

Matematická logika

(mgr. předmět KMI/MALO)

Petr Jančar

14. prosince 2020

Poznámky k textu. Tento text vzniká v průběhu kurzu v zimním semestru 2020/21 jako podpůrný studijní materiál, dávající přehled o celkovém průběhu a dotýkající se všeho podstatného z náplně kurzu. V tomto běhu se nekonají standardní přednášky a cvičení, výuka probíhá konzultační formou a převážně distančním způsobem (s online komunikací).

Současný kurz obsahuje a rozšiřuje látku kurzu, který dříve běžel v bakalářském studiu. Tento pracovní text tak vzniká úpravami a doplněními pracovního textu z onoho dřívějšího kurzu.

Text bude postupně přibývat, aktuálnost verze bude zřejmá z data uvedeného výše a také z počtu zahrnutých týdnů; text bude zhruba členěn po jednotlivých týdnech v semestru. Pro přehlednost zápis k jednotlivému týdnu začíná vždy na nové straně.

Náš pracovní text není zamýšlen jako studentům plně postačující. Předpokládá se samostudium z více zdrojů, speciálně z učebního textu [1]:

Bělohávek R.: Matematická logika (PřF UP, Olomouc, 2006),

který je přístupný na <http://belohlavek.inf.upol.cz/belohlavekteaching.html>.

V [1] najdete i další doporučenou literaturu.

Např. knihu Švejdar V.: Logika: neúplnost, složitost a nutnost (Academia 2002) zpřístupnil její autor (za určitých podmínek) na adrese

www1.cuni.cz/~svejdar/book/LogikaSve2002.pdf

Na webu lze samozřejmě nalézt i další materiály, např. skripta

Duží M.: Logika pro informatiky (VŠB-TU Ostrava, 2012)

www.cs.vsb.cz/duzi/Matlogika_ESF_Definite.pdf

či slidy k přednáškám

Kučera A.: Matematická logika (FI MUNI, Brno, 2018)

<https://www.fi.muni.cz/usr/kucera/teaching/logic/logika.pdf>.

Bělohávek R.: Matematická logika (PřF UP, Olomouc, 2006),

Studium přinejmenším textu R. Bělohávka [1] studentům našeho kurzu velmi doporučuji, zachycuje totiž detailně mnohé z toho, co zde v textu zmíníme jen stručně. Čtenáře by nemělo zmást, že budeme používat značení, které se někdy mírně liší od značení v [1].

R. Bělohávek také explicitně upozorňuje:

“Učební texty nejspíš obsahují chyby. Pokud je objevíte, sdělte mi je prosím.”

To se zpravidla týká všech textů (včetně používaných učebnic). Přes mou snahu jako autora se nepřesnosti/nejasnosti/chyby mohou samozřejmě objevovat i v tomto našem pracovním textu. Také prosím studenty o upozornění na taková místa.

Ještě poznamenám, že text je místy formulován jako zápis z přednášky, byť např. v současném běhu se přednášky nekonají. Na přednášce by příslušné téma bylo rozebráno samozřejmě podrobněji než zde v textu, studentům by ale měl zápis sloužit přinejmenším jako inspirace k samostudiu a vlastnímu přemýšlení.

Týden 1

Začali jsme příkladem Aristotelova sylogismu

z předpokladů “všechna P jsou M ” a “žádná S nejsou M ”
vyvodíme “žádná S nejsou P ”,

přičemž jsme si přiblížili, o čem je logika, jež zkoumá zásady správného usuzování. Připomněli jsme si Vennovy diagramy i Booleův přístup k ověření správnosti zmíněného sylogismu a podobných úsudků.

Pro zajímavost jsme uvedli strukturu Aristotelových sylogismů a letmo diskutovali i jiné než je výše uvedený “Camestres” (tedy AEE 2. formy), ale zkoušet se sylogismy samozřejmě nebudou. Postačí, když student rozpozná správnost/nesprávnost předloženého úsudku a svůj názor umí podložit řádnými argumenty.

Na příkladu z pěkné knížky

R. Smullyan: Jak se jmenuje tato knížka?

jsme si ukázali použití logiky při analýze jednoduchého problému “ze života”.

O R. Smullyanovi si přečtete např. na wikipedii. Narodil se v r. 1919 a zemřel teprve nedávno, v únoru 2017.

Náš příklad se týkal ostrova, kde žijí jen poctivci (každý jejich výrok je pravdivý) a padouši (každý jejich výrok je nepravdivý). Návštěvník ostrova potkal 3 obyvatele A, B, C , přičemž A mu řekl “všichni tři jsme padouši” a B řekl “právě jeden z nás je poctivec”. Zjistili jsme, že tato informace jednoznačně určuje charakter y osob A, B, C .

Při uvedené analýze jsme použili výrokové symboly (nebo též výrokové proměnné, či atomy) p_A, p_B, p_C (např. symbol p_A označuje výrok “ A je poctivec”), sestavili jsme jisté formule výrokové logiky a hledali pravdivostní ohodnocení, která je splňují

Také jsme se zamysleli nad situací, kdy nám návštěvník ostrova sdělí, že potkal obyvatele D a ten mu řekl “já jsem padouch”.

Cvičení 1 Vyřešte výše uvedené problémy z ostrova poctivců a padouchů.

Výroková logika

Připomněli jsme si, že (formální) *jazyk nad abecedou* Σ je podmnožina množiny Σ^* , tedy nějaká množina konečných posloupností prvků Σ , neboli *slov* či *řetězců* v abecedě Σ .

Např. pro $\Sigma = \{a, b\}$ je $\Sigma^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, \dots\}$, kde ε označuje *prázdné slovo* (délky nula). Příkladem jazyka $L \subseteq \{a, b\}^*$ je

$$L = \{u \in \{a, b\}^* \mid \text{počet výskytů } a \text{ ve slově } u \text{ je stejný jako počet výskytů } b \text{ v } u\}.$$

Předpokládejme, že máme pevně danou množinu VS *výrokových symbolů*. Postačí nám např. spočetná množina

$$VS = \{p, q, r, p_0, q_0, r_0, p_1, q_1, r_1, p_2, q_2, r_2, \dots\}.$$

Symbole psané p, q, r, \dots budeme používat jako (meta)proměnné, jejichž hodnoty jsou prvky VS (jak uvidíme hned v následující definici).

Množinu FML *výrokových formulí* (zkráceně *formulí*) lze chápat jako jazyk nad abecedou

$$\Sigma = VS \cup \{\neg, \wedge, \vee, \rightarrow, (,)\},$$

definovaný strukturální indukcí následovně:

1. Každý prvek VS je formulí, tedy prvkem FML; neboli, pro každé $p \in VS$ je p formule.

Zde vidíme použití p jako výše zmíněné (meta)proměnné. Symbol “ p ” je pro nás jeden konkrétní prvek množiny VS, takže např. zápis “pro každé $p \in VS$ je p formule” by byl nesprávný. Někdy ovšem k podobné kolizi ve značení v textech dojde; měli bychom si být ale vždy schopni ujasnit zamýšlený význam.

2. Je-li $\varphi \in \text{FML}$, pak $\neg\varphi \in \text{FML}$. (Je-li φ formule, je i řetězec $\neg\varphi$ formule.)

Je nám jasné, že symbol φ zde používáme jako proměnnou, jejíž hodnotou je prvek množiny FML, což je řetězec ve výše uvedené abecedě Σ ; symbol “ φ ” jako takový formulí není. Zápisem “ $\neg\varphi$ ” pochopitelně označujeme řetězec, který začíná symbolem “ \neg ” a pak pokračuje řetězcem, který je označený symbolem “ φ ” [neboli řetězcem, který je v daném kontextu hodnotou proměnné φ].

3. Je-li $\varphi_1 \in \text{FML}$ a $\varphi_2 \in \text{FML}$,
pak řetězce $(\varphi_1 \wedge \varphi_2)$, $(\varphi_1 \vee \varphi_2)$ a $(\varphi_1 \rightarrow \varphi_2)$ jsou formule (tedy prvky FML).

Jako vždy u definice tohoto typu se implicitně rozumí, že jiné řetězce než ty, které lze odvodit z uvedených pravidel, prvky FML nejsou.

Např. řetězec $((p \wedge \neg q) \rightarrow \neg(q \rightarrow \neg r))$ je formulí, zatímco řetězce $p \wedge q \rightarrow \neg(q \rightarrow \neg r)$ či $\forall p \neg q$ podle uvedené definice formulí nejsou.

Mluvili jsme také o syntaktickém stromu formule, či příslušném logickém obvodu. Je užitečné se nad tím zamyslet, byť formálně zde tyto pojmy nedefinujeme.

Někdy se také zavádí pojem *vytvorující posloupnosti* $\varphi_0, \varphi_1, \dots, \varphi_k$ formule φ_k ; např. posloupnost $\varphi_0 = p, \varphi_1 = q, \varphi_2 = \neg\varphi_1, \varphi_3 = (\varphi_0 \wedge \varphi_2)$ je jedna z vytvářejících posloupností formule $(p \wedge \neg q)$.

Cvičení 2 *Navrhněte definici pojmu syntaktický strom formule a nakreslete jej pro formulí $((p \wedge \neg q) \rightarrow \neg(q \rightarrow \neg r))$.*

Připomněli jsme pojem *pravdivostního ohodnocení* (zkráceně *ohodnocení*, anglicky můžeme říci *evaluation*), což je zobrazení typu

$$e : VS \longrightarrow \{0, 1\}.$$

Zde 0 znamená *nepravda* (hodnota *false*) a 1 znamená *pravda* (hodnota *true*). K ohodnocení e je přiřazeno jeho rozšíření

$$\bar{e} : \text{FML} \longrightarrow \{0, 1\}$$

definované následující strukturální indukcí; v ní používáme booleovské funkce $f_{\neg}, f_{\wedge}, f_{\vee}, f_{\rightarrow}$, o nichž bude řeč níže.

1. pro $p \in \text{VS}$ je $\bar{e}(p) = e(p)$;
2. $\bar{e}(\neg\varphi) = f_{\neg}(\bar{e}(\varphi))$;
3. $\bar{e}((\varphi_1 \wedge \varphi_2)) = f_{\wedge}(\bar{e}(\varphi_1), \bar{e}(\varphi_2))$;
 $\bar{e}((\varphi_1 \vee \varphi_2)) = f_{\vee}(\bar{e}(\varphi_1), \bar{e}(\varphi_2))$;
 $\bar{e}((\varphi_1 \rightarrow \varphi_2)) = f_{\rightarrow}(\bar{e}(\varphi_1), \bar{e}(\varphi_2))$.

Booleovskou funkcí n proměnných rozumíme funkci typu $f : \{0, 1\}^n \rightarrow \{0, 1\}$.

- Funkce f_{\neg} má 1 proměnnou a splňuje $f_{\neg}(0) = 1$ a $f_{\neg}(1) = 0$.
- Funkce f_{\wedge} , f_{\vee} , f_{\rightarrow} mají dvě proměnné a jsou definovány následovně:
 $f_{\wedge}(x, y) = 1$ právě tehdy, když $x = y = 1$;
 $f_{\vee}(x, y) = 0$ právě tehdy, když $x = y = 0$;
 $f_{\rightarrow}(x, y) = 0$ právě tehdy, když $x = 1$ a $y = 0$.

Úmluva.

- V dalším budeme rozšíření \bar{e} označovat rovněž e . Když tedy řekneme “ohodnocení” e , můžeme myslet zobrazení jak typu $e : \text{VS} \rightarrow \{0, 1\}$, tak typu $e : \text{FML} \rightarrow \{0, 1\}$. Zvlášť zdůrazníme, pokud to bude třeba rozlišovat.
- Hodnotu $e(\varphi)$ budeme také označovat $\|\varphi\|_e$ a říkáme jí *hodnota formule φ při pravidelném ohodnocení e* .
- Použijeme-li pro formuli φ zápis $\varphi(p_1, p_2, \dots, p_n)$, označujeme tím fakt, že ve φ se vyskytují jiné výrokové symboly než symboly z množiny $\{p_1, p_2, \dots, p_n\}$ (ovšem nemusí se v ní vyskytovat všechny). Např. pro formuli $\varphi = ((p \wedge \neg q) \rightarrow \neg(q \rightarrow \neg r))$ je v pořádku jak zápis $\varphi(p, q, r)$, tak třeba zápis $\varphi(p, p_1, q, r, r_3)$.

Použili jsme zde obecněji proměnné p_1, p_2, \dots pro prvky VS, nikoli přímo symboly p_1, p_2, \dots (což jsme také mohli udělat); význam by měl být opět jasný.

Strukturální indukci jsme snadno ukázali:

Tvrzení 1 *Shodují-li se ohodnocení e_1, e_2 na množině $\{p_1, p_2, \dots, p_n\}$ (tedy $e_1(p_i) = e_2(p_i)$ pro vš. $i \in \{1, 2, \dots, n\}$), pak pro $\varphi = \varphi(p_1, p_2, \dots, p_n)$ máme $\|\varphi\|_{e_1} = \|\varphi\|_{e_2}$.*

Cvičení 3 *Připomeňte si, co je to strukturální indukce, a tvrzení pořádně dokažte.*

Cvičení 4 *Navrhněte postup, jak lze k formuli $\varphi(p_1, p_2, \dots, p_n)$ přiřadit booleovskou funkci $B_{\varphi} : \{0, 1\}^n \rightarrow \{0, 1\}$ tak, že pro každé ohodnocení e platí $B_{\varphi}(e(p_1), e(p_2), \dots, e(p_n)) = \|\varphi\|_e$.*

Cvičení 5 *Navrhněte postup, jak lze k booleovské funkci $B : \{0, 1\}^n \rightarrow \{0, 1\}$ sestavit formuli φ_B v níž se vyskytují jen výrokové symboly p_1, p_2, \dots, p_n a pro každé $(b_1, b_2, \dots, b_n) \in \{0, 1\}^n$ platí $B(b_1, b_2, \dots, b_n) = \|\varphi_B\|_e$, kde $e(p_i) = b_i$ pro $i = 1, 2, \dots, n$. (Nápověda: začněte s funkcemi $B : \{0, 1\}^n \rightarrow \{0, 1\}$, které dávají 1 jen pro jednu n -tici vstupů.)*

Připomněli jsme definici následujících pojmů. Formule φ je

- *pravdivá při ohodnocení e* , jestliže $\|\varphi\|_e = 1$;
- *splnitelná*, jestliže existuje e tž. $\|\varphi\|_e = 1$;
- *tautologie*, neboli *logicky platná* (či *logicky pravdivá*), jestliže $\|\varphi\|_e = 1$ pro každé e ;
- *nesplnitelná*, neboli *kontradikce*, jestliže $\|\varphi\|_e = 0$ pro každé e .

Pozorování 2 *Formule φ je tautologie právě tehdy, když $\neg\varphi$ je nesplnitelná.*

Zavedli jsme pojem ekvivalence formulí:

φ_1 a φ_2 jsou (*sémanticky*) *ekvivalentní*, označujeme $\varphi_1 \equiv \varphi_2$, jestliže $\forall e : \|\varphi_1\|_e = \|\varphi_2\|_e$.

Relace \equiv je relací na množině FML, tedy $\equiv \subseteq \text{FML} \times \text{FML}$, která očividně je reflexivní, symetrická a tranzitivní; je to tedy relace ekvivalence a odpovídá jí příslušný rozklad množiny FML. (Uvědomme si ale, že $\varphi_1 \equiv \varphi_2$ není formule výrokové logiky ...)

Udělali jsme běžné dohody o vynechávání závorek ve formulích, mj. využitím priorit pro logické spojky (v pořadí $\neg, \wedge, \vee, \rightarrow$, kde \neg váže nejsilněji).

Strukturální indukci jsme definovali, co jsou *podformule* dané formule. Všimněme si, že např. $\varphi_1 = q \rightarrow r$ *není* podformulí formule $\varphi_2 = p \wedge q \rightarrow r$, protože plně uzavorkovaná φ_2 je $((p \wedge q) \rightarrow r)$ a její podformule jsou $p, q, r, (p \wedge q), ((p \wedge q) \rightarrow r)$ (první čtyři jsou *vlastní* podformule formule φ_2).

Např. u $\varphi = r \vee \neg p \vee q$ není jasné, zda vznikla vynecháním závorek z $\varphi_1 = ((r \vee \neg p) \vee q)$ nebo z $\varphi_2 = (r \vee (\neg p \vee q))$, ale to nám nevadí, protože očividně platí $\varphi_1 \equiv \varphi_2$. (Vynecháváním závorek se můžeme dopustit nejednoznačnosti ohledně reprezentované formule, ale reprezentovaná třída rozkladu podle ekvivalence \equiv je jednoznačná.)

Cvičení 6 *Najděte všechny podformule formule $(p \rightarrow q) \wedge \neg q \rightarrow p$. Pak zjistěte, zda je daná formule splnitelná a případně dokonce tautologie.*

Zmínili jsme i *prefixovou notaci*, kde se bez závorek zcela obejdeme, aniž se dopouštíme jakékoli nejednoznačnosti: zde je formule buď výrokový symbol, nebo je v jednom z tvarů $\neg\varphi_1, \wedge\varphi_1\varphi_2, \vee\varphi_1\varphi_2, \rightarrow\varphi_1\varphi_2$, kde φ_1, φ_2 jsou formule.

Na závěr jsme rozebrali tento (složený) výrok:

Není pravda, že nepřišli-li dnes na přednášku ti nejhorší studenti, pak nepřišli ani ti nejlepší.

Cvičení 7 *Zformulujte uvedenou větu jako výrokovou formuli a použijte ji k analýze situace.*

Týden 2

Řešení Cvičení 3. Měli jsme strukturální indukci dokázat tvrzení

Shodují-li se ohodnocení e_1, e_2 na množině $\{p_1, p_2, \dots, p_n\}$ (tedy $e_1(p_i) = e_2(p_i)$ pro vš. $i \in \{1, 2, \dots, n\}$), pak pro $\varphi = \varphi(p_1, p_2, \dots, p_n)$ máme $\|\varphi\|_{e_1} = \|\varphi\|_{e_2}$.

1. Když $\varphi = p$ (tedy φ je *atomická*, tj. výrokový symbol), tak $\|\varphi\|_e = e(p)$ a tvrzení je zřejmé (hodnota $\|p\|_e$ je určena hodnotou $e(p)$; na hodnotách $e(q)$ pro $q \neq p$ nezáleží).
2. Nechť $\varphi = \neg\psi$ a všechny výrokové symboly vyskytující se v ψ patří mezi výrokové symboly označené p_1, p_2, \dots, p_n ; lze tedy psát ψ jako $\psi(p_1, p_2, \dots, p_n)$ a také φ jako $\varphi(p_1, p_2, \dots, p_n)$.

Podle indukčního předpokladu (prováděné strukturální indukce) předpokládáme, že $\|\psi\|_e$ je určena hodnotami $e(p_1), e(p_2), \dots, e(p_n)$ (přičemž na hodnotách $e(q)$ pro $q \notin \{p_1, p_2, \dots, p_n\}$ nezáleží). Jelikož podle definice máme $\|\varphi\|_e = f_{\neg}(\|\psi\|_e)$, hodnota $\|\varphi\|_e$ je určena hodnotou $\|\psi\|_e$ a ta je určena hodnotami $e(p_1), e(p_2), \dots, e(p_n)$. Tedy i hodnota $\|\varphi\|_e$ je určena hodnotami $e(p_1), e(p_2), \dots, e(p_n)$ (přičemž na hodnotách $e(q)$ pro $q \notin \{p_1, p_2, \dots, p_n\}$ nezáleží).

3. Nechť $\varphi = (\psi_1 \wedge \psi_2)$ a všechny výrokové symboly vyskytující se v ψ_1 a ψ_2 patří mezi výrokové symboly označené p_1, p_2, \dots, p_n

Dokončete celý důkaz podrobně sami. □

Tabulková metoda.

Připomněli jsme si tabulkovou metodu, která k dané formuli φ mj. sestrojí tabulku reprezentované booleovské funkce $B_\varphi : \{0, 1\}^n \rightarrow \{0, 1\}$, kde n je počet výrokových symbolů vyskytujících se ve φ (jako atomické podformule). Uvědomili jsme si, že aby funkce B_φ byla jednoznačně daná formulí φ , musíme mít výrokové symboly nějak uspořádaný. Naše volba $VS = \{p, q, r, p_0, q_0, r_0, p_1, q_1, r_1, p_2, q_2, r_2, \dots\}$ přímo nabízí jedno takové uspořádání.

Cvičení 8 Sestrojte tabulku funkce B_φ , kde formule φ je $((q_2 \rightarrow \neg(p_1 \wedge r)) \rightarrow p_1)$.

Lze uvažovat také tuto ekvivalenci na množině FML: φ_1 a φ_2 jsou ekvivalentní, jestliže $B_{\varphi_1} = B_{\varphi_2}$. Rozmyslete si, proč je to jiná ekvivalence než \equiv .

Připomeňme, že *literál* je výrokový symbol, např. označený p , či jeho negace, např. $\neg p$; *klauzule* je formule tvaru $(\ell_1 \vee \ell_2 \cdots \vee \ell_k)$, kde $k \geq 1$ a ℓ_i jsou literály.

Pro $k = 0$ dostaneme *prázdnou klauzuli*, označovanou např. \square , což je nesplnitelná formule (kontradikce). Tu využijeme později při diskusi rezoluční metody.

Formule je v *konjunktivní normální formě* (KNF), když je tvaru $C_1 \wedge C_2 \cdots \wedge C_m$, kde $m \geq 1$ a C_i jsou klauzule. *Disjunktivní normální forma* (DNF) je definována analogicky, s prohozenou rolí \wedge a \vee .

Všimli jsme si, že pro fixní n máme 2^{2^n} booleovských funkcí n proměnných a ukázali jsme si, že k tabulce jakékoli funkce $f : \{0, 1\}^n \rightarrow \{0, 1\}$ umíme sestrojit formuli φ v (úplné) disjunktivní normální formě tak, že $B_\varphi = f$. Totéž jsme ukázali pro konjunktivní normální formu.

Cvičení 9 K formulí $((q_2 \rightarrow \neg(p_1 \wedge r)) \rightarrow p_1)$ z Cvičení 8 sestrojte KNF i DNF.

Dokázali jsme tak mj., že systém logických spojek $\{\neg, \wedge, \vee\}$ je *funkcionálně úplný*, a navíc:

Tvrzení 3 Ke každé formulí φ lze sestrojit φ_1 v KNF (Konjunktivní Normální Formě) a φ_2 v DNF (Disjunktivní Normální Formě) tak, že $\varphi \equiv \varphi_1 \equiv \varphi_2$.

Cvičení 10 Uvědomte si speciální případ tautologií a kontradikcí. Jak budou KNF a DNF vypadat u nich?

Připomněli jsme si de Morganovy zákony a další zřejmé ekvivalence formulí:

$$\varphi_1 \wedge \varphi_2 \equiv \neg(\neg\varphi_1 \vee \neg\varphi_2)$$

$$\varphi_1 \vee \varphi_2 \equiv \neg(\neg\varphi_1 \wedge \neg\varphi_2)$$

$$\varphi_1 \rightarrow \varphi_2 \equiv \neg\varphi_1 \vee \varphi_2$$

$$\varphi_1 \vee \varphi_2 \equiv \neg\varphi_1 \rightarrow \varphi_2$$

Z toho jsme mj. usoudili:

Tvrzení 4 Každý ze systémů $\{\neg, \wedge\}$, $\{\neg, \vee\}$ a $\{\neg, \rightarrow\}$ je *funkcionálně úplný*.

Všimli jsme si také, že spojka “NAND” (“ne oba”), neboli tzv. Shefferův operátor $|$ definovaný vztahem $p|q = \neg(p \wedge q)$, je sama funkcionalně úplným systémem. Je totiž $\neg p \equiv p|p$ a $p \wedge q \equiv \neg(p|q) \equiv \neg(p|q) \equiv (p|q)|(p|q)$. Podobně to platí pro “NOR” (“ani ani”). Logické obvody lze tedy v principu sestavovat z jednoho typu hradel.

Cvičení 11 Z kontextu by mělo být implicitně zřejmé, co myslíme funkcionalní úplností systému logických spojek. Definujte to ale explicitně. Pak argumentujte, proč systém $\{\wedge, \vee, \rightarrow\}$ není funkcionalně úplný. (Nápověda. Ukažte, že k formulí $\varphi = \neg p$ neexistuje formule ψ , v níž všechny logické spojky patří pouze do množiny $\{\wedge, \vee, \rightarrow\}$ a zároveň platí $B_\varphi = B_\psi$.)

Zavedli jsme logickou spojku \leftrightarrow jako zkratku:

$$\varphi \leftrightarrow \psi \text{ není formule, ale je to zkratka za formulí } (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi).$$

Jinou variantou je vzít \leftrightarrow jako plnohodnotou spojku, s příslušnou funkcí f_{\leftrightarrow} , kde $f_{\leftrightarrow}(x, y) = 1$ právě tehdy, když $x = y$, a příslušně doplnit náš jazyk výrokové logiky.

I při naší volbě zavedení \leftrightarrow jako zkratky ji můžeme při zápisu formulí používat (s nejmenší prioritou, pokud jde o závorky); jsme si přitom prostě vědomi, že náš zápis není striktně vzato formulí, ale jednoznačně reprezentuje řádnou formulí (či alespoň její třídu ekvivalence \equiv).

Nechali jsme dosud implicitní, že spojky $\neg, \wedge, \vee, \rightarrow$ nazýváme postupně *negace*, *konjunkce*, *disjunkce*, *implikace*. Spojku \leftrightarrow přirozeně nazveme (*logická*) *ekvivalence*, ale je to něco jiného než relace na množině. Promysleli jsme si proto důkladně následující tvrzení a jeho důkaz.

Tvrzení 5 Pro libovolné formule φ_1, φ_2 platí $\varphi_1 \equiv \varphi_2$ (tedy φ_1, φ_2 jsou ekvivalentní, tedy $\forall e : \|\varphi_1\|_e = \|\varphi_2\|_e$) právě tehdy, když $\varphi_1 \leftrightarrow \varphi_2$ je tautologie.

Pro stručnost bychom mohli napsat: $\varphi_1 \equiv \varphi_2 \iff \varphi_1 \leftrightarrow \varphi_2 \in \text{TAUT}$, kde TAUT je množina tautologií. Tady symbol \iff nahrazuje ono “právě tehdy, když” a je to tedy symbol pro logickou ekvivalenci na *metaúrovni*.

Cvičení 12 Udělejte si důkaz Tvzení pořádně. Jedná se o dvě implikace (na metaúrovni). Nejprve tedy ukážeme, že když $\varphi_1 \equiv \varphi_2$, tak $\varphi_1 \leftrightarrow \varphi_2$ je tautologie Pak ukážeme, že když $\varphi_1 \leftrightarrow \varphi_2$ je tautologie, tak $\varphi_1 \equiv \varphi_2$...

Cvičení 13 Připomeňte si (najděte) axiomy Booleovy algebry a vyjádřete je jako sadu tautologií výrokové logiky.

Dodatek k funkcionální úplnosti. Připomeňme, že systém logických spojek je funkcionálně úplný, jestliže ke každé booleovské funkci f existuje výroková formule φ , v níž se nevyskytují logické spojky mimo těch ze systému a pro kterou máme $B_\varphi = f$.

Všimli jsme si, že systém $\{\wedge, \vee, \rightarrow\}$ není funkcionálně úplný. Pro jakoukoli formuli $\varphi(p_1, p_2, \dots, p_n)$ v tomto systému očividně máme $f_\varphi(1, 1, \dots, 1) = 1$; tedy např. funkci f_{\neg} (kterou jsme definovali vztahy $f_{\neg}(0) = 1, f_{\neg}(1) = 0$) nelze reprezentovat žádnou formulí v systému $\{\wedge, \vee, \rightarrow\}$.

Dodatek k normálním formám. Formule je v konjunktivní normální formě (KNF), jestliže je to konjunkce konečného počtu *elementárních disjunkcí* (tedy tzv. klauzulí, tj. disjunkcí konečného počtu literálů). Formule je v disjunktivní normální formě (DNF), jestliže je to disjunkce konečného počtu *elementárních konjunkcí* (konjunkcí konečného počtu literálů).

Vedle “tabulkového” postupu konstrukce *úplných* normálních forem, jsme si ukázali i převod formulí do KNF či DNF využitím strukturální indukce. Klíčovým byl přitom fakt, že formule

$$(C_1 \wedge C_2 \cdots \wedge C_m) \vee (C'_1 \wedge C'_2 \cdots \wedge C'_n)$$

je ekvivalentní formulí

$$(C_1 \vee C'_1) \wedge (C_1 \vee C'_2) \cdots \wedge (C_1 \vee C'_n) \wedge (C_2 \vee C'_1) \wedge \cdots \wedge (C_2 \vee C'_n) \wedge \cdots \wedge (C_m \vee C'_1) \wedge \cdots \wedge (C_m \vee C'_n),$$

neboli

$$\left(\bigwedge_{1 \leq i \leq m} C_i \right) \vee \left(\bigwedge_{1 \leq j \leq n} C'_j \right) \equiv \bigwedge_{1 \leq i \leq m, 1 \leq j \leq n} (C_i \vee C'_j).$$

Tento fakt, a duální fakt s prohozenými konjunkcemi a disjunkcemi, lze odvodit např. využitím “distributivních zákonů”.

Vzpomeňte si na naše vyjádření axiomů Booleovy algebry jako tautologií výrokové logiky.

Máme mj. $\varphi_1 \vee (\varphi_2 \wedge \varphi_3) \equiv (\varphi_1 \vee \varphi_2) \wedge (\varphi_1 \vee \varphi_3)$ a také $\varphi_1 \wedge (\varphi_2 \vee \varphi_3) \equiv (\varphi_1 \wedge \varphi_2) \vee (\varphi_1 \wedge \varphi_3)$.

Uvědomili jsme si tak mj., že máme i jiné možnosti převodu formule do KNF (či DNF) než přes tabulku. (Mj. se také uplatní de Morganovy zákony ...)

Týden 3

Ze zápisu z týdne 2 jsem vypustil chybnou poznámku o monotonii funkcí f_\wedge , f_\vee a f_\rightarrow , protože jedna z nich monotónní není. (Je vám jasné která?)

Sémantické vyplývání.

Řekneme, že množina formulí $T \subseteq \text{FML}$ je *splněna pravdivostním ohodnocením* e , jestliže $\|\varphi\|_e = 1$ pro každou $\varphi \in T$. Množina T je *splnitelná*, jestliže existuje pravdivostní ohodnocení e , které ji splňuje; v opačném případě je T *nesplnitelná*.

Zavedli jsme značení $T \models \varphi$ (čteme “ φ sémanticky vyplývá z T ” nebo také “ φ je tautologickým důsledkem T ”). $T \models \varphi$ platí, jestliže pro každé pravdivostní ohodnocení e splňující T máme $\|\varphi\|_e = 1$.

Píšeme také $T, \varphi \models \psi$ místo $T \cup \{\varphi\} \models \psi$, dále $\varphi_1, \varphi_2 \models \psi$ místo $\{\varphi_1, \varphi_2\} \models \psi$, apod. Také píšeme $\models \varphi$ místo $\emptyset \models \varphi$. Uvědomili jsme si, že

$$\models \varphi \text{ je vlastně vyjádření faktu, že } \varphi \text{ je tautologie,}$$

a také že

$$\text{když } T \text{ je nesplnitelná, tak pro všechny formule } \varphi \text{ máme } T \models \varphi.$$

Cvičení 14 Vysvětlete, proč platí $p \rightarrow q, q \rightarrow r \models p \rightarrow r$ a proč neplatí $p \rightarrow q \models \neg p \rightarrow \neg r$. Zjistěte, zda platí $T \models \varphi$, kde $T = \{r \rightarrow p, \neg q \rightarrow r\}$ a $\varphi = \neg(p \wedge \neg q)$.

Uvědomili jsme si jednoduchý užitečný fakt:

Tvrzení 6 $T \models \varphi$ právě tehdy, když $T \cup \{\neg\varphi\}$ je nesplnitelná.

Důkaz. Podle definice, $T \cup \{\neg\varphi\}$ je nesplnitelná právě tehdy, když neexistuje pravdivostní ohodnocení e splňující zároveň T i $\neg\varphi$, tedy právě tehdy, když každé pravdivostní ohodnocení e splňující T nesplňuje $\neg\varphi$; přitom e nesplňuje $\neg\varphi$ právě tehdy, když splňuje φ . \square

Jednoduchá fakta o substitucích ve formulích se dají prezentovat následujícím dvěma body (kterým můžeme říkat *věta o substituci* a *věta o ekvivalenci*):

Tvrzení 7

1. Když platí $\models \varphi$ (neboli φ je tautologie) a φ' vznikne z φ nahrazením všech výskytů výrokového symbolu p (jakoukoli) formulí ψ , tak $\models \varphi'$.
2. Jestliže φ' vznikne z φ nahrazením (jednoho) výskytu podformule ψ ekvivalentní formulí ψ' (máme tedy $\psi \equiv \psi'$), tak $\varphi \equiv \varphi'$ (neboli $\models \varphi \leftrightarrow \varphi'$, neboli $\varphi \leftrightarrow \varphi'$ je tautologie).

Také jsme si ukázali tzv. *sémantickou větu o dedukci*:

Tvrzení 8 $T, \varphi \models \psi$ právě tehdy, když $T \models \varphi \rightarrow \psi$.

Cvičení 15 Promyslete si, jak byste předchozí dvě tvrzení dokázali, a důkaz alespoň jednoho z nich napište.

Všimněme si, že při zavedení $T \models \varphi$ jsme nemluvili o případě, kdy je T nekonečná (což je možné v některých kontextech uvažovat). Doposud nejtěžší úvahy jsme provedli při důkazu následující věty:

Věta 9 (o kompaktnosti). $T \subseteq \text{FML}$ je splnitelná právě tehdy, když každá konečná $T' \subseteq T$ je splnitelná. (Tedy když T je nesplnitelná, tak existuje konečná $T' \subseteq T$, která je nesplnitelná.)

Důkaz. Jeden směr tvrzení je zřejmý (který?).

Pro druhý směr je klíčové si uvědomit, že když každá konečná $T' \subseteq T$ je splnitelná a p ani $\neg p$ nepatří do T (obě formule p a $\neg p$ do T pochopitelně patřit nemohou), tak nutně buď platí, že každá konečná $T' \subseteq T \cup \{p\}$ je splnitelná, nebo platí, že každá konečná $T' \subseteq T \cup \{\neg p\}$ je splnitelná. Kdyby totiž existovala konečná $T_1 \subseteq T \cup \{p\}$, která je nesplnitelná, a zároveň konečná $T_2 \subseteq T \cup \{\neg p\}$, která je nesplnitelná, tak $T_1 \cup T_2$ je nesplnitelná. (Proč?) \square

Cvičení 16 Dokončete předchozí důkaz kompletně. (Připomeňte si, že množinu VS výrokových symbolů máme uspořádanu a tato množina je spočetná. Pro účely důkazu zde označme její prvky p_0, p_1, p_2, \dots . Úvahu v důkazu proveďte postupně pro p_0 , pak pro p_1 , atd. K čemu dojdeme na závěr tohoto nekonečného procesu?)

Důsledek 10 $T \models \varphi$ právě tehdy, když existuje konečná $T' \subseteq T$ taková, že $T' \models \varphi$, tedy právě tehdy, když $\models \varphi_1 \rightarrow (\varphi_2 \rightarrow (\dots \varphi_{n-1} \rightarrow (\varphi_n \rightarrow \varphi) \dots))$ pro nějaké $\varphi_1, \varphi_2, \dots, \varphi_n \in T$ (kde může být $n = 0$; v tom případě $\models \varphi$).

Cvičení 17 Dokažte, že když $T' \models \varphi$ a $T' = \{\varphi_1, \varphi_2, \dots, \varphi_n\}$, tak platí $\models \varphi_1 \rightarrow (\varphi_2 \rightarrow (\dots \varphi_{n-1} \rightarrow (\varphi_n \rightarrow \varphi) \dots))$.
(Použijte sémantickou větu o dedukci.)

Týden 4

Axiomatický systém výrokové logiky.

Omezili jsme se teď na funkcionálně úplný systém $\{\neg, \rightarrow\}$ stejně jako [1]. Formule používající také některou ze spojek \wedge, \vee (nebo \leftrightarrow) zde tedy formálně považujeme za zkratky formulí v systému $\{\neg, \rightarrow\}$. (Připomeňme si, že $\varphi \vee \psi \equiv \neg\varphi \rightarrow \psi$ a $\varphi \wedge \psi \equiv \neg(\varphi \rightarrow \neg\psi)$.)

Uvedli jsme postupně tři schémata axiomů jako v [1]:

1. $\varphi \rightarrow (\psi \rightarrow \varphi)$
2. $(\varphi \rightarrow (\psi_1 \rightarrow \psi_2)) \rightarrow ((\varphi \rightarrow \psi_1) \rightarrow (\varphi \rightarrow \psi_2))$
3. $(\neg\psi \rightarrow \neg\varphi) \rightarrow (\varphi \rightarrow \psi)$

a dedukční (odvozovací) pravidlo MP (Modus Ponens):

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi},$$

které čteme “z formulí φ a $\varphi \rightarrow \psi$ (nad čarou) lze odvodit formuli ψ (pod čarou)”.

Řekli jsme, co je to *důkaz formule* φ v teorii T (zde T je nějaká, třeba i nekonečná, množina formulí, tedy podmnožina množiny FML) a definovali jsme značení

$$T \vdash \varphi,$$

které značí, že formule φ je *dokazatelná* z T , tedy že existuje důkaz formule φ z T .

Důkazem φ z T je jakákoli posloupnost formulí $\varphi_1, \varphi_2, \dots, \varphi_k$, kde pro každé $i \in \{1, 2, \dots, k\}$ platí, že φ_i je buď axiom (tedy instance nějakého axiomového schématu), nebo prvek množiny T , nebo se dá odvodit pravidlem MP z formulí φ_{j_1} a φ_{j_2} pro nějaká $j_1, j_2 \in \{1, 2, \dots, i-1\}$.

Sestavme si důkaz formule $p \rightarrow p$ z \emptyset , tedy ukažme $\emptyset \vdash p \rightarrow p$, což také píšeme jako $\vdash p \rightarrow p$:

1. φ_1 je: $p \rightarrow ((p \rightarrow p) \rightarrow p)$ (instance ax. schématu 1 [$\varphi = p$, $\psi = (p \rightarrow p)$]),
2. φ_2 je: $(p \rightarrow ((p \rightarrow p) \rightarrow p)) \rightarrow ((p \rightarrow (p \rightarrow p)) \rightarrow (p \rightarrow p))$ (instance ax. schématu 2),
3. φ_3 je: $(p \rightarrow (p \rightarrow p)) \rightarrow (p \rightarrow p)$ (vznikne aplikací MP na φ_1 a φ_2),
4. φ_4 je: $p \rightarrow (p \rightarrow p)$ (instance ax. schématu 1),
5. φ_5 je: $p \rightarrow p$ (vznikne aplikací MP na φ_4 a φ_3).

Ověřili jsme korektnost axiomatického systému:

Věta 11 (*o korektnosti*). Jestliže $T \vdash \varphi$, pak $T \models \varphi$.

Cvičení 18 *Dokažte větu o korektnosti indukcí podle délky důkazu; konkrétně ukažte, že pro každý důkaz $\varphi_1, \varphi_2, \dots, \varphi_k$ z T platí, že φ_k je pravdivá pro každé pravdivostní ohodnocení splňující T .*

Opačná věta, věta o úplnosti (jestliže $T \models \varphi$, pak $T \vdash \varphi$) je obtížnější; dokážeme ji postupně. Začneme (syntaktickou) větou o dedukci.

Nejprve připomeňme triviální pozorování:

Pozorování 12 Jestliže $T \vdash \varphi$ a $T \subseteq T'$, pak $T' \vdash \varphi$.

Nyní již k oné (syntaktické) větě o dedukci:

Věta 13 (o dedukci). Pro každé $T \subseteq \text{FML}$ a $\varphi, \psi \in \text{FML}$ platí

$$T, \varphi \vdash \psi \text{ právě tehdy, když } T \vdash \varphi \rightarrow \psi.$$

Důkaz. Provedli jsme důkaz obdobně jako v [1]. (Jistě teď dokážete opravit drobná nedopatření v onom důkazu v [1].) \square

Všimli jsme si, že k důkazu stačila schémata axiomů (1) a (2), tedy $\varphi \rightarrow (\psi \rightarrow \varphi)$ a $(\varphi \rightarrow (\psi_1 \rightarrow \psi_2)) \rightarrow ((\varphi \rightarrow \psi_1) \rightarrow (\varphi \rightarrow \psi_2))$.

Pak jsme se pustili do důkazu věty doplňující zmíněnou větu o korektnosti:

Věta 14 (o úplnosti). Jestliže $T \models \varphi$, pak $T \vdash \varphi$.

Provedli jsme důkaz obdobně jako v [1]. Začali jsme ovšem rovnou Lemmatem 2.39 (bez předchozích vět) a zkusili, kam dojdeme strukturální indukcí, tedy co nám bude případně chybět k dokončení důkazu. Všimli jsme si, že se nám v důkazu náramně hodilo schéma (3) z definice axiomů (tedy $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$) a uvědomili si, že k dokončení důkazu by se nám hodilo mít jako axiomy také schéma $\varphi \rightarrow \neg\neg\varphi$ a schéma $\varphi_1 \rightarrow (\neg\varphi_2 \rightarrow \neg(\varphi_1 \rightarrow \varphi_2))$. Tato schémata ovšem jako axiomy brát nemusíme, jsou totiž odvoditelná z axiomů (1),(2),(3), jak jsme si ukázali při demonstraci (tranzitivity implikace a) Věty 2.31 z [1] na cvičení. (Opět si jistě snadno opravíte drobná nedopatření v důkazu v [1].)

Dokončili jsme důkaz věty o úplnosti (Věty 14) s tím, že jsme se spolehli na platnost věty o důkazu rozbořem případů (Věta 2.36 v [1]), konkrétně na následující implikaci:

Tvrzení 15 Jestliže $T, \varphi_1 \vdash \psi$ a $T, \varphi_2 \vdash \psi$, pak také $T, (\varphi_1 \vee \varphi_2) \vdash \psi$.

Připomínáme, že $\varphi_1 \vee \varphi_2$ je zkratka za $\neg\varphi_1 \rightarrow \varphi_2$. My jsme speciálně využili, že z předpokladů $T, p \vdash \psi$ a $T, \neg p \vdash \psi$ plyne $T, (p \vee \neg p) \vdash \psi$, a tedy také $T \vdash \psi$ (protože dříve ukázaný fakt $\vdash \varphi \rightarrow \varphi$ implikuje $\vdash \neg p \rightarrow \neg p$). Příště dokončíme důkaz tvrzení (a uvědomíme si i opačnou implikaci, zachycenou ve větě 2.36 v [1]).

Poznámka. Jedná se o zápis z dřívějšího běhu. V tomto běhu vám navrhnou probrání online v MSTeams.

Týden 5

Zrekapitulovali jsme probranou látku z oblasti výrokové logiky a dodělali několik technických věcí. Připomeňme si nejprve, že jsme ukázali, že platí $\vdash p \rightarrow p$. Analogickým postupem se dá samozřejmě ukázat, že platí

$$\vdash \varphi \rightarrow \varphi$$

pro jakoukoli formuli φ . Připomněli jsme si důkaz **věty o dedukci**

$$T, \varphi \vdash \psi \text{ právě tehdy, když } T \vdash \varphi \rightarrow \psi.$$

Důkaz. Implikace “ \Leftarrow ” je jednoduchá:

Jestliže platí $T \vdash \varphi \rightarrow \psi$, tak samozřejmě také platí $T, \varphi \vdash \varphi \rightarrow \psi$. Triviálně platí $T, \varphi \vdash \varphi$. Použitím pravidla MP tedy vyvodíme, že $T, \varphi \vdash \psi$.

Implikaci “ \Rightarrow ” dokážeme takto:

Předpokládáme, že platí $T, \varphi \vdash \psi$. Existuje tedy důkaz formule ψ z teorie $T \cup \{\varphi\}$, tj. příslušná posloupnost formulí $\varphi_1, \varphi_2, \dots, \varphi_k$, kde $\varphi_k = \psi$. Ukážeme indukcí pro $i = 1, 2, \dots, k$, že $T \vdash \varphi \rightarrow \varphi_i$; z toho plyne, že $T \vdash \varphi \rightarrow \psi$. Rozlišíme přitom tyto případy:

1. φ_i je axiom,
2. $\varphi_i \in (T \cup \{\varphi\})$; zde rozlišíme podpřípady
 - (a) $\varphi_i \in T$,
 - (b) $\varphi_i = \varphi$,
3. φ_i je vyvozena z φ_j a φ_ℓ pomocí pravidla MP (pro nějaké j, ℓ menší než i).

□

Cvičení 19 *Provedte pečlivě celý důkaz. (V bodě 3 tedy předpokládáme, že např. φ_ℓ je tvaru $\varphi_j \rightarrow \varphi_i$, a z indukčního předpokladu plyne, že $T \vdash \varphi \rightarrow \varphi_j$ a $T \vdash \varphi \rightarrow (\varphi_j \rightarrow \varphi_i)$.)*

Cvičení 20 *Použijte větu o dedukci k důkazu tvrzení o **tranzitivitě implikace**: pokud platí $T \vdash \varphi_1 \rightarrow \varphi_2$ a $T \vdash \varphi_2 \rightarrow \varphi_3$, tak také platí $T \vdash \varphi_1 \rightarrow \varphi_3$.*

Mj. jsme připomněli **větu o neutrální formuli**

$$(T, \varphi \vdash \psi \text{ a } T, \neg\varphi \vdash \psi) \text{ právě tehdy, když } T \vdash \psi,$$

což je věta 2.37 v [1]. Rovněž jsme diskutovali **větu o důkazu sporem** (2.35):

$$T \vdash \varphi \text{ právě tehdy, když } T, \neg\varphi \vdash \neg(\psi \rightarrow \psi) \text{ (pro jakékoli } T, \varphi, \psi).$$

Vzpomněli jsme si na dřívější sémantické tvrzení

$$T \models \varphi \text{ právě tehdy, když } T \cup \{\neg\varphi\} \text{ je nesplnitelná}$$

a z vět o korektnosti a úplnosti (tedy z faktu $T \vdash \varphi \iff T \models \varphi$) jsme pak platnost věty o důkazu sporem snadno vyvodili.

Cvičení 21 *Jako cvičení si proveďte přímý důkaz věty o důkazu sporem, podobně jako v [1].*

Věta o důkazu sporem se dá také formulovat takto:

$$T \vdash \varphi \text{ právě tehdy, když } T \cup \{\neg\varphi\} \text{ je sporná,}$$

přičemž pojem sporné množiny je definován následovně: *množina formulí T je sporná*, jestliže z T lze dokázat každá formule. Následující tvrzení totiž ukazuje, že T je sporná právě tehdy, když z T lze dokázat nějakou kontradikci. Platnost tvrzení zase plyne ihned z vět o korektnosti a úplnosti (tedy z faktu $T \vdash \varphi \iff T \models \varphi$).

Tvrzení 16 *Pro každou množinu $T \subseteq \text{FML}$ platí:*

$$T \vdash \varphi \text{ pro nějakou kontradikci } \varphi \text{ právě tehdy, když } T \vdash \psi \text{ pro každou formuli } \psi.$$

O **větě o ekvivalenci** (2.34) jsme se jen zmínili, posluchači si ji jistě snadno promyslí. Základem je fakt, že vznikne-li formule φ' z formule φ nahrazením jednoho výskytu podformule ψ formulí ψ' , pak $\psi \leftrightarrow \psi' \vdash \varphi \leftrightarrow \varphi'$ (tedy z předpokladu, že ψ a ψ' jsou ekvivalentní lze dokázat ekvivalenci φ a φ'). Z faktu “ $T \vdash \varphi \iff T \models \varphi$ ” lze zase odvodit snadno.

Cvičení 22 *Existuje ovšem i přímý důkaz věty o ekvivalenci, zkuste si na něm procvičit strukturální indukci.*

Příklady analýzy pomocí logiky. Rozebrali jsme si jednoduchý “příklad ze života” o zvířatech putujících do českých zoo, na což nám stačilo modelování v rámci výrokové logiky.

Pak jsme se podívali na jednoduchý počítačový program provádějící celočíselné dělení a zamysleli se nad důkazem jeho správnosti. K formulaci invariantu cyklu (podmínky, která platí vždy na začátku provádění cyklu) i k formulaci dalších výroků už nám výroková logika nestačila. Uvědomili jsme si, že potřebujeme výroky strukturovat, nevystačíme s výrokovými symboly. Při důkazu správnosti jsme využili tzv. predikátovou logiku (prvního řádu); zatím jsme se spolehli na její intuitivní pochopení.

Také jsme predikátovou logiku intuitivně využili při rozboru příkladu ze Smullyanovy knížky; jednalo se o soubor dvou tvrzení “Já nemám bratra” a “Otec muže na obrázku je synem mého otce”, z nichž máme zjistit, kdo je na obrázku.

Pak jsme diskutovali syntaxi predikátové logiky (rámcově podle kap. 3.1. v [1]).

Týden 6

Podrobněji jsme ještě probrali důkaz věty o kompaktnosti pro VL (výrokovou logiku):

Věta (o kompaktnosti). $T \subseteq \text{FML}$ je splnitelná právě tehdy, když každá konečná $T' \subseteq T$ je splnitelná. (Tedy když T je nespjitelná, tak existuje konečná $T' \subseteq T$, která je nespjitelná.)

Důkaz. Směr “ \Rightarrow ” je zřejmý: Když existuje pravdivostní ohodnocení e , které splňuje T , tedy takové, že $\|\varphi\|_e = 1$ pro všechny $\varphi \in T$, tak přímo toto e ukazuje, že každá $T' \subseteq T$ je splnitelná, tedy i každá konečná $T' \subseteq T$ je splnitelná.

Ukážeme směr “ \Leftarrow ”. Předpokládáme tedy, že každá konečná $T' \subseteq T$ je splnitelná, tedy pro každou konečnou $T' \subseteq T$ existuje e takové, že $\|\varphi\|_e = 1$ pro všechny $\varphi \in T'$. Není ovšem hned zřejmé, že existuje jedno fixní e' , které splňuje každou konečnou $T' \subseteq T$. (Takové e' by pak samozřejmě splňovalo celou T . Proč?) My ale takové e' vybudujeme.

Pro jednoduchost přeznačme výrokové symboly tak, že $VS = \{p_1, p_2, p_3, \dots\}$. Všimněme si, že pro každé $i \geq 1$ máme $\{p_i, \neg p_i\} \not\subseteq T$, jelikož $\{p_i, \neg p_i\}$ je konečná množina, která očividně není splnitelná.

Položíme $T_0 = T$ a pro $i = 1, 2, \dots$ budeme definovat $e'(p_i)$ a množinu T_i tak, že $T_i = T_{i-1} \cup \{p_i\}$ když $e'(p_i) = 1$ a $T_i = T_{i-1} \cup \{\neg p_i\}$ když $e'(p_i) = 0$. Budeme přitom udržovat vlastnost, že každá konečná $T' \subseteq T_i$ je splnitelná nějakým ohodnocením e , které se na množině $\{p_1, p_2, \dots, p_i\}$ shoduje s e' . (Pro T_0 to tedy jen říká, že každá její konečná podmnožina je splnitelná.)

Pro $i = 1, 2, 3, \dots$ postupujeme takto:

1. Pokud platí $p_i \in T_{i-1}$, tak definujeme $T_i = T_{i-1}$ a $e'(p_i) = 1$.

Ověřme, že každá konečná $T' \subseteq T_i$ je splněna nějakým ohodnocením e , které se na $\{p_1, p_2, \dots, p_i\}$ shoduje s e' : Jelikož $T' \cup \{p_i\}$ je konečnou podmnožinou T_{i-1} , je tato množina splněna ohodnocením e , které se na $\{p_1, p_2, \dots, p_{i-1}\}$ shoduje s e' (podle indukčního předpokladu); navíc nutně platí i $e(p_i) = 1$.

2. Pokud platí $\neg p_i \in T_{i-1}$, tak definujeme $T_i = T_{i-1}$ a $e'(p_i) = 0$.

Ověření, že každá konečná $T' \subseteq T_i$ je splněna nějakým ohodnocením e , které se na $\{p_1, p_2, \dots, p_i\}$ shoduje s e' , se provede podobně jako výše.

3. Pokud máme $p_i \notin T_{i-1}$ a $\neg p_i \notin T_{i-1}$, tak platí (alespoň) jedna z těchto podmínek:

- (a) každá konečná $T' \subseteq T_{i-1}$ je splněna nějakým ohodnocením e , které se na $\{p_1, p_2, \dots, p_{i-1}\}$ shoduje s e' a navíc platí $e(p_i) = 1$,
- (b) každá konečná $T' \subseteq T_{i-1}$ je splněna nějakým ohodnocením e , které se na $\{p_1, p_2, \dots, p_{i-1}\}$ shoduje s e' a navíc platí $e(p_i) = 0$.

Kdyby totiž neplatilo ani (a) ani (b), tak by existovala konečná $T' \subseteq T_{i-1}$ taková, že pro každé e splňující T' , které se na $\{p_1, p_2, \dots, p_{i-1}\}$ shoduje s e' , platí $e(p_i) = 0$, a zároveň by existovala konečná $T'' \subseteq T_{i-1}$ taková, že pro každé e splňující T'' , které se na $\{p_1, p_2, \dots, p_{i-1}\}$ shoduje s e' , platí $e(p_i) = 1$. Pak ovšem konečná $T' \cup T'' \subseteq T_{i-1}$ není splnitelná žádným e , které se na $\{p_1, p_2, \dots, p_{i-1}\}$ shoduje s e' , což je spor s udržovanou vlastností (která je zde součástí indukčního předpokladu).

V případě (a) definujeme $T_i = T_{i-1} \cup \{p_i\}$ a $e'(p_i) = 1$; pokud (a) neplatí (a tedy nutně platí (b)), definujeme $T_i = T_{i-1} \cup \{\neg p_i\}$ a $e'(p_i) = 0$.

I zde pro T_i tedy očividně platí, že každá její konečná množina je splnitelná nějakým ohodnocením e , které se na množině $\{p_0, p_1, \dots, p_i\}$ shoduje s e' .

Vidíme, že pro množinu $\bar{T} = \bigcup_{i \geq 0} T_i$ platí, že pro každé $i \geq 1$ je v \bar{T} právě jeden z literálů p_i a $\neg p_i$. Je přitom zřejmé, že e' splňuje každou formuli v \bar{T} (tedy také splňuje množinu $T = T_0$). Pro každou formuli $\varphi \in \bar{T}$ existuje totiž j takové, že všechny výrokové symboly ve φ jsou obsaženy v množině $\{p_1, p_2, \dots, p_j\}$. Máme tedy $\varphi \in T_j$ a φ je proto splněna ohodnocením e , které se na $\{p_1, p_2, \dots, p_j\}$ shoduje s e' , což v tomto případě znamená, že φ je splněna i ohodnocením e' . \square

Také jsme se vrátili k důkazu **věty o úplnosti pro VL**:

Jestliže $T \models \varphi$, pak $T \vdash \varphi$.

Klíčem bylo následující Churchovo lemma, kde jsme použili tuto notaci (pro formuli φ a ohodnocení e):

$$\varphi^e = \begin{cases} \varphi, & \text{jestliže } \|\varphi\|_e = 1, \\ \neg\varphi, & \text{jestliže } \|\varphi\|_e = 0. \end{cases}$$

(Např. pro $\varphi = (p \rightarrow (\neg q \rightarrow r))$ a e , kde $e(p) = 1$ a $e(q) = e(r) = 0$, výraz φ^e označuje formuli $\neg(p \rightarrow (\neg q \rightarrow r))$.)

Lemma 17 Pro každou $\varphi(p_1, \dots, p_n)$ a každé $e : VS \rightarrow \{0, 1\}$ platí $p_1^e, \dots, p_n^e \vdash \varphi^e$.

Důkaz. Pro $\varphi = p$ je to triviální, neboť platí $p \vdash p$ i $\neg p \vdash \neg p$.

Pro $\varphi = \neg\psi$, kde φ je $\varphi(p_1, \dots, p_n)$ a tedy také ψ je $\psi(p_1, \dots, p_n)$, postupujeme takto:

1. $\|\varphi\|_e = 1$

Zde tedy $\varphi^e = \varphi = \neg\psi$ a $\psi^e = \neg\psi$. Podle indukčního předpokladu $p_1^e, \dots, p_n^e \vdash \psi^e$, a tedy $p_1^e, \dots, p_n^e \vdash \neg\psi$; jelikož $\neg\psi = \varphi = \varphi^e$, máme $p_1^e, \dots, p_n^e \vdash \varphi^e$.

2. $\|\varphi\|_e = 0$

Zde tedy $\varphi^e = \neg\varphi = \neg\neg\psi$ a $\psi^e = \psi$. Podle indukčního předpokladu $p_1^e, \dots, p_n^e \vdash \psi^e$, a tedy $p_1^e, \dots, p_n^e \vdash \psi$. Kdybychom měli dokázáno, že

$$\boxed{\vdash \psi \rightarrow \neg\neg\psi} \tag{1}$$

tak pravidlem MP odvodíme $p_1^e, \dots, p_n^e \vdash \neg\neg\psi$, tedy $p_1^e, \dots, p_n^e \vdash \varphi^e$. ((1) bude jako cvičení.)

Pro $\varphi = (\varphi_1 \rightarrow \varphi_2)$, kde φ je $\varphi(p_1, \dots, p_n)$ a tedy také φ_1 je $\varphi_1(p_1, \dots, p_n)$ a φ_2 je $\varphi_2(p_1, \dots, p_n)$, postupujeme takto:

1. $\|\varphi\|_e = 1$

(a) $\|\varphi_1\|_e = 0$ (cvičení)

(b) $\|\varphi_2\|_e = 1$ (cvičení)

2. $\|\varphi\|_e = 0$

Zde tedy $\|\varphi_1\|_e = 1$ a $\|\varphi_2\|_e = 0$. Podle ind. předp. $p_1^e, \dots, p_n^e \vdash \varphi_1$ a $p_1^e, \dots, p_n^e \vdash \neg\varphi_2$. Chceme ukázat, že $p_1^e, \dots, p_n^e \vdash \neg(\varphi_1 \rightarrow \varphi_2)$. Kdybychom věděli, že

$$\boxed{\vdash \varphi_1 \rightarrow (\neg\varphi_2 \rightarrow \neg(\varphi_1 \rightarrow \varphi_2))} \quad (2)$$

tak pravidlem MP odvodíme. ((2) bude jako cvičení.)

□

Cvičení 23 Dokončete důkaz kompletně za předpokladu, že platí (1) a (2).

Cvičení 24 Ukažte, že platí (1) a (2). (Věta 2.31 v [1].)

Cvičení 25 Připomněte si, co je potřeba k dokončení důkazu věty o úplnosti.

Predikátová logika

Kromě rekapitulace před zápočtovou písemkou (z výrokové logiky), která se psala na cvičení, jsme se věnovali sémantice predikátové logiky.

Připomněli jsme si, jak vypadá konkrétní jazyk predikátové logiky (prvního řádu). Tedy, že kromě obecně dané (nekonečné spočetné) množiny *proměnných* (také tzv. předmětových proměnných, či individuových proměnných), jejíž prvky jsou typicky značeny x, y, z, x_1, x_2, \dots apod., symbolů *logických spojek* $\neg, \wedge, \vee, \rightarrow$ (případně ještě \leftrightarrow), *kvantifikátorů* \forall, \exists a *pomocných symbolů* (závorky a čárka), je konkrétní jazyk určen množinou *funkčních symbolů*, obecně typicky značených f, g, h, f_1, f_2, \dots apod., a množinou *predikátových symbolů* (také nazývaných *relační symboly*), obecně typicky značených P, Q, R, P_1, P_2, \dots apod.; každý funkční symbol a predikátový symbol musí mít přiřazenu svou *árnost*, též nazývanou *arita* či *četnost*, což je nezáporné celé číslo.

Znovu jsme se vrátili k příkladu “Kdo je na obrázku?” a navrhli jsme jej formalizovat v jazyce, který měl unární funkční symbol *otec*, unární predikátový symbol *Muz*, binární predikátové symboly *Bratr* a *Syn*, a dále konstanty (tj. nulární funkční symboly) *mluvci* a *clovekZobrazku*. (Pro stručnost jsme tyto symboly psali zkráceně.)

Přitom jsme si připomněli, co jsou to *termy* a *formule* (v daném jazyce); využili jsme samozřejmě strukturální indukci. Také jsme připomněli, že jako základní stačí brát spojky negace \neg a implikace \rightarrow a univerzální kvantifikátor \forall ; speciálně jsme si připomněli, že $(\exists x)\varphi$ chápeme jako zkratku za $\neg(\forall x)\neg\varphi$.

Sémantika predikátové logiky. V principu jsme postupovali podle části 3.2. v [1]. Uvědomili jsme si, že k jazyku \mathcal{J} určenému trojicí $(\mathcal{F}, \mathcal{R}, \text{AR})$, kde \mathcal{F} je množina funkčních symbolů, \mathcal{R} množina predikátových (neboli relačních) symbolů, a AR je zobrazení $\text{AR} : \mathcal{F} \cup \mathcal{R} \rightarrow \mathbb{N}$ určující aritu jednotlivých symbolů, existuje nekonečně mnoho možných realizací, nebo též interpretací; konkrétní realizace je dána strukturou

$$\mathbf{M} = (U^{\mathbf{M}}, \mathcal{F}^{\mathbf{M}}, \mathcal{R}^{\mathbf{M}}),$$

kde $U^{\mathbf{M}}$ je neprázdná množina zvaná *univerzum* a množiny $\mathcal{F}^{\mathbf{M}}, \mathcal{R}^{\mathbf{M}}$ obsahují konkrétní funkce a predikáty na $U^{\mathbf{M}}$.

Funkčnímu symbolu f s aritou n je přiřazena funkce $f^{\mathbf{M}} : (U^{\mathbf{M}})^n \rightarrow U^{\mathbf{M}}$ a predikátovému symbolu P s aritou n je přiřazen predikát $P^{\mathbf{M}}$, tedy množina $P^{\mathbf{M}} \subseteq (U^{\mathbf{M}})^n$. Výrazem $(U^{\mathbf{M}})^n$ zde značíme kartézský součin $U^{\mathbf{M}} \times U^{\mathbf{M}} \times \dots \times U^{\mathbf{M}}$ s n výskyty $U^{\mathbf{M}}$.

Máme-li konkrétní strukturu \mathbf{M} , *ohodnocením* (valuací) rozumíme zobrazení

$$v : \text{VAR} \rightarrow U^{\mathbf{M}},$$

kde VAR označuje množinu (předmětových) proměnných. Definovali jsme si, co to je hodnota termu t pro dané \mathbf{M}, v ; je to jistý prvek $U^{\mathbf{M}}$, který označujeme $\|t\|_{\mathbf{M},v}$. Hodnota $\|\varphi\|_{\mathbf{M},v}$ pro formuli φ je prvek množiny $\{0, 1\}$ (nebo též prvek množiny $\{\text{FALSE}, \text{TRUE}\}$).

Uvědomili jsme si terminologii, mj. význam následujících pojmů:

- formule φ je pravdivá (nebo splněna) ve struktuře \mathbf{M} při ohodnocení v (tj. $\|\varphi\|_{\mathbf{M},v} = 1$),
- formule φ je pravdivá ve struktuře \mathbf{M} (čímž se rozumí, že je pravdivá v \mathbf{M} při každém ohodnocení v),
- formule φ je logicky platná (nebo vždy pravdivá, nebo tautologie); tím se rozumí, že je pravdivá v každé struktuře \mathbf{M} (realizující příslušný jazyk).

Definovali jsme a demonstrovali, co jsou *vázané* a *volné výskyty* proměnných ve formuli a zavedli značení $\varphi(x/t)$ pro formuli vzniklou z φ substitucí termu t za všechny *volné* výskyty proměnné x . Přitom jsme si uvědomili, co znamená pojem “ve formuli φ je term t substituovatelný za proměnnou x ”: žádný výskyt proměnné y v t se nesmí ve $\varphi(x/t)$ stát vázaným. Uvědomili jsme si i důvod tohoto omezení.

Např. term $z \cdot x$ není substituovatelný za y ve formuli $y < z \rightarrow (\exists x)y + x = z$.

Příkladem si také připomínáme běžnou infixovou notaci pro binární funkce a predikáty.

Striktně podle definice bychom měli uvedenou formuli psát $<(y, z) \rightarrow (\exists x) = (+ (y, x), z)$.

Uvědomili jsme si, že v našem příkladu s mužem na obrázku jsme z uvedených formalizovaných předpokladů vyvodili závěr $\text{Syn}(\text{clovekZobrazku}, \text{mluvci})$ (neboli “člověk na obrázku je synem mluvčího”) díky naší znalosti zamýšlené realizace použitého jazyka; vše jsme totiž interpretovali v příslušné struktuře LIDSTVO . Pak jsme si uvědomili, že k předpokladům stačí dodat několik vybraných formulí našeho jazyka, které jsou pravdivé ve struktuře LIDSTVO (při všech konkrétních ohodnoceních proměnných), a z nich lze pak už závěr $\text{Syn}(\text{clovekZobrazku}, \text{mluvci})$ vyvodit “syntakticky”, bez odvolávání se na znalost konkrétní struktury LIDSTVO .

De facto jsme tak intuitivně ukázali, že závěr je dokazatelný v teorii sestávající z příslušných předpokladů a oněch vybraných formulí (říkejme jim dohromady výchozí formule), a je tak pravdivý v každé struktuře, v nichž jsou výchozí formule pravdivé (tedy nejen ve struktuře LIDSTVO). V dalších přednáškách postavíme tuto intuici na pevnou rigorózní bázi.

Týden 7

Ekvivalence formulí.

Napadla nás možnost rozšířit ekvivalenci \equiv , kterou jsme zavedli u výrokové logiky, takto:

položíme $\varphi \equiv \psi$, jestliže pro každou strukturu \mathbf{M} a ohodnocení v platí $\|\varphi\|_{\mathbf{M},v} = \|\psi\|_{\mathbf{M},v}$;

jinými slovy: $\varphi \equiv \psi$, jestliže $\varphi \leftrightarrow \psi$ je logicky platná (neboli tautologie). Uvědomili jsme si, že takto jsou např. ekvivalentní formule

$$(\varphi \rightarrow (\forall x)\psi) \text{ a } (\forall x)(\varphi \rightarrow \psi) \text{ za předpokladu, že } x \text{ není volná ve } \varphi.$$

(Říkáme, že proměnná x není volná ve formuli φ , jestliže v ní nemá žádný volný výskyt.)

Jiná dvojice ekvivalentních formulí je

$$((\forall x)\varphi \rightarrow \psi) \text{ a } (\exists x)(\varphi \rightarrow \psi) \text{ za předpokladu, že } x \text{ není volná v } \psi.$$

Cvičení 26 *Promyslete si důkladně a podrobně demonstруйте, proč jsou formule v uvedených dvojicích opravdu ekvivalentní a proč jsou uvedené podmínky o proměnné x důležité.*

Sémantické vyplývání; pojem $T \models \varphi$.

Zavedli jsme pojem *teorie*; je to prostě množina formulí (může být i nekonečná) v daném jazyce predikátové logiky (určeném množinami funkčních a predikátových symbolů); prvkům takové množiny T se také říká *axiomy teorie T* .

Dostali jsme přirozený nápad definovat $T \models \varphi$ takto: pro každou strukturu \mathbf{M} (k příslušnému jazyku) a každé ohodnocení v musí platit: když $\|\psi\|_{\mathbf{M},v} = 1$ pro každou $\psi \in T$, tak $\|\varphi\|_{\mathbf{M},v} = 1$. *Takto ale pojem sémantického vyplývání nebudeme používat!*

Definovali jsme, kdy je

struktura \mathbf{M} (pro daný jazyk) *modelem teorie T* ,

totiž tehdy, když každá formule $\varphi \in T$ je pravdivá v \mathbf{M} .

Někdy se používá značení $\mathbf{M} \models T$ pro fakt, že \mathbf{M} je modelem T ; to ale raději nebudeme používat, ať se nám nemíchá s níže zavedeným $T \models \varphi$.

Definice. Výraz $T \models \varphi$ znamená, že formule φ je pravdivá v každém modelu teorie T .

Pokud jsou formule v T uzavřené (tedy bez volných proměnných), tak je definice totožná s naším původním nápadem výše. Uvědomili jsme si ale, že např. v právě uvedeném smyslu

$$\begin{aligned} &\text{platí } P(x) \leftrightarrow Q(x) \models P(y) \leftrightarrow Q(y), \\ &\text{ale neplatí } \models (P(x) \leftrightarrow Q(x)) \rightarrow (P(y) \leftrightarrow Q(y)). \end{aligned}$$

Cvičení 27 *Vysvětlete, proč neplatí $\models (P(x) \leftrightarrow Q(x)) \rightarrow (P(y) \leftrightarrow Q(y))$. Pak ukažte, zda platí či neplatí $\models (\forall x)(P(x) \leftrightarrow Q(x)) \rightarrow (P(y) \leftrightarrow Q(y))$.*

Připomněli jsme si mj. standardní axiomatizaci teorie grup G užitím axiomů, které nejsou všechny uzavřené; konkrétně šlo o axiomy

$$\boxed{x \cdot (y \cdot z) = (x \cdot y) \cdot z}, \boxed{x \cdot 1 = x}, \boxed{1 \cdot x = x}, \boxed{(\forall x)(\exists y)x \cdot y = 1}, \boxed{(\forall x)(\exists y)y \cdot x = 1}.$$

Všimli jsme si mj., že neplatí $G \models x \cdot y = y \cdot x$, ale platí např. $G \models (y \cdot x=1 \wedge z \cdot x=1) \rightarrow y = z$. Připomněli jsme totiž

speciální vlastnost predikátu rovnosti “=”

(jazyku, který ho obsahuje, říkáme *jazyk s rovností*), totiž to, že predikát “=” musíme v každé struktuře interpretovat relací identity (to vyžaduje definice sémantiky predikátového počtu pro jazyk s rovností).

Cvičení 28 *Demonstrujte, proč platí $G \models (y \cdot x=1 \wedge z \cdot x=1) \rightarrow y = z$.*

(Hilbertovský) důkazový kalkulus pro predikátovou logiku.

Promysleli jsme si rozšíření důkazového kalkulu pro výrokovou logiku, které zahrnuje práci s kvantifikátory. Diskutovali jsme tak

axiomové schéma *specializace* (nebo též *konkretizace* či *substituce*)

$$(\forall x)\varphi \rightarrow \varphi(x/t), \text{ kde } t \text{ je term substituovatelný za } x \text{ ve } \varphi.$$

Cvičení 29 *Ověřte, že za dané podmínky substituovatelnosti platí $\models (\forall x)\varphi \rightarrow \varphi(x/t)$, a ukažte, proč je ta podmínka pro tuto platnost důležitá.*

Dále jsme diskutovali axiomové schéma *distribuce* (kvantifikátoru)

$$(\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi) \text{ za předpokladu, že } x \text{ není volná ve } \varphi.$$

Cvičení 30 *Ověřte, že za dané podmínky platí $\models (\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi)$, a ukažte, proč je ta podmínka pro tuto platnost důležitá.*

Přidali jsme dedukční pravidlo *generalizace*:

z φ odvod $(\forall x)\varphi$, psáno také

$$\frac{\varphi}{(\forall x)\varphi}.$$

Cvičení 31 *Uvědomte si platnost této implikace: $T \models \varphi$ implikuje $T \models (\forall x)\varphi$.*

Tak jsme dostali pojem *dokazatelnosti* $T \vdash \varphi$ i pro predikátovou logiku.

Diskutovali jsme pak *větu o korektnosti* (pro predikátovou logiku):

$$T \vdash \varphi \text{ implikuje } T \models \varphi.$$

Týden 8

Připomněli jsme si větu o korektnosti pro predikátový počet (tj. $T \vdash \varphi$ implikuje $T \models \varphi$) a argumenty pro její platnost. Pak jsme se věnovali větě o úplnosti pro predikátový počet:

Věta 18 (Věta o úplnosti predikátového počtu.)

Pro každou teorii T a každou formuli φ (v jazyce teorie T) platí: jestliže $T \models \varphi$, pak $T \vdash \varphi$.

Věta tedy tvrdí, že naše (tj. hilbertovské) axiomy a dedukční pravidla dostačují k tomu, že každý sémantický důsledek (totiž fakt, že formule φ je pravdivá v každém modelu T , kterých je obecně nekonečně mnoho a mohou být nekonečné) může být demonstrován syntakticky, konečnou posloupností formulí, která představuje příslušný důkaz (ukazující, že φ je dokazatelná z T , neboli že φ je teorémem teorie T).

Pokusili jsme se o poněkud netradiční postup demonstrace platnosti věty o úplnosti, kdy potřebná pomocná tvrzení zjišťujeme až v průběhu (a odkazujeme se na jejich důkazy v následujícím textu či v [1]).

Tímto postupem simulujeme situaci, kdy se v praxi pokoušíme nějaký problém řešit, nějaké tvrzení (např. o nějakém systému) dokázat, a při tomto pokusu zjišťujeme příslušné (pod)problémy, které je třeba dořešit. V učebních textech obvykle tento postup vytváření důkazu není zachycen a čtenáři je předložen už “vyleštěný důkaz”, v němž jsou pomocná tvrzení uvedena předem, ve chvíli, kdy jejich role v celkovém důkazu nemusí být ještě zřejmá.

Nejprve se budeme zabývat teoriemi s *jazyky bez rovnosti* (tj. bez speciálního binárního predikátu “=”). Na případ jazyků s rovností rozšíříme důkaz až následně.

Představme si teď situaci, že máme konkrétní teorii T a formuli φ , kde platí $T \models \varphi$ a $T \not\vdash \varphi$ (což označuje, že neplatí $T \vdash \varphi$); postupně ukážeme, že taková situace není možná. Nejprve si uvědomme, že formule φ nemusí být uzavřená (tj. může mít nějaké volné proměnné); v takových případech může dojít k jistým problémům v deduktivním uvažování. Pro neuzavřené formule např. neplatí úplně analogie věty o dedukci, kterou známe z výrokového počtu.

Minule jsme si všimli, že $\varphi \models \psi$ obecně neimplikuje $\models \varphi \rightarrow \psi$. Kdyby tedy obecně platilo, že $T, \varphi \vdash \psi$ implikuje $T \vdash \varphi \rightarrow \psi$, byl by náš důkazový systém nekorektní. Implikace $T, \varphi \vdash \psi \Rightarrow T \vdash \varphi \rightarrow \psi$ ovšem platí v případě, že φ je uzavřená.

Podle definice sémantiky predikátové logiky máme $T \models \varphi$ právě, když $T \models \bar{\varphi}$, kde $\bar{\varphi}$ je *uzávěr formule* φ .

Má-li φ volné proměnné x_1, x_2, \dots, x_n , pak $\bar{\varphi} = (\forall x_1)(\forall x_2) \dots (\forall x_n)\varphi$; pokud je $n = 0$ (tedy φ je uzavřená), pak $\bar{\varphi} = \varphi$. Pořadí proměnných zde není důležité (snadno nahlédneme, že platí $\models (\forall x)(\forall y)\psi \leftrightarrow (\forall y)(\forall x)\psi$ pro libovolnou formuli ψ), ale nějaké dohodnuté uspořádání proměnných se hodí k tomu, že uzávěr formule lze definovat jednoznačně. Jiná možnost je povolit více uzávěrů k dané formuli φ ; pak $\bar{\varphi}$ prostě označuje jeden z nich.

Poznamenejme ještě, že někdy se také používá *existenční uzávěr* $(\exists x_1)(\exists x_2) \dots (\exists x_n)\varphi$; výše definovaný uzávěr $\bar{\varphi}$ je také nazýván *univerzálním uzávěrem*.

Sémantický fakt “ $T \models \varphi$ právě tehdy, když $T \models \bar{\varphi}$ ” je reflektován i v našem (syntaktickém) kalkulu: je totiž $T \vdash \varphi$ právě tehdy, když $T \vdash \bar{\varphi}$.

Cvičení 32 *Dokažte následující větu.*

Věta o uzávěru.

Pro každou teorii T a každou formuli φ (v jazyce teorie T) platí:

$$T \vdash \varphi \text{ právě tehdy, když } T \vdash \neg\varphi.$$

(Nápověda. Bude se hodit dedukční pravidlo generalizace a axiom konkretizace.)

V situaci $T \models \varphi$ a $T \not\models \varphi$ máme tedy také $T \models \neg\varphi$ a $T \not\models \neg\varphi$. Z předpokladu $T \not\models \neg\varphi$ ovšem plyne, že teorie $T \cup \{\neg\varphi\}$ je bezesporná.

Intuitivně je vidět, že pokud z T nelze dokázat $\neg\varphi$, pak $\neg\varphi$ nebude dokazatelná ani po přidání $\neg\varphi$ k T ; jinými slovy, $T \not\models \neg\varphi$ implikuje $T, \neg\varphi \not\models \neg\varphi$ (což znamená, že z $T \cup \{\neg\varphi\}$ nelze dokázat všechny formule, a tudíž $T \cup \{\neg\varphi\}$ je bezesporná).

Obecně totiž platí $\vdash (\neg\varphi \rightarrow \varphi) \rightarrow \varphi$, podle jednoduché, ale velmi užitečné,

věty o dosazení do tautologie výrokového počtu

(což je Lemma 3.42 v [1]); formule $(\neg\varphi \rightarrow \varphi) \rightarrow \varphi$ vznikne dosazením do tautologie $(\neg p \rightarrow p) \rightarrow p$ a proto je dokazatelná (v každé teorii; dokonce je tzv. *výrokově dokazatelná*, tj. je dokazatelná výhradně z axiomů výrokového počtu s využitím dedukčního pravidla Modus Ponens).

Kdyby tedy platilo $T, \neg\varphi \vdash \neg\varphi$, tak by podle věty o dedukci (viz Věta 3.44 v [1]) platilo i $T \vdash \neg\varphi \rightarrow \neg\varphi$ (jelikož $\neg\varphi$ nemá volné proměnné); pak ovšem díky $\vdash (\neg\varphi \rightarrow \varphi) \rightarrow \varphi$ pomocí pravidla Modus Ponens vyvodíme $T \vdash \varphi$ — což je spor s předpokladem $T \not\models \varphi$. (Lemma 3.56 v [1] ukazuje obecněji, že $T \vdash \varphi$ právě, když $T \cup \{\neg\varphi\}$ je sporná.)

Cvičení 33 *Promyslete si podrobněji zmíněné Lemma 3.42 a Větu 3.44 v [1] s důkazy.*

Předpokládejme teď, že ona bezesporná teorie $T \cup \{\neg\varphi\}$ má nějaký model \mathbf{M} ; v něm je tedy pravdivá každá formule z T a také formule $\neg\varphi$. Struktura \mathbf{M} je tedy také modelem teorie T a proto je v ní pravdivá také formule φ (díky našemu předpokladu $T \models \varphi$). Není ovšem možné, aby v \mathbf{M} byla pravdivá jak φ tak $\neg\varphi$. Takže buď $T \cup \{\neg\varphi\}$ nemá žádný model nebo případ $T \models \varphi$, $T \not\models \neg\varphi$ (a tedy ani případ $T \models \varphi$, $T \not\models \varphi$) neexistuje. Následně ukážeme větu 19 (každá bezesporná teorie má model), z čehož vyplyne, že případ $T \models \varphi$, $T \not\models \varphi$ neexistuje, a tedy věta 18 (o úplnosti) skutečně platí.

Věta 19 *Každá bezesporná teorie má model.*

Důkaz. Uvažujme bezespornou teorii T . O teorii T tedy nic víc nevíme, než že je bezesporná, tedy nelze z ní dokázat všechny formule; speciálně pro žádnou formuli φ nemůže platit $T \vdash \varphi$ a zároveň $T \vdash \neg\varphi$.

Spornost teorie je obvykle definována takto: teorie je sporná, jestliže z ní lze dokázat všechny formule. Jiná ekvivalentní definice říká, že teorie T je sporná, jestliže z T lze dokázat nějakou kontradikci; speciálně jestliže $T \vdash \neg(\varphi \rightarrow \varphi)$ pro nějakou formuli φ . (Připomeňme si, že $\neg(\varphi \rightarrow \varphi)$ je vlastně “překladem” formule $\varphi \wedge \neg\varphi$.) Ta druhá definice spornosti je opravdu ekvivalentní té první: pro libovolné formule φ, ψ totiž máme $\vdash \neg(\varphi \rightarrow \varphi) \rightarrow \psi$ (jelikož $\neg(\varphi \rightarrow \varphi) \rightarrow \psi$ vznikne dosazením do tautologie $\neg(p \rightarrow p) \rightarrow q$ výrokového počtu); z toho plyne, že $T \vdash \neg(\varphi \rightarrow \varphi)$ implikuje $T \vdash \psi$ pro každou formuli ψ (užitím Modus Ponens).

Dokázat, že T má model, lze nejlépe jeho sestrojením. K teorii T sice přísluší nějaký jazyk $\mathcal{J} = (\mathcal{F}, \mathcal{R}, ar)$, ale my o něm nic bližšího nevíme; jakou strukturu tedy máme zvolit k jeho realizaci? Přicházíme k hlavní myšlence důkazu: uvažujeme tzv. *kanonickou strukturu* teorie T , označenou $\mathbf{M}_T = (U^{\mathbf{M}_T}, \mathcal{F}^{\mathbf{M}_T}, \mathcal{R}^{\mathbf{M}_T})$, kde jako univerzum $U^{\mathbf{M}_T}$ vezmeme množinu všech uzavřených termů jazyka \mathcal{J} (teorie T); *uzavřeným termem* chápeme term neobsahující žádnou proměnnou.

Procvičme si strukturální indukci: každá konstanta (tedy nulární funkce jazyka \mathcal{J}) je prvkem $U^{\mathbf{M}_T}$; je-li $f \in \mathcal{F}$ funkční symbol s aritou $ar(f) = n > 0$ a t_1, t_2, \dots, t_n jsou prvky $U^{\mathbf{M}_T}$, pak také řetězec $f(t_1, t_2, \dots, t_n)$ je prvkem $U^{\mathbf{M}_T}$.

Nemáme ovšem zaručeno, že jazyk \mathcal{J} nějakou konstantu obsahuje; kdyby neobsahoval, tak množina $U^{\mathbf{M}_T}$ by byla prázdná a nesplňovala by tak podmínku neprázdnoti, kterou klademe na univerza. V takovém případě prostě libovolnou konstantu c k jazyku teorie T přidáme; vzniklou teorii označme T_c . Je zřejmé, že T_c je rovněž bezesporná; přidání konstanty c , o níž nic speciálního nepředpokládáme, nemůže vést ke sporu. V dalším tedy rovnou předpokládáme, že T obsahuje alespoň jednu konstantu.

Formálně můžeme říci, že rozšíření T_c teorie T je konzervativní. Přesnější a obecnější vyjádření tohoto faktu obsahuje *věta o konstantách*, která je uvedena jako Věta 3.52 v [1].

Máme tedy definováno neprázdné univerzum $U^{\mathbf{M}_T}$. Musíme rozhodnout, jak budeme interpretovat funkční symboly, tedy jakou konkrétní funkci $f^{\mathbf{M}_T}$ přiřadíme n -árnímu funkčnímu symbolu f . Pro každou n -tici (t_1, t_2, \dots, t_n) prvků univerza $U^{\mathbf{M}_T}$, tedy pro n -tici uzavřených termů, musíme určit prvek univerza $U^{\mathbf{M}_T}$, který je hodnotou $f^{\mathbf{M}_T}(t_1, t_2, \dots, t_n)$. Jelikož řetězec $f(t_1, t_2, \dots, t_n)$ je také uzavřený term (tedy prvek $U^{\mathbf{M}_T}$), přirozeně se nabízí následující interpretace:

$$f^{\mathbf{M}_T}(t_1, t_2, \dots, t_n) = f(t_1, t_2, \dots, t_n).$$

Konstanta (nulární funkce) je speciální případ uvedené definice: máme tedy $c^{\mathbf{M}_T} = c$.

Jako příklad můžeme vzít jazyk s binárním funkčním symbolem “ f ” a konstantou “ 1 ”. Příslušné univerzum je tedy nekonečná množina řetězců v abecedě obsahující symboly “ 1 ”, “ f ”, “(”, “)” a “;”, konkrétně množina $\{1; f(1, 1); f(1, f(1, 1)); f(f(1, 1), 1); f(f(1, 1), f(1, 1)); f(1, f(1, f(1, 1))); \dots\}$, v jejímž zápisu je použit symbol “;” pro oddělení jednotlivých prvků.

Máme-li místo f binární funkční symbol “ \cdot ” a použijeme-li infixovou notaci, je příslušné univerzum $\{1; (1 \cdot 1); (1 \cdot (1 \cdot 1)); ((1 \cdot 1) \cdot 1); ((1 \cdot 1) \cdot (1 \cdot 1)); (1 \cdot (1 \cdot (1 \cdot 1))); \dots\}$. Aplikujeme-li funkci $\cdot^{\mathbf{M}_T}$ např. na argumenty $(1 \cdot 1)$ a 1 , dostaneme jako výsledek $((1 \cdot 1) \cdot 1)$.

Dále musíme rozhodnout, jak interpretovat predikátové symboly z \mathcal{R} , konkrétně, kdy zařadíme n -tici (t_1, t_2, \dots, t_n) uzavřených termů do množiny $P^{\mathbf{M}_T}$ pro n -ární predikátový symbol P (tedy, kdy prohlásíme $P^{\mathbf{M}_T}(t_1, t_2, \dots, t_n)$ za pravdivý).

Viděli jsme, že univerzum a interpretace funkčních symbolů jsou plně určeny jazykem teorie T (či jejího rozšíření T_c), nejsou přitom důležité axiomy teorie T .

Připomeňme, že pojmem *axiomy teorie T* rozumíme formule, které jsou prvky T . (Říká se jim také *mimologické axiomy*, ať se odliší od obecně platných logických axiomů odpovídajících pěti schémátům hilbertovského kalkulu.) Pojmem *teorémy teorie T* rozumíme

všechny formule, které jsou dokazatelné z T (tedy všechny φ , pro něž máme $T \vdash \varphi$). Každý axiom teorie T je tedy také teorémem teorie T (ale ne nutně naopak).

Interpretace predikátových symbolů už ovšem na axiomech T závisí. Chceme totiž, aby struktura \mathbf{M}_T byla modelem teorie T , tedy aby všechny axiomy teorie T byly v \mathbf{M}_T pravdivé; pak tam ovšem budou pravdivé i všechny teorémy teorie T (podle věty o korektnosti). Definujeme tedy n -ární $P^{\mathbf{M}_T}$ tak, že pro každou n -tici uzavřených termů (t_1, t_2, \dots, t_n) máme

$$P^{\mathbf{M}_T}(t_1, t_2, \dots, t_n) \text{ právě tehdy, když } T \vdash P(t_1, t_2, \dots, t_n).$$

Když tedy platí $T \vdash P(t_1, t_2, \dots, t_n)$, pak platí $P^{\mathbf{M}_T}(t_1, t_2, \dots, t_n)$; pokud $T \nvdash P(t_1, t_2, \dots, t_n)$, platí $\neg P^{\mathbf{M}_T}(t_1, t_2, \dots, t_n)$. Zde připouštíme možnost, že z T nelze dokázat ani $P(t_1, t_2, \dots, t_n)$ ani $\neg P(t_1, t_2, \dots, t_n)$. Potřeba tzv. úplnosti teorie T vyvstane až za chvíli.

Pro demonstraci toho, že struktura \mathbf{M}_T je modelem teorie T , stačí ukázat, že pro každý axiom $\varphi \in T$ je jeho uzávěr $\overline{\varphi}$ pravdivý v \mathbf{M}_T .

Budeme postupovat strukturální indukcí. Jak tomu ovšem často bývá, k tomu, abychom dokázali požadované, ukáže se potřebným zesílit indukční předpoklad. Zesílíme ho nejdříve tak, že pro každou uzavřenou formuli φ budeme chtít, aby z platnosti $T \vdash \varphi$ plynulo $\|\varphi\|_{\mathbf{M}_T} = 1$ (neboli: každý uzavřený teorém teorie T je pravdivý v \mathbf{M}_T).

Toto jistě platí pro uzavřené atomické formule $P(t_1, \dots, t_n)$, protože v tom případě jsou t_1, \dots, t_n uzavřené termy a z $T \vdash P(t_1, \dots, t_n)$ plyne $\|P(t_1, \dots, t_n)\|_{\mathbf{M}_T} = 1$ přímo z naší definice struktury \mathbf{M}_T .

Zkusme teď uplatnit strukturální indukci na případ $\varphi = \neg\psi$; jelikož diskutujeme jen uzavřené formule, je φ uzavřená, a tedy také ψ je uzavřená (tj. nemá volné proměnné).

Pokud platí $T \vdash \psi$, tak podle indukčního předpokladu máme $\|\psi\|_{\mathbf{M}_T} = 1$; v tom případě je vše v pořádku, protože $\|\neg\psi\|_{\mathbf{M}_T} = 0$ a nemůže platit $T \vdash \neg\psi$, protože T je bezesporná. Když tedy $T \nvdash \psi$, tak máme $T \nvdash \varphi$ a $\|\varphi\|_{\mathbf{M}_T} = 0$.

Pokud ovšem máme $T \nvdash \psi$, indukční předpoklad nám moc nepomůže. Musíme ho ještě zesílit takto: chceme docílit, aby pro každou uzavřenou φ platilo, že

$$T \vdash \varphi \text{ právě tehdy, když } \|\varphi\|_{\mathbf{M}_T} = 1. \quad (3)$$

To ovšem pro naši teorii T nemusí platit. Můžeme totiž mít $T \nvdash P(t_1, \dots, t_n)$ a zároveň $T \nvdash \neg P(t_1, \dots, t_n)$; pak pro $\varphi = \neg P(t_1, \dots, t_n)$ máme $\|\varphi\|_{\mathbf{M}_T} = 1$ ale $T \nvdash \varphi$. Jistě nás napadne, že v takovém případě lze do T přidat $P(t_1, \dots, t_n)$ (nebo $\neg P(t_1, \dots, t_n)$); vznikne tak sice nekonzervativní rozšíření T' teorie T , ale je to bezesporné rozšíření (jak jsme si již v obecnější formě všimli dříve); pochopitelně každý model teorie T' (pokud nějaký existuje) je i modelem teorie T .

To nás vede k pojmu úplné teorie T a k větě o zúplnění bezesporné teorie, kterou se budeme zabývat později. Dále tedy budeme rovnou předpokládat, že naše T je *úplná*, tedy že pro každou uzavřenou formuli φ platí právě jedna z možností $T \vdash \varphi$ a $T \vdash \neg\varphi$.

Pojem úplnosti teorie je samozřejmě jiný než pojem úplnosti predikátového počtu. Teorie je úplná, jestliže je bezesporná a zároveň každou uzavřenou formuli φ “rozhoduje”, tj. dokáže buď ji samotnou nebo její negaci.

Pusťme se teď do důkazu vztahu (3) pro uzavřené formule φ strukturální indukcí.

1. Příklad, kdy φ je atomická.
Podle definice \mathbf{M}_T máme $T \vdash P(t_1, \dots, t_n)$ právě tehdy, když $\|P(t_1, \dots, t_n)\|_{\mathbf{M}_T} = 1$ (pro uzavřené termy t_1, \dots, t_n).
2. Příklad $\varphi = \neg\psi$.
 - (Pod)příklad $T \vdash \psi$ jsme už vyřešili dříve.
 - Když $T \not\vdash \psi$, tak z indukčního předpokladu (3) aplikovaného na ψ (která je uzavřená, protože φ je uzavřená) plyne $\|\psi\|_{\mathbf{M}_T} = 0$, a tedy $\|\varphi\|_{\mathbf{M}_T} = 1$ (neboť $\varphi = \neg\psi$); přitom z faktu $T \not\vdash \psi$ a z úplnosti T plyne $T \vdash \neg\psi$, tj. $T \vdash \varphi$.
3. Příklad $\varphi = (\psi_1 \rightarrow \psi_2)$.
Využitím indukčního předpokladu pro ψ_1 a ψ_2 (obě jsou uzavřené, jelikož φ je uzavřená) rutinně prověříme, že ve všech čtyřech možnostech ohledně (ne)dokazatelnosti ψ_1, ψ_2 z teorie T skutečně platí, že $T \vdash \varphi$ právě tehdy, když $\|\varphi\|_{\mathbf{M}_T} = 1$.

4. Příklad $\varphi = (\forall x)\psi$.
Vztah (3) dokazujeme pro uzavřené formule, uvažujeme tedy uzavřenou φ ; to ovšem nevylučuje, že ψ má jednu volnou proměnnou (označenou zde x). Nelze tedy přímo využít platnost indukčního předpokladu pro ψ . Můžeme ho ovšem využít pro každou uzavřenou instanci formule ψ , tj. pro každou formuli $\psi(x/t)$, kde t je uzavřený term (tedy prvek univerza $U^{\mathbf{M}_T}$). Čili podle indukčního předpokladu máme

$$\text{pro každý term } t \in U^{\mathbf{M}_T} \text{ platí } T \vdash \psi(x/t) \text{ právě tehdy, když } \|\psi(x/t)\|_{\mathbf{M}_T} = 1$$

a chceme vyvodit, že

$$T \vdash (\forall x)\psi \text{ právě tehdy, když } \|(\forall x)\psi\|_{\mathbf{M}_T} = 1. \quad (4)$$

Připomeňme, že podle definice sémantiky predikátové logiky je $\|(\forall x)\psi\|_{\mathbf{M}_T} = 1$ právě tehdy, když pro každé ohodnocení v přiřazující proměnným prvky univerza $U^{\mathbf{M}_T}$ platí $\|\psi\|_{\mathbf{M}_T, v} = 1$. Víme, že z ohodnocení v je zde významná pouze hodnota $v(x)$, což je nějaký uzavřený term t . Podle definice $U^{\mathbf{M}_T}$ pro uzavřený term t platí $\|t\|_{\mathbf{M}_T, v} = t$ (pro libovolné v), takže $\|(\forall x)\psi\|_{\mathbf{M}_T} = 1$ právě tehdy, když pro každý uzavřený term t je $\|\psi(x/t)\|_{\mathbf{M}_T} = 1$.

- (Pod)příklad, kdy pro nějaký uzavřený term t máme $T \not\vdash \psi(x/t)$.
Podle indukčního předpokladu zde máme $\|\psi(x/t)\|_{\mathbf{M}_T} = 0$, z čehož také plyne $\|(\forall x)\psi\|_{\mathbf{M}_T} = 0$. Protože $T \not\vdash \psi(x/t)$, máme také $T \not\vdash (\forall x)\psi$ (neboť z $T \vdash (\forall x)\psi$ by díky axiomu konkretizace $(\forall x)\psi \rightarrow \psi(x/t)$ plynulo $T \vdash \psi(x/t)$). Máme zde tedy $T \not\vdash (\forall x)\psi$ a $\|(\forall x)\psi\|_{\mathbf{M}_T} = 0$, což odpovídá dokazovanému vztahu (4).
- (Pod)příklad, kdy pro všechny uzavřené termy t máme $T \vdash \psi(x/t)$.
Podle indukčního předpokladu zde máme $\|\psi(x/t)\|_{\mathbf{M}_T} = 1$ pro všechny $t \in U^{\mathbf{M}_T}$, z čehož také plyne $\|(\forall x)\psi\|_{\mathbf{M}_T} = 1$. K důkazu vztahu (4) potřebujeme, aby zde platilo $T \vdash (\forall x)\psi$.
Ale ouha! Obecné teorie (byť třeba úplné) nemají vlastnost, že by $T \vdash (\forall x)\psi$ nutně plynulo z toho, že $T \vdash \psi(x/t)$ pro všechny uzavřené termy t .

Mějme např. jazyk daný konstantou c a unárním predikátovým symbolem P (jiné funkční a predikátové symboly tedy jazyk nemá). Uvažujme teorii T obsahující jedinou formuli, a sice $P(c)$. Pro formuli $\varphi = P(x)$ máme očividně $T \vdash \varphi(x/t)$ pro všechny uzavřené termy t ; jediným uzavřeným termem v našem jazyce je totiž c a máme $T \vdash P(c)$. Nemáme ale $T \vdash (\forall x)\varphi$, tj. nemáme $T \vdash (\forall x)P(x)$; např. struktura \mathbf{M} s univerzem $\{1, 2\}$, v níž $c^{\mathbf{M}} = 1$ a $P^{\mathbf{M}} = \{1\}$, je modelem teorie T (protože $\|P(c)\|_{\mathbf{M}} = 1$), v němž formule $(\forall x)P(x)$ není pravdivá (protože $\|P(x)\|_{\mathbf{M},v} = 0$, když $v(x) = 2$). Neplatí tedy $T \models (\forall x)P(x)$ a podle věty o korektnosti nemůže tedy platit ani $T \vdash (\forall x)P(x)$.

V průběhu důkazu jsme si postupně uvědomili potřebnost rozšíření teorie T tak, aby měla aspoň jednu konstantu a aby byla úplná; teď si uvědomujeme, že potřebujeme ještě další vlastnost. Tuto vlastnost naštěstí opět můžeme získat vhodným rozšířením uvažované teorie. Půjde o tzv. henkinovské rozšíření původní teorie T , které je konzervativní (a tak zachovává bezespornost) a v němž bude při jeho úplnosti skutečně zaručeno $T \vdash (\forall x)\psi$ v případě, že platí $T \vdash \psi(x/t)$ pro všechny uzavřené termy t . Zbývá tedy definovat henkinovské teorie a dokázat, že každá bezesporná teorie má úplné henkinovské rozšíření.

Henkinovské teorie se standardně definují s využitím existenčního kvantifikátoru: *teorie T je henkinovská*, jestliže pro každou formuli φ s jednou volnou proměnnou, označenou x , existuje nějaká konstanta c taková, že $T \vdash (\exists x)\varphi \rightarrow \varphi(x/c)$.

Pro úplnou henkinovskou teorii T snadno odvodíme, že platnost $T \vdash \psi(x/t)$ pro všechny uzavřené termy t implikuje $T \vdash (\forall x)\psi$ (kde x je jediná volná proměnná formule ψ):

Předpokládejme $T \not\vdash (\forall x)\psi$; díky úplnosti teorie T máme $T \vdash \neg(\forall x)\psi$, tj. $T \vdash (\exists x)\neg\psi$. Díky henkinovosti existuje pro formuli $\neg\psi$ konstanta c taková, že $T \vdash (\exists x)\neg\psi \rightarrow \neg\psi(x/c)$. Pak ovšem $T \vdash \neg\psi(x/c)$, a tedy $T \not\vdash \psi(x/c)$ (neboť T je úplná, což také zahrnuje, že není sporná). Tedy neplatí, že $T \vdash \psi(x/t)$ pro všechny uzavřené termy t .

Později ukážeme, že každou bezespornou teorii T lze rozšířit na T' , která je úplná (a tedy bezesporná) a henkinovská.

Důkaz věty (že každá bezesporná teorie má model) tím bude tedy ukončen, zatím pro případ teorií v jazycích bez rovnosti. \square

Týden 9

Vybraná tvrzení (na jejichž užitečnost jsme narazili při důkazu věty o úplnosti).

Připomeňme si, co je (univerzální) uzavěr $\overline{\varphi}$ formule φ , a následující větu:

Věta 20 (Věta o uzavěru.)

Pro každou teorii T a každou formuli φ (v jazyce teorie T) platí: $T \vdash \varphi$ právě, když $T \vdash \overline{\varphi}$.

Důkaz. Z $T \vdash \varphi$ plyne $T \vdash \overline{\varphi}$ (vícenásobným) užitím pravidla generalizace. Jelikož $(\forall x)\varphi \rightarrow \varphi$ je instance axiomu konkretizace (je totiž $\varphi = \varphi(x/x)$), je fakt, že z $T \vdash \overline{\varphi}$ plyne $T \vdash \varphi$, také zřejmý. \square

Věta 21 (Věta o dedukci.)

Pro každou teorii T , každou uzavřenou formuli φ (tedy φ bez volných proměnných) a každou formuli ψ platí:

$$T, \varphi \vdash \psi \text{ právě tehdy, když } T \vdash \varphi \rightarrow \psi.$$

Cvičení 34 *Připomeňte si důkaz věty pro výrokovou logiku a ten rozšířte pro predikátovou logiku. Připomeňte si také, proč je zde uzavřenost φ důležitá.*

Připomeňme, že teorie S je *rozšířením* teorie T , jestliže jazyk \mathcal{J}_S teorie S je rozšířením jazyka \mathcal{J}_T teorie T (tj. všechny funkční a predikátové symboly jazyka \mathcal{J}_T jsou také příslušnými symboly, se stejnými aritami, v jazyce \mathcal{J}_S , přičemž jazyk \mathcal{J}_S může obsahovat i nějaké další symboly) a každý teorém teorie T je teorémem teorie S (tedy $T \vdash \varphi$ implikuje $S \vdash \varphi$). Jedná se o *konzervativní rozšíření*, jestliže navíc každý teorém teorie S v jazyce \mathcal{J}_T je rovněž teorémem teorie T (v jazyce \mathcal{J}_T tedy z teorie S lze dokázat přesně ty formule, které jsou dokazatelné z T).

Cvičení 35 *Když S je rozšířením T , platí nutně, že $T \subseteq S$? (Zdůvodněte, proč ne.)*

Další věta mj. říká, jak lze udělat formuli uzavřenou jinak než dodáním kvantifikátorů — za volné proměnné dodáme nové konstanty (o nichž nic nepředpokládáme).

Věta 22 (Věta o konstantách.)

Přidáme-li k jazyku teorie T nové konstanty c_1, c_2, \dots, c_n , dostaneme rozšíření teorie T , které můžeme označit T_{c_1, c_2, \dots, c_n} . Pro každou formuli φ jazyka teorie T a libovolné proměnné x_1, x_2, \dots, x_n pak platí

$$T \vdash \varphi \text{ právě tehdy, když } T_{c_1, c_2, \dots, c_n} \vdash \varphi(x_1/c_1, x_2/c_2, \dots, x_n/c_n).$$

(Z toho rovněž plyne, že T_{c_1, c_2, \dots, c_n} je konzervativním rozšířením teorie T .)

Důkaz. Připomněli jsme nejprve důkaz pro $n = 1$:

- Nechť $T \vdash \varphi$; vezměme nějaký důkaz $\varphi_1, \varphi_2, \dots, \varphi_k$ formule φ z T , tedy mj. platí $\varphi_k = \varphi$. Posloupnost $\varphi_1, \varphi_2, \dots, \varphi_k$ je tedy i důkazem v T_{c_1} . Přidáme formuli $\varphi_{k+1} = (\forall x_1)\varphi$ (použili jsme pravidlo generalizace na φ_k), $\varphi_{k+2} = (\forall x_1)\varphi \rightarrow \varphi(x_1/c_1)$ (instance axiomu konkretizace) a $\varphi_{k+3} = \varphi(x_1/c_1)$ (použijeme Modus Ponens na φ_{k+2} a φ_{k+1}). Takto jsme demonstrovali, že $T_{c_1} \vdash \varphi(x_1/c_1)$.

- Necht $T_{c_1} \vdash \varphi(x_1/c_1)$ a posloupnost $\psi_1, \psi_2, \dots, \psi_m$ je příslušným důkazem (kde $\psi_m = \varphi(x_1/c_1)$). Zvolíme-li proměnnou y , která se v žádné formuli v důkazu nevyskytuje, a nahradíme-li každý výskyt konstanty c_1 v každé formuli ψ_i onou proměnnou y , dostaneme důkaz v teorii T (jak lze snadno ověřit postupně pro $\psi_1, \psi_2, \dots, \psi_m$).

Z toho plyne $T \vdash \varphi(x_1/y)$, a tedy také $T \vdash (\forall y)\varphi(x_1/y)$. Jelikož $(\forall y)\varphi(x_1/y) \rightarrow (\varphi(x_1/y))(y/x_1)$ je instance axiomu konkretizace (x_1 je substituovatelná za y) a $(\varphi(x_1/y))(y/x_1) = \varphi$, vyvodíme, že platí $T \vdash \varphi$.

Dokázali jsme tedy, že pro každou φ v jazyce teorie T platí $T \vdash \varphi$ právě tehdy, když $T_{c_1} \vdash \varphi(x_1/c_1)$. Tím jsme také dokázali, že pro každou ψ v jazyce teorie T_{c_1} platí $T_{c_1} \vdash \psi$ právě tehdy, když $T_{c_1, c_2} \vdash \psi(x_2/c_2)$. Pro každou ξ v jazyce teorie T_{c_1, c_2} platí $T_{c_1, c_2} \vdash \xi$ právě tehdy, když $T_{c_1, c_2, c_3} \vdash \psi(x_3/c_3)$, atd. Z toho již tvrzení věty snadno vyvodíme. \square

Další věta říká, proč je volba vázaných proměnných v (pod)formulích nepodstatná, pokud nekoliduje s volnými proměnnými.

Cvičení 36 Vysvětlete, proč např. formule $(\forall x)(\exists y)P(x, y, z)$ je ekvivalentní s formulí $(\forall x)(\exists y')P(x, y', z)$, ale není ekvivalentní s formulí $(\forall y)(\exists y)P(y, y, z)$ [kde y není substituovatelná za x v $(\exists y)P(x, y, z)$] či s formulí $(\forall z)(\exists y)P(z, y, z)$ [kde sice z je substituovatelná za x v $(\exists y)P(x, y, z)$, ale z má volný výskyt v $(\exists y)P(x, y, z)$].

Věta 23 (Věta o variantách.)

Nechť y není volná v ψ a je substituovatelná za x v ψ . Pokud φ' vznikne z φ nahrazením podformule $(\forall x)\psi$ formulí $(\forall y)(\psi(x/y))$, tak platí $\vdash \varphi \leftrightarrow \varphi'$.

Důkaz. Ukažme nejprve, že za uvedených předpokladů platí $\vdash (\forall x)\psi \leftrightarrow (\forall y)(\psi(x/y))$. (Obecná forma je nechána jako cvičení.)

Nejprve ukažme $\vdash (\forall x)\psi \rightarrow (\forall y)(\psi(x/y))$:

Využijeme větu o konstantách a předpokládáme, že ve formuli $(\forall x)\psi \rightarrow (\forall y)(\psi(x/y))$ nejsou volné proměnné (byly případně nahrazeny novými konstantami). Platí $\vdash (\forall x)\psi \rightarrow \psi(x/y)$, neboť je to axiom konkretizace. Pak podle věty o dedukci (jednodušší směr) máme $(\forall x)\psi \vdash \psi(x/y)$ a užitím pravidla generalizace odvodíme, že platí $(\forall x)\psi \vdash (\forall y)(\psi(x/y))$. Nyní pomocí věty o dedukci (druhý směr, vyžadující, že $(\forall x)\psi$ je uzavřená) vyvodíme, že platí $\vdash (\forall x)\psi \rightarrow (\forall y)(\psi(x/y))$.

Analogicky se ukáže $\vdash (\forall y)(\psi(x/y)) \rightarrow (\forall x)\psi$.

Stačí tedy vyvodit, že také platí $\vdash ((\forall x)\psi \rightarrow (\forall y)(\psi(x/y))) \wedge ((\forall y)(\psi(x/y)) \rightarrow (\forall x)\psi)$.

Ovšem obecně platí $\vdash \varphi_1 \rightarrow (\varphi_2 \rightarrow (\varphi_1 \wedge \varphi_2))$, neboť se jedná o dosazení do tautologie výrokového počtu ve formě $p \rightarrow (q \rightarrow (p \wedge q))$. \square

Cvičení 37 Promyslete si, jak dokončit důkaz předchozí věty.

Věta 24 (Věta o zúplnění.)

Ke každé bezesporné teorii T existuje její rozšíření T' se stejným jazykem, které je úplnou teorií (tedy pro každou uzavřenou φ platí právě jedna z možností $T' \vdash \varphi$, $T' \vdash \neg\varphi$).

Důkaz. Diskutovali jsme již, že když pro uzavřenou formuli φ máme $T \not\vdash \varphi$, tak $T \cup \{\neg\varphi\}$ je bezesporná. Jestliže tedy máme pro uzavřenou φ jak $T \not\vdash \varphi$ tak $T \not\vdash \neg\varphi$, tak teorie $T \cup \{\varphi\}$ i teorie $T \cup \{\neg\varphi\}$ jsou bezesporné.

V (pro nás standardním) případě, že formulí v jazyce teorie T je (jen) spočetně mnoho, lze všechny uzavřené formule uspořádat do posloupnosti $\varphi_0, \varphi_1, \varphi_2, \dots$ a definovat teorie T_0, T_1, T_2, \dots následovně:

- $T_0 = T$ (tedy T_0 je výchozí bezesporná teorie);
- Pokud $T_i \not\vdash \varphi_i$ a $T_i \not\vdash \neg\varphi_i$, pak položíme $T_{i+1} = T_i \cup \{\varphi_i\}$; jinak $T_{i+1} = T_i$.

Je zřejmé, že pro každé $i = 0, 1, 2, \dots$ je T_i bezesporná. Pak je ovšem bezesporná i $T' = T_0 \cup T_1 \cup T_2 \cup \dots$. (Kdyby v T' bylo možné dokázat nějakou kontradikci, tak by příslušný důkaz byl důkazem už v T_i pro nějaké i .)

Teorie T' tak má stejný jazyk jako T , platí $T \subseteq T'$ a T' je úplná (pro každé $i \in \mathbb{N}$ platí právě jeden ze vztahů $T' \vdash \varphi_i$ a $T' \vdash \neg\varphi_i$).

(Poznámka (pro hloubavé čtenáře). Kdyby bylo nespočetně mnoho formulí v jazyce teorie T , tj. jazyk teorie T by obsahoval nespočetně mnoho funkčních a predikátových symbolů, použili bychom nějaké dobré uspořádání uzavřených formulí a transfinite indukci pro definici teorií T_λ , kde λ probíhá příslušný počáteční úsek ordinálních čísel, nejen přirozených. Pro limitní ordinál λ pak definujeme T_λ jako $\bigcup_{\kappa < \lambda} T_\kappa$.)

□

Připomeňme si, jak je definována henkinovská teorie; neformálně řečeno, každá existence je potvrzena speciální konstantou. Přesněji: teorie T je henkinovská, jestliže pro každou formuli φ s jednou volnou proměnnou, označenou x , existuje nějaká konstanta c taková, že $T \vdash (\exists x)\varphi \rightarrow \varphi(x/c)$. Ukážeme teď větu, která se nám hodila pro důkaz věty o úplnosti pro predikátovou logiku.

Věta 25 (Věta o henkinovském rozšíření.)

Ke každé teorii existuje její konzervativní rozšíření, které je henkinovskou teorií.

Důkaz. Uvažujme nějakou teorii T a formuli φ s jednou volnou proměnnou, označenou x , pro niž neexistuje konstanta c taková, že $T \vdash (\exists x)\varphi \rightarrow \varphi(x/c)$. Rozšíříme nejdříve jazyk teorie T o novou (dosud se v tom jazyce nevyskytující) konstantu c ; vzniklá teorie, označená T_c , je konzervativním rozšířením teorie T (podle věty o konstantách). Navíc přidejme (henkinovský) axiom $(\exists x)\varphi \rightarrow \varphi(x/c)$; teorii T_c jsme tak rozšířili na $T'_c = T_c \cup \{(\exists x)\varphi \rightarrow \varphi(x/c)\}$.

Ukažme, že T'_c je konzervativní rozšíření teorie T . Nechť tedy $T'_c \vdash \psi$ pro nějakou formuli ψ v jazyce teorie T . Podle věty o dedukci máme

$$T_c \vdash ((\exists x)\varphi \rightarrow \varphi(x/c)) \rightarrow \psi.$$

Pokud v příslušném důkazu v teorii T_c nahradíme každý výskyt konstanty c proměnnou y , která se v žádné formuli důkazu nevyskytuje, dostaneme důkaz v teorii T , jak lze snadno ověřit. Ukázali jsme tak, že

$$T \vdash ((\exists x)\varphi \rightarrow \varphi(x/y)) \rightarrow \psi.$$

Použitím generalizace a korektní distribucí kvantifikátorů (o práci s kvantifikátory jsme pojednali a ještě pojednáme zvlášť) dostaneme postupně:

$$\begin{aligned}
T &\vdash (\forall y)((\exists x)\varphi \rightarrow \varphi(x/y)) \rightarrow \psi, \\
T &\vdash ((\exists y)((\exists x)\varphi \rightarrow \varphi(x/y))) \rightarrow \psi, \\
T &\vdash ((\exists x)\varphi \rightarrow (\exists y)\varphi(x/y)) \rightarrow \psi.
\end{aligned}$$

Podle věty o variantách máme $\vdash (\exists x)(\varphi) \rightarrow (\exists y)\varphi(x/y)$, neboť y se ve φ nevyskytuje. Užitím Modus Ponens dostáváme $T \vdash \psi$. Takže T'_c je skutečně konzervativním rozšířením teorie T .

Znovu uvažujme výchozí teorii T , označenou také T_0 . Ukázali jsme, jak zařídit “henkinovost” pro jednu formuli $\varphi(x)$. Nyní uvažujme proces, který to udělá naráz pro všechny příslušné formule s jednou volnou proměnnou: pro každou formuli typu $\varphi(x)$ přidá její výlučnou novou “henkinovskou konstantu” c_φ a příslušný henkinovský axiom $(\exists x)\varphi \rightarrow \varphi(x/c_\varphi)$. Tím vznikne teorie T_1 , která je konzervativním rozšířením T_0 , jak lze snadno ověřit (úvahami jako výše). Ovšem T_1 nemusí být henkinovská, její jazyk byl oproti T_0 rozšířen. Proto uvažujme stejný proces rozšíření T_1 , čímž dostaneme T_2 , atd. Nakonec pro teorii $T' = T_0 \cup T_1 \cup T_2 \cup \dots$ snadno ověříme, že je henkinovská a přitom je konzervativním rozšířením teorie T . \square

Týden 10

Začneme ještě procvičením práce s kvantifikátory.

Cvičení 38 *Ukažte, že platí*

$$\models (\forall x)(\varphi \rightarrow \psi) \rightarrow ((\forall x)\varphi \rightarrow (\forall x)\psi),$$

$$\models (\forall x)(\varphi \rightarrow \psi) \rightarrow ((\exists x)\varphi \rightarrow (\exists x)\psi).$$

Jsou logicky platné i obrácené implikace?

Cvičení 39 *Ukažte, že*

1. $(\forall x)(\varphi \rightarrow \psi) \rightarrow ((\forall x)\varphi \rightarrow (\forall x)\psi)$ je ekvivalentní s $((\forall x)(\varphi \rightarrow \psi) \wedge (\forall x)\varphi) \rightarrow (\forall x)\psi$;

2. $(\forall x)(\varphi \rightarrow \psi) \rightarrow ((\exists x)\varphi \rightarrow (\exists x)\psi)$ je ekvivalentní s $((\forall x)(\varphi \rightarrow \psi) \wedge (\exists x)\varphi) \rightarrow (\exists x)\psi$.

(Nápověda. Všimněte si, že $(p \rightarrow (q \rightarrow r)) \leftrightarrow ((p \wedge q) \rightarrow r)$ je tautologie výrokové logiky.)

Jazyky s rovností (a věta o úplnosti).

Dokončili jsme již důkaz věty o úplnosti predikátového počtu pro teorie s jazyky bez rovnosti.

Teď zkoumáme *jazyky a teorie s rovností*; připomínáme, že u nich se (binární) predikátový symbol “=” musí ve strukturách povinně realizovat identitou. To sice axiomy predikátového počtu nevynutí, ale k dosavadním axiomovým schémátům se (alespoň) dodají tzv. *axiomy rovnosti*:

1. $x = x$;
2. $(x_1 = y_1 \wedge x_2 = y_2 \wedge \dots \wedge x_n = y_n) \rightarrow f(x_1, x_2, \dots, x_n) = f(y_1, y_2, \dots, y_n)$,
pro každý n -ární funkční symbol f v příslušném jazyku;
3. $(x_1 = y_1 \wedge x_2 = y_2 \wedge \dots \wedge x_n = y_n) \rightarrow (P(x_1, x_2, \dots, x_n) \rightarrow P(y_1, y_2, \dots, y_n))$,
pro každý n -ární predikátový symbol v příslušném jazyku.

Tyto formule jsou očividně pravdivé v každé struktuře, kde je relační (neboli predikátový) symbol “=” realizován identitou. Věta o korektnosti ($T \vdash \varphi$ implikuje $T \models \varphi$) tedy platí i pro teorie s rovností.

Mluvili jsme také o závislosti a nezávislosti v množinách axiomů. Mj. bychom mezi axiomy rovnosti mohli očekávat formule “ $x = y \rightarrow y = x$ ” a “ $(x = y \wedge y = z) \rightarrow x = z$ ”. Uvědomili jsme si ale, že ty se dají odvodit (v našem hilbertovském predikátovém kalkulu) díky axiomům rovnosti 1 a 3.

Speciálně jsme si to ukázali pro symetrii (tj. pro formuli $x = y \rightarrow y = x$):

Jednou z instancí axiomu rovnosti 3 je

$$(x = y \wedge x = x) \rightarrow (x = x \rightarrow y = x).$$

Z toho mj. plyne, že platí $\vdash x = x \rightarrow (x = y \rightarrow y = x)$. (Využili jsme zde toho, že

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

je tautologie výrokového počtu.) Protože $x = x$ je axiom, platí také $\vdash x = y \rightarrow y = x$.

Cvičení 40 Zkuste podobně ukázat, že platí $\vdash (x = y \wedge y = z) \rightarrow x = z$.

Když nepožadujeme od realizace relačního symbolu “=” nic víc, než splnění uvedených axiomů rovnosti, pak v modelu \mathbf{M} teorie T může být “=” realizován nějakou kongruencí vzhledem k realizacím všech funkčních a predikátových symbolů příslušného jazyka.

Připomeňme, že relace ρ na množině U je *ekvivalence*, jestliže je binární ($\rho \subseteq U \times U$), reflexivní ($x\rho x$), symetrická ($x\rho y$ implikuje $y\rho x$) a tranzitivní ($x\rho y$ a $y\rho z$ implikuje $x\rho z$). Ekvivalence ρ je *kongruencí vzhledem k funkci* (neboli operaci) $f : U^n \rightarrow U$, jestliže z $x_1\rho y_1, x_2\rho y_2, \dots, x_n\rho y_n$ plyne $f(x_1, x_2, \dots, x_n) \rho f(y_1, y_2, \dots, y_n)$. Relaci ρ chápeme jako *kongruenci vzhledem k predikátu* $P \subseteq U^n$, jestliže z $x_1\rho y_1, x_2\rho y_2, \dots, x_n\rho y_n$ plyne, že $(x_1, \dots, x_n) \in P$ právě tehdy, když $(y_1, \dots, y_n) \in P$.

Z věty 19 (každá bezesporná teorie má model) plyne, že i každá bezesporná teorie s rovností má model, pokud dovolíme realizovat symbol “=” jakoukoli relací splňující axiomy rovnosti; taková relace je pak nutně kongruence vůči realizacím všech příslušných funkčních a predikátových symbolů. Musíme ale dokázat, že v tom případě existuje i model, v němž je symbol “=” realizován identitou. K tomu stačí příslušnou strukturu faktorizovat podle oné kongruence:

Máme-li strukturu $\mathbf{M} = (U, \mathcal{F}, \mathcal{R})$, ve které je nějaká relace \equiv kongruencí vzhledem ke všem $f \in \mathcal{F}$ a $P \in \mathcal{R}$, pak definujeme strukturu \mathbf{M}/\equiv (faktorizace \mathbf{M} podle kongruence \equiv) jako trojici $(U', \mathcal{F}', \mathcal{R}')$ sestavenou takto:

- jako univerzum U' vezmeme množinu všech tříd ekvivalence \equiv , tedy

$$U' = \{[a]_{\equiv} \mid a \in U\}, \text{ kde } [a]_{\equiv} = \{b \in U \mid b \equiv a\};$$

- ke každé n -ární funkci $f \in \mathcal{F}$ zařadíme do \mathcal{F}' n -ární funkci f' splňující

$$f'([a_1]_{\equiv}, \dots, [a_n]_{\equiv}) = [f(a_1, \dots, a_n)]_{\equiv};$$

- pro každý n -ární predikát $P \in \mathcal{R}$ zařadíme do \mathcal{R}' n -ární predikát P' , pro nějž platí

$$P'([a_1]_{\equiv}, \dots, [a_n]_{\equiv}) \text{ právě tehdy, když } P(a_1, \dots, a_n).$$

Díky tomu, že \equiv je kongruence, je uvedená definice korektní (tedy opravdu jednoznačně definuje funkce f' a predikáty P' , jak lze snadno ověřit). Zároveň je zřejmé, že když \mathbf{M} je modelem teorie T , tak také struktura \mathbf{M}/\equiv je modelem této teorie. Navíc pro relaci \equiv v \mathbf{M} je její protějšek \equiv' ve struktuře \mathbf{M}/\equiv identitou.

Máme totiž $[a]_{\equiv} \equiv' [b]_{\equiv}$ právě tehdy, když $a \equiv b$, tedy právě tehdy, když třídy ekvivalence $[a]_{\equiv}$ a $[b]_{\equiv}$ jsou si rovny.

Když tedy \mathbf{M} je modelem teorie T , ve kterém relace \equiv realizuje symbol “=”, pak \mathbf{M}/\equiv je modelem teorie T , ve kterém je symbol “=” realizován identitou.

Faktorizaci podle kongruence jsme si také připomněli na známé struktuře $(\mathbf{Z}, \{+, \cdot\}, \{\equiv_5\})$ množiny celých čísel s operacemi sčítání a násobení a s kongruencí “modulo 5” (kde $a \equiv_5 b$, jestliže hodnoty $(a \bmod 5)$ a $(b \bmod 5)$ jsou si rovny; např. $17 \equiv_5 2 \equiv_5 -8$).

Tím jsme dokončili důkaz věty o úplnosti ($T \models \varphi$ implikuje $T \vdash \varphi$) i pro teorie s rovností.

Věta o kompaktnosti.

Všimněme si zobecnění věty o kompaktnosti, kterou jsme diskutovali u výrokové logiky; uvedeme ji ve dvou verzích:

Věta 26 (Věta o kompaktnosti (pro predikátovou logiku).)

1. *Teorie T má model právě tehdy, když každá konečná $T' \subseteq T$ má model.*
2. *$T \models \varphi$ právě tehdy, když existuje konečná $T' \subseteq T$, pro niž platí $T' \models \varphi$.*

Všimněme si, že je to tvrzení o sémantice. V případě výrokové logiky jsme příslušné tvrzení dokázali přímo a pak jsme jej použili k demonstraci úplnosti (syntaktického) axiomatického systému výrokového počtu. U predikátové logiky toto tvrzení naopak elegantně dokážeme využitím věty o úplnosti:

Důkaz. 1. Model teorie T je pochopitelně modelem i každé $T' \subseteq T$. Předpokládejme teď, že T nemá model; je tedy sporná (protože každá bezesporná má model). V T tedy existuje důkaz sporu, tedy důkaz nějaké kontradikce. Tento důkaz je ovšem konečnou posloupností formulí, takže je to důkaz i v nějaké konečné $T' \subseteq T$; tedy existuje i konečná $T' \subseteq T$, která je sporná a tudíž nemá model.

2. Implikace “ \Leftarrow ” plyne snadno z definice \models . Pro důkaz “ \Rightarrow ” předpokládejme $T \models \varphi$. Podle věty o úplnosti máme i $T \vdash \varphi$. Příslušný důkaz je důkazem i v nějaké konečné $T' \subseteq T$, tedy $T' \vdash \varphi$, a podle věty o korektnosti máme $T' \models \varphi$. \square

Uveďme alespoň jednu aplikaci věty o kompaktnosti; ukazuje, že v predikátové logice prvního řádu (kterou se zabýváme) nelze zachytit pojem konečnosti struktur:

Tvrzení 27

Když má teorie T konečné modely neomezených velikostí, tak má i nekonečný model.

Důkaz. Uvažujme teorii T , pro niž pro libovolné $n \in \mathbb{N}$ existuje model, jehož univerzum je konečné a má více než n prvků. Definujme množinu formulí $\alpha_1, \alpha_2, \alpha_3, \dots$, kde

$$\alpha_i \text{ je formule } (\forall x_1)(\forall x_2) \cdots (\forall x_i)(\exists y)(x_1 \neq y \wedge x_2 \neq y \wedge \cdots \wedge x_i \neq y).$$

(Zápis $x \neq y$ je pochopitelně zkratka za $\neg(x = y)$.)

Snadno odvodíme, že každá konečná podmnožina množiny $T \cup \{\alpha_1, \alpha_2, \alpha_3, \dots\}$ má model. (Odvoďte.)

Podle věty 26(1) má tedy i množina $T \cup \{\alpha_1, \alpha_2, \alpha_3, \dots\}$ model. V něm jsou pravdivé mj. všechny formule α_i , z čehož vyvodíme, že onen model nemůže být konečný. \square

Prenexní forma formulí. Na variantě příkladu 3.74 z [1] jsme si přiblížili převod formule φ na ekvivalentní formuli φ' v prenexní formě (neboli v prenexním tvaru).

Formule φ je v *prenexní formě*, jestliže je ve tvaru $(Q_1x_1)(Q_2x_2) \cdots (Q_nx_n)\psi$, kde x_1, x_2, \dots, x_n jsou navzájem různé proměnné, $Q_i \in \{\exists, \forall\}$ pro každé $i = 1, 2, \dots, n$ a ψ neobsahuje žádné kvantifikátory.

K převodu se speciálně hodí si připomenout ekvivalence zachycené např. ve větě 3.47 v [1], umožňující korektně “prohazovat implikace s kvantifikátory”. (Probírali jsme při přednáškách a mj. diskutovali chybu v poslední ekvivalenci, (24), v 3.47 v [1].)

Týden 11

Presburgerova aritmetika.

Připomněli jsme si základní pojmy teorie vyčíslitelnosti, speciálně pojem *rozhodnutelné množiny* (neboli rekurzivní množiny) a *částečně rozhodnutelné množiny* (neboli rekurzivně spočetné množiny) (či obecně algoritmicky [částečně] rozhodnutelného problému).

Věta 28 *Presburgerova aritmetika, tj. množina $Th(\mathbb{N}, Plus)$, je rozhodnutelná.*

Množinu $Th(\mathbb{N}, Plus)$ chápeme jako množinu těch uzavřených formulí predikátové logiky prvního řádu s ternárním predikátovým symbolem *Plus*, které jsou pravdivé ve standardním modelu s univerzem $\mathbb{N} = \{0, 1, 2, \dots\}$ při interpretaci $Plus(x, y, z)$ jako vztahu $x + y = z$.

Důkaz se dá elegantně provést využitím teorie konečných automatů (neprovedli jsme).

Gödelovy věty o neúplnosti.

Následující důležitý výsledek v 30. letech 20. století vzbudil mezi matematiky velký rozruch:

Věta 29 *Množina $Th(\mathbb{N}, Plus, Mult)$ není rozhodnutelná.*

Množina $Th(\mathbb{N}, Plus, Mult)$ je definovaná analogicky jako $Th(\mathbb{N}, Plus)$, přičemž predikát $Mult(x, y, z)$ je interpretován jako vztah $x \cdot y = z$.

Podstatou důkazu nerozhodnutelnosti je, že ke každému Turingovu stroji M a jeho vstupu w lze algoritmicky sestavit formuli $\Phi_{M,w}(x)$ v jazyce s *Plus* a *Mult* (v níž je x jediná volná proměnná) tak, že M se zastaví na w právě tehdy, když (uzavřená) formule $(\exists x)\Phi_{M,w}$ je pravdivá (ve standardním modelu \mathbb{N} , tj. je prvkem $Th(\mathbb{N}, Plus, Mult)$). Formule $\Phi_{M,w}(x)$ je konstruována tak, že de facto říká: číslo x je kódem výpočtu stroje M na w , který skončí v koncové konfiguraci. (Číslo x tedy kóduje příslušnou posloupnost konfigurací stroje M ; podmínka, že posloupnost odpovídá instrukcím stroje M se dá vyjádřit pomocí sčítání a násobení, což vyžaduje kus technické víceméně rutinní práce.)

Další velmi důležitý výsledek se týká neúplnosti axiomatizací aritmetiky (tzv. *první Gödelova věta o neúplnosti*):

Věta 30 *Každá axiomatizace struktury $(\mathbb{N}, Plus, Mult)$ v jazyce predikátové logiky prvního řádu, která je korektní (tj. všechny její uzavřené dokazatelné formule patří do $Th(\mathbb{N}, Plus, Mult)$) a rozhodnutelná (tj. existuje algoritmus, který rozhoduje, zda daná formule je axiomem), je neúplná, což znamená, že existuje formule v $Th(\mathbb{N}, Plus, Mult)$, která není dokazatelná (neboli existuje pravdivá formule, která není dokazatelná).*

V důkazu lze využít výše zmíněné formule $\Phi_{M,w}(x)$ a větu o rekurzi, a dále očividný fakt, že pro každou uvedenou axiomatizaci existuje enumerátor \mathcal{E} , který generuje všechny uzavřené dokazatelné formule. (V takové axiomatizaci je množina důkazů rozhodnutelná a množina dokazatelných formulí částečně rozhodnutelná.)

Věta o rekurzi je důležitý výsledek teorie vyčíslitelnosti; dá se formulovat tak, že říká, že příkaz “získej svůj vlastní kód” lze chápat jako korektní instrukci programu (Turingova stroje) – dá se totiž implementovat standardními instrukcemi.

Konkrétně můžeme sestavit Turingův stroj S , který se pro každý vstup chová následovně: Získej svůj kód $\langle S \rangle$ a sestav formuli $\neg(\exists x)\Phi_{S,0}$ (která říká “Stroj S se nezastaví na vstup 0”). Spust’ enumerátor \mathcal{E} ; pokud ten někdy vygeneruje onu formuli $\neg(\exists x)\Phi_{S,0}$, zastav se.

Je zřejmé, že program S se na vstup 0 nemůže zastavit (jinak bychom dostali spor s korektností axiomatizace). Formule $\neg(\exists x)\Phi_{S,0}$ je tedy pravdivá (patří do $Th(\mathbb{N}, Plus, Mult)$), ale není v dané axiomatizaci dokazatelná. (Když ji přidáme jako další axiom, enumerátor \mathcal{E} a tím i stroj S se příslušně změní a dostaneme opět pravdivou nedokazatelnou formuli $\neg(\exists x)\Phi_{S',0}$, kde S' je onen “změněný S ”.)

Druhá Gödelova věta o neúplnosti.

První Gödelova věta o neúplnosti se většinou formuluje tak, že jakýkoli konzistentní formální systém F obsahující základní aritmetiku není úplný – existuje tedy uzavřená formule φ , pro niž systém F nedokáže ani φ ani $\neg\varphi$.

Druhá Gödelova věta o neúplnosti říká, že zmíněný systém F nedokáže svou vlastní bezespornost (není v něm dokazatelná formule $Cons(F)$, která vyjadřuje, že v F není dokazatelná kontradikce).

Důkaz druhé věty je založen na formalizaci důkazu první věty v rámci F .

Logické programování (Prolog), rezoluční metoda, SLD rezoluce,

Uvažovali jsme následující jednoduchý program v programovacím jazyku Prolog. (Název “ProLog” je de facto zkratka za “Programming in Logic”.)

```
parent(adam,peter). % adam is a parent of peter
parent(eve,peter).
parent(adam,paul).
parent(mary,paul).
parent(paul,john).
```

```
descendent(D,A):-parent(A,D).
descendent(D,A):-parent(P,D),descendent(P,A).
```

Poznámka. Jedná se o standardní příklad při úvodu do jazyka Prolog (či obecně při úvodu do logického programování); viz např. webovou stránku R. Bartáka na MFF UK Praha:

<http://ktiml.mff.cuni.cz/~bartak/prolog/contents.html>.

Z Internetu si nějakou implementaci Prologu snadno můžete nainstalovat a vyzkoušet (což vám samozřejmě velmi doporučuji).

Pokud programu výše (např. v souboru facts.pl) zadáme (consult('facts.pl'). a pak) dotaz

```
?- descendent(X,adam),parent(mary,Y).
```

odpoví nám (postupně, např. nový řádek vypíše vždy po zadání středníku)

```
X = peter, Y = paul ;
X = Y, Y = paul ;
X = john, Y = paul ;
false.
```

Týden 12

Diskutovali jsme vztah uvedeného příkladu prologovského programu k predikátové logice. Přirozeně jsme navrhli tento jazyk odpovídající našemu programu:

- výrazy `adam`, `john`, `mary`, `peter`, `paul` chápeme jako konstanty (tedy funkční symboly arity 0);
- výrazy `parent`, zkráceně P , a `descendent`, zkráceně D , chápeme jako predikátové (neboli relační) symboly arity 2;
- výraz `descendent(D,A):-parent(A,D)` chápeme jako formuli $P(y,x) \rightarrow D(x,y)$ (symboly D,A chápeme jako proměnné a nahradili jsme je tak raději našimi zavedenými symboly x,y pro proměnné), která je ekvivalentní formuli $D(x,y) \vee \neg P(y,x)$;
- výraz `descendent(D,A):-parent(P,D),descendent(P,A)` chápeme jako formuli $(P(z,x) \wedge D(z,y)) \rightarrow D(x,y)$, která je ekvivalentní formuli $D(x,y) \vee \neg P(z,x) \vee \neg D(z,y)$.

Prologovský program pak chápeme jako “teorii”, tedy množinu formulí. V našem příkladu ji označíme `PROG`; je to množina těchto formulí:

1. $P(adam, peter)$
2. $P(eve, peter)$
3. $P(adam, paul)$
4. $P(mary, paul)$
5. $P(paul, john)$
6. $D(x, y) \vee \neg P(y, x)$
7. $D(x, y) \vee \neg P(z, x) \vee \neg D(z, y)$

Dotaz (položený prologovskému programu)

`?- descendent(X,adam), parent(mary,Y)`

lze chápat jako formuli $(\exists x_1)(\exists y_1)(D(x_1, adam) \wedge P(mary, y_1))$, označme ji jako `DOTAZ`, a položení dotazu lze chápat tak, že zjišťujeme, zda platí

$$PROG \models DOTAZ.$$

To ovšem platí právě tehdy, když množina $PROG \cup \{\neg DOTAZ\}$ je nesplnitelná, tedy nemá žádný model, neboli když

$$PROG, \neg DOTAZ \models \square,$$

kde \square označuje (nějakou) kontradikci. V našem konkrétním případě to znamená, že když k uvedeným formulím 1 – 7 přidáme formuli

8. $\neg D(x_1, adam) \vee \neg P(mary, y_1)$,

tak z formulí 1 – 8 plyne kontradikce. Podle věty o úplnosti je tedy teorie 1 – 8 sporná, je v ní dokazatelná každá formule (k čemuž stačí, že je v ní dokazatelná nějaká kontradikce). Implementace Prologu ovšem nejsou založeny na hledání důkazu v hilbertovském kalkulu, ale na tzv. rezoluční metodě.

Princip rezoluční metody se u výrokové logiky dá zachytit následovně:

$$(p \vee \varphi), (\neg p \vee \psi) \models \varphi \vee \psi.$$

Pokud φ a ψ jsou “prázdné formule” (tedy ve výrazu chybí), dostáváme

$$p, \neg p \models \square.$$

V našem příkladu z predikátové logiky můžeme zkusit uplatnit rezoluci na formule 6 a 8, označme je φ_6 a φ_8 , ale potřebujeme uplatnit tzv. unifikaci pomocí (vhodné) substituce. Substituce σ je zobrazení přiřazující proměnným termy. V našem příkladě použijme substituci $\sigma_1 = (x_1/x, y/adam)$, čímž znázorňujeme zobrazení, které přiřazuje proměnné x_1 term x , proměnné y term $adam$ a na ostatních proměnných je identitou. Formule $\varphi_6\sigma_1$ (tj. formule φ_6 na niž aplikujeme substituci σ_1) je tedy

$$D(x, adam) \vee \neg P(adam, x)$$

a $\varphi_8\sigma_1$ je

$$\neg D(x, adam) \vee \neg P(mary, y_1).$$

Rezolučním pravidlem vyvodíme φ_9 :

$$9. \neg P(adam, x) \vee \neg P(mary, y_1)$$

Aplikací substituce $\sigma_2 = (x/peter)$ na φ_1 a φ_9 vyvodíme

$$10. \neg P(mary, y_1)$$

a aplikací substituce $\sigma_3 = (y_1/paul)$ na φ_4 a φ_{10} vyvodíme \square . Teď už vidíme, jak Prolog přišel na svou první odpověď $X = peter, Y = paul$. (Jak?)

Stručně jsme diskutovali i další souvislosti (včetně prologovského prohledávání do hloubky), speciálně z pohledu našich znalostí predikátové logiky. Mluvili jsme mj. o

- *Skolemově klauzulární formě* (což je speciální případ prenexní formy, zachovávající splnitelnost původní formule),
- *Herbrandově větě*,
- *algoritmech*, které *částečně rozhodují* tautologičnost formulí predikátové logiky (tento problém není algoritmicky rozhodnutelný!),
- *rezoluční metodě*, využívající mj. *unifikaci* termů a formulí,
- *Hornových klauzulích* (které mohou být *definitní*, neboli *fakty* a *pravidla* [z nichž je tvořen prologovský program], nebo *cílové* [odpovídající dotazům v Prologu]),
- *SLD* (Selective Linear Definite clause) *rezoluci* a specifické implementaci v Prologu,

• ...

Potenciál užitečnosti programování v Prologu jsme si ještě naznačili na příkladu obarvení grafu (reprezentujícího mapu států střední Evropy); diskutovali jsme program

```
color(red).
color(green).
color(blue).

diffcol(X,Y) :- color(X), color(Y), X\= Y.

colmideur(CZ,SK,PL,GE,AU,HG) :-
diffcol(CZ, SK), diffcol(CZ, PL), diffcol(CZ, GE), diffcol(CZ, AU),
diffcol(SK, PL), diffcol(SK, AU), diffcol(SK, HG),
diffcol(PL, GE),
diffcol(GE, AU),
diffcol(AU, HG).
```

a dotaz

```
?- colmideur(CZ,SK,PL,GE,AU,HG).
```

(Připomněli jsme si mj. způsob prohledávání implementovaný v interpretech Prologu, a také jsme diskutovali známý problém čtyř barev ...)

Fuzzy logika. Jen stručně jsme si nastínili, proč je někdy výhodné rozšířit množinu pravdivostních hodnot $\{1,0\}$ (neboli $\{true, false\}$), např. v případě práce s neurčitostí. Větší podrobnosti lze nalézt v [1] a jinde.

Speciálně jsme zauvažovali nad případem výrokové logiky, v němž pravdivostní ohodnocení nepřisuzuje výrokovým symbolům hodnoty 0 a 1, ale podmnožiny jisté množiny \mathcal{E} (představme si pod \mathcal{E} např. množinu expertů). Tedy ohodnocení e je zde typu $VS \rightarrow \mathcal{P}(\mathcal{E})$.

$\mathcal{P}(\mathcal{E})$ označuje potenční množinu množiny \mathcal{E} , tedy množinu $\{X \mid X \subseteq \mathcal{E}\}$. Tato množina se také někdy označuje $2^{\mathcal{E}}$; je to de facto množina zobrazení z \mathcal{E} do množiny $\{0,1\}$.

Jistě vidíme přirozené rozšíření e na zobrazení typu $FML \rightarrow \mathcal{P}(\mathcal{E})$ (kde FML je množina formulí výrokové logiky s množinou výrokových symbolů VS). Speciálně pro toto rozšíření e např. platí $\|\varphi \wedge \psi\|_e = \|\varphi\|_e \cap \|\psi\|_e$ a také $\|\varphi \rightarrow \psi\|_e = (\|\varphi\|_e)' \cup \|\psi\|_e$, kde $'$ je operace doplňku, tedy $X' = (\mathcal{E} \setminus X)$. Zde “plnou pravdu”, tedy 1, reprezentuje celá množina \mathcal{E} , a “plnou nepravdu”, tedy 0, reprezentuje prázdná množina \emptyset .

Jinou přirozenou možností je uvažovat pravdivostní ohodnocení e jako zobrazení typu $VS \rightarrow [0,1]$; oborem (pravdivostních) hodnot je tedy interval reálných čísel od 0 do 1. Zde se ovšem naskytá více rozumných možností, jak definovat např. $\|\varphi \wedge \psi\|_e$ a $\|\varphi \rightarrow \psi\|_e$; jednou z možností jsou Gödelovy operace: pro konjunkci definujeme $\|\varphi \wedge \psi\|_e = \min(\|\varphi\|_e, \|\psi\|_e)$ a pro implikaci bude hodnota $\|\varphi \rightarrow \psi\|_e$ rovna 1 v případě $\|\varphi\|_e \leq \|\psi\|_e$ a rovna $\|\psi\|_e$ v případě $\|\varphi\|_e > \|\psi\|_e$.

Tyto a jiné možnosti struktur pravdivostních hodnot jsou zobecněny pojmem *úplný reziduovaný svaz*. (Opět můžeme odkázat k [1] a dalším snadno dostupným zdrojům pro podrobnosti a další související informace.)

Modální logika, temporální logika.

Připomněli jsme si následující protokol, který má zamezit dvěma souběžným procesům současný přístup do kritické zóny (např. nemohou zároveň tisknout na sdílené tiskárně).

Petersonův protokol (zamezení situace s dvěma procesy v kritické sekci)

Process A :

**** noncritical region ****

$flag_A := true$

$turn := B$

waitfor

$(flag_B = false \vee turn = A)$

**** critical region ****

$flag_A := false$

**** noncritical region ****

Process B :

**** noncritical region ****

$flag_B := true$

$turn := A$

waitfor

$(flag_A = false \vee turn = B)$

**** critical region ****

$flag_B := false$

**** noncritical region ****

Např. pro automatickou verifikaci příslušných vlastností se k vyjádření těchto vlastností (typu “nikdy nenastane případ, že oba procesy se současně ocitnou v kritické sekci”) přirozeně hodí modální logika, či speciálně temporální logika (interpretovaná na tzv. Kripkeho struktuře, tedy struktuře možných světů, v našem případě stavů programu [kde stav zahrnuje aktuální hodnoty programových proměnných a aktuální pozice v provádění jednotlivých procesů]).

Průběh zkoušky. Na závěr jsme probrali otázky ke zkoušce (na další straně) a připomněli si tak probranou látku.

Seznam otázek k ústní zkoušce.

A) Otázky důkazové (VL (výroková logika): 1.–6., PL (predikátová logika): 7.–12.)

1. Věta o dedukci (syntaktická verze).
2. Věta o důkazu sporem ($T \vdash \varphi$ právě tehdy, když $T, \neg\varphi \vdash \neg(\psi \rightarrow \psi)$).
3. Věta o korektnosti.
4. Churchovo lemma: pro libovolnou formuli φ , která neobsahuje jiné výrokové symboly než p_1, \dots, p_n , platí $p_1^e, \dots, p_n^e \vdash \varphi^e$.
5. Věta o kompaktnosti.
6. Věta o úplnosti (kde lze předpokládat platnost věty o kompaktnosti).
7. Věta o konstantách.
8. Věta o henkinovské konstantě.
9. Věta o henkinovském rozšíření.
10. Věta o zúplňování teorií.
11. Věta o úplnosti.
12. Věta o prenexním tvaru.

B) Otázky pojmové a přehledové

1. Co a k čemu je logika? (vymezení pojmu logika, trocha historie, logické paradoxy).
2. Základní syntaktické a sémantické pojmy VL (jazyk, formule, pravdivostní ohodnocení, sémantické vyplývání).
3. Normální formy, tabulková metoda.
4. Axiomatický systém VL (axiomy, pravidlo MP, pojem důkazu).
5. Korektnost a úplnost VL.
6. Základní syntaktické pojmy PL (jazyk, termy, formule).
7. Struktury pro PL, ohodnocení, ohodnocení termů a formulí.
8. Tautologie, splnitelné formule, sémantické vyplývání, teorie a model teorie v PL.
9. Axiomatický systém PL (axiomy, pravidla MP a G, pojem důkazu).
10. Korektnost a úplnost PL.
11. Gödelovy věty o neúplnosti.
12. Logické programování (Prolog), speciálně teoretické základy (hornovské klauzule, substituce, unifikace, rezoluční pravidlo).

Poznámky k průběhu zkoušky:

bez splněního zápočtu nelze jít na zkoušku;

přihlašování na termíny vypsáné v IS STAG (pokud není dohodnuto jinak např. emailem);
zkoušení bude probíhat zejména do konce zkouškového období zimního semestru, při problémech v individuálních případech budu vstřícný domluvě o případném pozdějším termínu;
zkouška bude ústní, s písemnou přípravou: student si náhodně vytáhne dvě otázky, jednu z okruhu A) a druhou z okruhu B);

čas na písemnou přípravu: minimálně 20 minut (s možností nahlížení studenta do svých přinesených studijních materiálů a poznámek); čas na ústní zkoušení: zhruba 30 minut.

Reference

- [1] Radim Bělohávek. *Matematická logika* (belohlavek.inf.upol.cz/vyuka/ML.pdf). 2006.