ pro každý konstantní symbol c).
  Poznámka *Na rozdíl od kanonické struktury nejsou předepsané relace.*
  Např. $\mathcal{A} = \langle A, P^A, f^A, c^A \rangle$, kde $P^A = \emptyset$, $c^A = c$ a $f^A(c,c) = f(c,c)$, ...
- *Herbrandův model* teorie T je Herbrandova struktura, jež je modelem T.

Herbrandova věta

Věta *Nechť T je otevřená teorie jazyka L bez rovnosti a s alespoň jedním konstantním symbolem. Pak*

(a) *T má Herbrandův model, anebo*

(b) *existuje konečně mnoho základních instancí axiomů z T, jejichž konjunkce je nesplnitelná, a tedy T nemá model.*

Důkaz Nechť T' je množina všech základních instancí axiomů z T. Uvažme dokončené (např. systematické) tablo τ z T' v jazyce L (bez přidávání nových konstant) s položkou $F\perp$ v kořeni.

- Obsahuje-li tablo τ bezespornou větev V, kanonický model z větve V je Herbrandovým modelem teorie T.
- Jinak je τ sporné, tj. $T' \vdash \perp$. Navíc je konečné, tedy $\perp$ je dokazatelný jen z konečně mnoha formulí T', tj. jejich konjunkce je nesplnitelná. $\square$

Poznámka *V případě jazyka L s rovností teorii T rozšíříme na T^* o axiomy rovnosti pro L a pokud T^* má Herbrandův model $\mathcal{A}$, zfaktorizujeme ho dle $=^{\mathcal{A}}$.*

Důsledky Herbrandovy věty

Nechť L je jazyk obsahující alespoň jeden konstantní symbol.

Důsledek *Pro každou otevřenou $\varphi(x_1, \dots, x_n)$ jazyka L je $(\exists x_1) \dots (\exists x_n)\varphi$ pravdivá, právě když existují konstantní termy t_{ij} jazyka L takové, že*

$$\varphi(x_1/t_{11}, \dots, x_n/t_{1n}) \vee \dots \vee \varphi(x_1/t_{m1}, \dots, x_n/t_{mn})$$

je (výroková) tautologie.

Důkaz $(\exists x_1) \dots (\exists x_n)\varphi$ je pravdivá $\Leftrightarrow$ $(\forall x_1) \dots (\forall x_n)\neg\varphi$ je nesplnitelná $\Leftrightarrow$ $\neg\varphi$ je nesplnitelná. Ostatní vyplývá z Herbrandovy věty pro $\neg\varphi$. $\square$

Důsledek *Otevřená teorie T jazyka L má model, právě když teorie T' všech základních instancí axiomů z T má model.*

Důkaz Má-li T model $\mathcal{A}$, platí v něm každá instance každého axiomu z T, tedy $\mathcal{A}$ je modelem T'. Nemá-li T model, dle H. věty existuje (konečně) formulí z T', jejichž konjunkce je nesplnitelná, tedy T' nemá model. $\square$