Matematická logika

(mgr. předmět KMI/MALO)

Petr Jančar

20. prosince 2025

Poznámky k textu. Tento text vznikl v průběhu kurzu v zimním semestru 2025/26 jako podpůrný studijní materiál, dávající přehled o celkovém průběhu a dotýkající se všeho podstatného z náplně kurzu. Jedná se o mírnou modifikaci dřívějšího materiálu. Text je 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]:

> Bělohlávek 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`.

Studium přinejmenším textu R. Bělohlávka [1] studentům našeho kurzu velmi doporučuji, popisuje totiž detailněji i některé části, které zde v textu zmíníme jen stručně. Čtenáře by nemělo zmást, že budeme používat značení, které se někdy mírně liší od značení v [1].

> R. Bělohlávek 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 tento pracovní text je místy formulován jako zápis z přednášky, nikoli jako učební text pro kompletní samostudium. Uvedené příklady k řešení jsou řešeny na cvičeních, ale určitě ne všechny. Každý student by si přinejmenším tyto uvedené příklady měl sám kompletně vyřešit. Další příklady najde v odkazované literatuře, mj. ve sbírce řešených příkladů doc. Kolaříka, která je odkazována na web-stránce našeho předmětu.

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 přečtěte 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 charaktery 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 dánu množinu VS *výrokových symbolů*. Postačí nám např. spočetná množina

$$\mathrm{VS} = \{\mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{p}_0, \mathrm{q}_0, \mathrm{r}_0, \mathrm{p}_1, \mathrm{q}_1, \mathrm{r}_1, \mathrm{p}_2, \mathrm{q}_2, \mathrm{r}_2, \dots\}.$$

Symboly psané $p, q, r, \cdots$ 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

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

definovaný strukturální indukcí následovně:

1. Každý prvek VS je formulí, tedy prvkem FML; neboli, pro každé $p \in \mathrm{VS}$ 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 $\mathrm{p} \in \mathrm{VS}$ 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 $\varphi \in \mathrm{FML}$, pak $\neg\varphi \in \mathrm{FML}$. (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 $\varphi_1 \in \mathrm{FML}$ a $\varphi_2 \in \mathrm{FML}$,
   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 $((\mathrm{p} \wedge \neg\mathrm{q}) \rightarrow \neg(\mathrm{q} \rightarrow \neg\mathrm{r}))$ je formulí, zatímco řetězce $\mathrm{p} \wedge \mathrm{q} \rightarrow \neg(\mathrm{q} \rightarrow \neg\mathrm{r})$ či $\vee\mathrm{p}\neg\mathrm{q}$ podle uvedené definice formulemi 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 *vytvořující posloupnosti* $\varphi_0, \varphi_1, \dots, \varphi_k$ *formule* φ_k; např. posloupnost $\varphi_0 = \mathrm{p}, \varphi_1 = \mathrm{q}, \varphi_2 = \neg\varphi_1, \varphi_3 = (\varphi_0 \wedge \varphi_2)$ je jedna z vytvořujících posloupností formule $(\mathrm{p} \wedge \neg\mathrm{q})$.

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

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

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

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

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

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

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

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

- Funkce $f_\neg$ má 1 proměnnou a splňuje $f_\neg(0) = 1$ a $f_\neg(1) = 0$.
- Funkce $f_\wedge$, $f_\vee$, $f_\to$ 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 $x = y = 0$;
  $f_\to(x, y) = 0$ 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 $e : \mathrm{VS} \longrightarrow \{0,1\}$, tak typu $e : \mathrm{FML} \longrightarrow \{0,1\}$. Zvlášť zdůrazníme, pokud to bude třeba rozlišovat.
- Hodnotu $e(\varphi)$ budeme také označovat $\|\varphi\|_e$ a říkáme jí *hodnota formule φ při pravdivostním ohodnocení e*.
- Použijeme-li pro formuli φ zápis $\varphi(p_1, p_2, \ldots, p_n)$, označujeme tím fakt, že ve φ se nevyskytují jiné výrokové symboly než symboly z množiny $\{p_1, p_2, \ldots, p_n\}$ (ovšem nemusí se v ní vyskytovat všechny). Např. pro formuli $\varphi = ((p \wedge \neg q) \to \neg(q \to \neg r))$ 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 $p_1, p_2, \ldots$ pro prvky VS, nikoli přímo symboly $\mathrm{p}_1, \mathrm{p}_2, \ldots$ (což jsme také mohli udělat); význam by měl být opět jasný.

Strukturální indukcí jsme snadno ukázali:

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

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

Řešení:

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 $p_1, p_2, \ldots, p_n$; lze tedy psát ψ jako $\psi(p_1, p_2, \ldots, p_n)$ a také φ jako $\varphi(p_1, p_2, \ldots, p_n)$.

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

   Dokončete celý důkaz podrobně sami. □

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

Cvičení 5 *Navrhněte postup, jak lze k booleovské funkci $B : \{0,1\}^n \longrightarrow \{0,1\}$ sestrojit formuli φ_B v níž se vyskytují jen výrokové symboly $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n$ a pro každé $(b_1, b_2, \ldots, b_n) \in \{0,1\}^n$ platí $B(b_1, b_2, \ldots, b_n) = \|\varphi_B\|_e$, kde $e(\mathrm{p}_i) = b_i$ pro $i = 1, 2, \ldots, n$. (Nápověda: začněte s funkcemi $B : \{0,1\}^n \longrightarrow \{0,1\}$, 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 $\equiv \subseteq \mathrm{FML} \times \mathrm{FML}$, 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 indukcí 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 uzávorkovaná 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* $(\mathrm{p} \to \mathrm{q}) \wedge \neg \mathrm{q} \to \mathrm{p}$. *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 $\neg\varphi_1$, $\wedge\varphi_1\varphi_2$, $\vee\varphi_1\varphi_2$, $\to \varphi_1\varphi_2$, 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

Tabulková metoda.

Připomněli jsme si tabulkovou metodu, která k dané formuli φ mj. sestrojí tabulku reprezentované booleovské funkce $B_\varphi : \{0,1\}^n \longrightarrow \{0,1\}$, 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 uspořádány. Naše volba $\mathrm{VS} = \{\mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{p}_0, \mathrm{q}_0, \mathrm{r}_0, \mathrm{p}_1, \mathrm{q}_1, \mathrm{r}_1, \mathrm{p}_2, \mathrm{q}_2, \mathrm{r}_2, \dots\}$ přímo nabízí jedno takové uspořádání.

Cvičení 8 *Sestrojte tabulku funkce B_φ, kde formule φ je $((\mathrm{q}_2 \to \neg(\mathrm{p}_1 \wedge \mathrm{r})) \to \mathrm{p}_1)$.*

> 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 $\equiv$.

Normální formy formulí.

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 $f : \{0,1\}^n \longrightarrow \{0,1\}$ umíme sestrojit formuli φ v (úplné) disjunktivní normální formě tak, že $B_\varphi = f$. Totéž jsme ukázali pro konjunktivní normální formu. Ukázali jsme tedy i platnost následujícího tvrzení.

Tvrzení 3 *Ke každé formuli 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 9 *K formuli $((\mathrm{q}_2 \to \neg(\mathrm{p}_1 \wedge \mathrm{r})) \to \mathrm{p}_1)$ z Cvičení 8 sestrojte ekvivalentní formule v KNF i DNF.*

Cvičení 10 *Uvědomte si speciální případ tautologií a kontradikcí. Jak navrhnete ekvivalentní formule v KNF a DNF u nich?*

Funkcionální úplnost systému logických spojek.

Systém logických spojek je *funkcionálně úplný*, jestliže ke každé booleovské funkci f existuje výroková formule φ, v níž se nevyskytují logické spojky, které nejsou v systému, a pro kterou máme $B_\varphi = f$.

Dokázali jsme už, že systém logických spojek $\{\neg, \wedge, \vee\}$ je funkcionálně úplný. (Proč?)

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

$$\varphi_1 \wedge \varphi_2 \equiv \neg(\neg\varphi_1 \vee \neg\varphi_2), \quad \varphi_1 \vee \varphi_2 \equiv \neg(\neg\varphi_1 \wedge \neg\varphi_2),$$
$$\varphi_1 \to \varphi_2 \equiv \neg\varphi_1 \vee \varphi_2, \quad \varphi_1 \vee \varphi_2 \equiv \neg\varphi_1 \to \varphi_2.$$

Z toho jsme snadno odvodili:

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 funkcionálně úplným systémem. Je totiž $\neg p \equiv p|p$ a $p \wedge q \equiv \neg(\neg(p \wedge q)) \equiv \neg(p|q) \equiv (p|q)|(p|q)$. Podobně to platí pro "NOR" ("ani ani"). Logické obvody lze tedy v principu sestavovat z jednoho typu hradel.

Cvičení 11 *Argumenujte, proč systém* $\{\wedge, \vee, \rightarrow\}$ *není funkcionálně úplný. (Nápověda. Ukažte, že k formuli* $\varphi = \neg$p *neexistuje formule* ψ*, v níž všechny logické spojky patří pouze do množiny* $\{\wedge, \vee, \rightarrow\}$ *a zároveň platí* $B_\varphi = B_\psi$*.)*

Logická spojka $\leftrightarrow$ jako zkratka.

Zavedli jsme logickou spojku $\leftrightarrow$ jako zkratku:

$(\varphi \leftrightarrow \psi)$ není (formálně vzato) formule, ale je to zkratka za formuli $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$.

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 formuli (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: $\varphi_1 \equiv \varphi_2 \iff \varphi_1 \leftrightarrow \varphi_2 \in$ 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 Tvrzení 5 pořádně. Jedná se o dvě implikace (na metaúrovni). Nejprve tedy ukažte, že když* $\varphi_1 \equiv \varphi_2$*, tak* $\varphi_1 \leftrightarrow \varphi_2$ *je tautologie. Pak ukažte, že když* $\varphi_1 \leftrightarrow \varphi_2$ *je tautologie, tak* $\varphi_1 \equiv \varphi_2$*.*

Řešení:

Implikace "$\Rightarrow$".

Předpokládejme, že platí $\varphi_1 \equiv \varphi_2$, tedy že pro každé pravdivostní ohodnocení e máme $\|\varphi_1\|_e = \|\varphi_2\|_e$. Uvažme nyní formuli ψ odpovídající zápisu $\varphi_1 \leftrightarrow \varphi_2$, tedy vlastně formuli $(\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1)$. Ukážeme, že ψ je tautologie:

Uvažme libovolné ohodnocení e a připomeňme si, že

$$\|\psi\|_e = f_\wedge\,(f_\rightarrow(\|\varphi_1\|_e, \|\varphi_2\|_e), f_\rightarrow(\|\varphi_2\|_e, \|\varphi_1\|_e)).$$

Jelikož $\|\varphi_1\|_e = \|\varphi_2\|_e$, máme

$$\text{buď } \|\psi\|_e = f_\wedge(f_\to(0,0), f_\to(0,0)) \text{ nebo } \|\psi\|_e = f_\wedge(f_\to(1,1), f_\to(1,1)).$$

Protože $f_\to(0,0) = f_\to(1,1) = 1$ a $f_\wedge(1,1) = 1$, vyjde v obou případech $\|\psi\|_e = 1$.

Implikace "$\Leftarrow$".

Udělejte sami. □

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

Řešení:

Použijme 1 jako zkratku za formuli $(\mathrm{p} \vee \neg\mathrm{p})$ a 0 jako zkratku za formuli $(\mathrm{p} \wedge \neg\mathrm{p})$.

Komutativita $\vee$: $(\varphi \vee \psi) \leftrightarrow (\psi \vee \varphi)$,

komutativita $\wedge$: $(\varphi \wedge \psi) \leftrightarrow (\psi \wedge \varphi)$,

asociativita $\vee$: $((\varphi \vee \psi) \vee \xi) \leftrightarrow (\varphi \vee (\psi \vee \xi))$,

asociativita $\wedge$: $((\varphi \wedge \psi) \wedge \xi) \leftrightarrow (\varphi \wedge (\psi \wedge \xi))$,

absorpční zákony: $(\varphi \wedge (\varphi \vee \psi)) \leftrightarrow \varphi$ a $(\varphi \vee (\varphi \wedge \psi)) \leftrightarrow \varphi$,

distributivní zákony: $\varphi \wedge (\psi \vee \xi) \leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \xi)$ a $\varphi \vee (\psi \wedge \xi) \leftrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \xi)$,

komplementarita: $(\varphi \vee \neg\varphi) \leftrightarrow 1$ a $(\varphi \wedge \neg\varphi) \leftrightarrow 0$.

(Později se zmíníme o vzájemné (ne)závislosti těchto axiomů ...)

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 formuli

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

neboli

$$\Big(\bigwedge_{1 \le i \le m} C_i\Big) \vee \Big(\bigwedge_{1 \le j \le n} C'_j\Big) \quad \equiv \quad \bigwedge_{1 \le i \le m, 1 \le j \le n} (C_i \vee C'_j)\,.$$

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

Věta o substituci a věta o ekvivalenci.

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

Tvrzení 6

1. *Když φ je tautologie a φ' vznikne z φ nahrazením všech výskytů výrokového symbolu p (jakoukoli) formulí ψ, tak φ' je také tautologie.*

2. *Jestliže φ' vznikne z φ nahrazením (jednoho) výskytu podformule ψ ekvivalentní formulí ψ' (máme tedy $\psi \equiv \psi'$), tak $\varphi \equiv \varphi'$ (neboli $\varphi \leftrightarrow \varphi'$ je tautologie).*

Před uvedením důkazu si všimněme, že tiše předpokládáme, že příslušným nahrazováním vznikají zase formule. To lze samozřejmě snadno ukázat strukturální indukcí, jak žádají následující dvě cvičení.

Cvičení 14 *Mějme výrokový symbol $p \in \mathrm{VS}$ a formule $\varphi, \psi \in \mathrm{FML}$. Ukažte, že když ve φ nahradíme každý výskyt symbolu p (pokud tam takový je) formulí ψ, tak vznikne formule; tuto výslednou formuli můžeme označit φ'.*

> **Řešení.** Pokud se p ve φ nevyskytuje, je tvrzení triviální (a $\varphi' = \varphi$). Předpokládejme dále, že se p ve φ vyskytuje. Při provedení strukturální indukce rozlišíme 3 případy (omezíme se na funkcionálně úplný systém logických spojek $\{\neg, \to\}$):
>
> - φ je atomická; v našem případě tedy $\varphi = p$:
>   zde je očividně $\varphi' = \psi$;
> - $\varphi = \neg\xi$:
>   podle indukčního předpokladu, nahrazením všech výskytů p ve formuli ξ formulí ψ vznikne formule ξ'; nahradíme-li tedy všechny výskyty p ve formuli $\neg\xi$ formulí ψ, vznikne formule $\neg\xi'$, což je kýžená φ';
> - $\varphi = (\varphi_1 \to \varphi_2)$:
>   podle indukčního předpokladu, nahrazením všech výskytů p ve formuli φ_1 formulí ψ vznikne formule φ_1' a nahrazením všech výskytů p ve formuli φ_2 formulí ψ vznikne formule φ_2'; nahradíme-li tedy všechny výskyty p ve formuli $(\varphi_1 \to \varphi_2)$ formulí ψ, vznikne formule $(\varphi_1' \to \varphi_2')$, což je kýžená φ'.

Cvičení 15 *Mějme formuli φ, její podformuli ψ a formuli ψ'. Ukažte, že nahradíme-li jeden výskyt ψ ve φ formulí ψ', dostaneme formuli, kterou můžeme označit φ'.*

Důkaz. (Tvrzení 6)

1. Mějme φ, p, ψ, φ' jak je popsáno v tvrzení. Zvolme libovolně pravdivostní ohodnocení e; hodnotu $\|\psi\|_e$ označme b ($b \in \{0,1\}$). Je zřejmé (a strukturální indukcí snadno demonstrovatelné), že hodnota $\|\varphi'\|_e$ je stejná jako $\|\varphi\|_{e'}$, kde $e'(p) = b$ a $e'(q) = e(q)$ pro každé $q \in \mathrm{VS} \setminus \{p\}$. Jelikož φ je tautologie, máme $\|\varphi\|_{e'} = 1$, a tedy také $\|\varphi'\|_e = 1$. Jelikož e bylo zvoleno libovolně, dokázali jsme, že φ' je tautologie.

2. Důkaz je přenechán čtenáři. □

Sémantické vyplývání.

Řekneme, že *množina formulí* $T \subseteq \mathrm{FML}$ 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

$\models \varphi$ je vlastně vyjádření faktu, že φ je tautologie,

a také že

když T je nesplnitelná, tak pro všechny formule φ máme $T \models \varphi$.

Cvičení 16 *Vysvětlete, proč platí* $p \to q, q \to r \models p \to r$ *a proč neplatí* $p \to q \models \neg p \to \neg r$. *Zjistěte, zda platí* $T \models \varphi$, *kde* $T = \{r \to p, \neg q \to r\}$ *a* $\varphi = \neg(p \wedge \neg q)$.

Uvědomili jsme si jednoduchý užitečný fakt:

Tvrzení 7 *$T \models \varphi$ 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 (všechny formule v) 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. □

Sémantická věta o dedukci.

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

Důkaz.

"⇒" (implikace zleva doprava):
Předpokládejme, že pro každé pravdivostní ohodnocení e platí: jestliže e splňuje T a φ, tak splňuje také ψ. Uvažme teď libovolné pravdivostní ohodnocení e' splňující T; ukážeme, že e' splňuje formuli $(\varphi \to \psi)$, čímž bude důkaz (implikace zleva doprava) hotov.

Pokud $\|\varphi\|_{e'} = 0$, pak máme $\|(\varphi \to \psi)\|_{e'} = 1$ (jelikož $f_\to(0, b) = 1$ pro obě $b \in \{0, 1\}$). Pokud $\|\varphi\|_{e'} = 1$, pak podle úvodního předpokladu platí $\|\psi\|_{e'} = 1$, a tedy $\|(\varphi \to \psi)\|_{e'} = 1$ (jelikož $f_\to(1, 1) = 1$).

"⇐" (implikace zprava doleva): cvičení. □

Cvičení 17 *Doplňte část "⇐" v předchozím důkazu.*

Uvedené tvrzení se také nazývá sémantická věta o dedukci; později uvedeme její syntaktickou verzi.

Věta o kompaktnosti výrokové logiky.

Všimněme si, že při zavedení $T \models \varphi$ jsme nemluvili o případu, kdy je T nekonečná, což je užitečné v některých kontextech uvažovat. Dokážeme teď následující větu, ze které např. plyne, že když vrcholy nekonečného grafu G nelze obarvit k barvami (tak, aby žádné dva vrcholy spojené hranou neměly stejnou barvu), tak takto nelze obarvit ani vrcholy nějakého konečného podgrafu G' grafu G.

Věta 9 *(o kompaktnosti). $T \subseteq$ 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. Směr "$\Rightarrow$" je zřejmý (když je množina formulí splnitelná, tak každá její podmnožina je splnitelná).

Pro důkaz směru "$\Leftarrow$" je klíčové si uvědomit, že když každá konečná $T' \subseteq T$ je splnitelná a pro nějaký výrokový symbol p platí, že 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 $T' \subseteq T \cup \{\mathrm{p}\}$ je splnitelná, nebo platí, že každá konečná $T' \subseteq T \cup \{\neg\mathrm{p}\}$ 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 $(T_1 \cup T_2) \setminus \{p, \neg p\}$ je nesplnitelná. (Proč?)

Připomeňme si teď, že množinu VS výrokových symbolů máme uspořádánu a tato množina je spočetná. Pro účely důkazu zde označme její prvky $p_0, p_1, p_2, \ldots$. Výše uvedenou úvahu provedeme postupně pro p_0, pak pro p_1, atd., a zamyslíme se, k čemu dojdeme po provedení tohoto nekonečného procesu.

Vycházíme z množiny T, o níž předpokládáme, že každá její konečná podmnožina je splnitelná. Množinu T postupně rozšiřujeme tak, že nakonec dospějeme k množině $\bar{T} \supseteq T$, pro niž také platí, že každá její konečná podmnožina je splnitelná, a navíc pro každý výrokový symbol p platí, že právě jedna z formulí p a $\neg p$ patří do $\bar{T}$. Pak ovšem pravdivostní ohodnocení e definované

$$e(p) = \begin{cases} 1 \ \ldots \text{ jestliže } p \in \bar{T} \\ 0 \ \ldots \text{ jestliže } \neg p \in \bar{T} \end{cases}$$

splňuje všechny formule z $\bar{T}$, a tedy i všechny formule z T. Skutečně: kdyby totiž existovala $\varphi = \varphi(p_1, p_2, \ldots, p_n)$ v $\bar{T}$ taková, že $\|\varphi\|_e = 0$, tak množina $T' = \{\bar{p}_1, \bar{p}_2, \ldots, \bar{p}_n, \varphi\}$, kde $\bar{p}_i$ jen ten prvek množiny $\{p_i, \neg p_i\}$, který patří do $\bar{T}$, je nesplnitelná (což je spor, protože T' je konečná podmnožina množiny $\bar{T}$). □

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

Cvičení 18 *Dokažte, že když $T' \models \varphi$ a $T' = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$, tak platí*
$\models \varphi_1 \to (\varphi_2 \to (\cdots \varphi_{n-1} \to (\varphi_n \to \varphi) \cdots))$.
(Použijte sémantickou větu o dedukci.)

Týden 4

Nejprve ukážeme ještě podrobnější důkaz věty o kompaktnosti pro výrokovou logiku než minule.

Věta (o kompaktnosti). $T \subseteq \mathrm{FML}$ *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. Směr "⇒"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 "⇐". 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 $\mathrm{VS} = \{\mathrm{p}_1, \mathrm{p}_2, \mathrm{p}_3, \dots\}$. Všimněme si, že pro každé $i \geq 1$ máme $\{\mathrm{p}_i, \neg\mathrm{p}_i\} \not\subseteq T$, jelikož $\{\mathrm{p}_i, \neg\mathrm{p}_i\}$ je konečná množina, která očividně není splnitelná.

Položíme $T_0 = T$ a pro $i = 1, 2, \dots$ budeme definovat $e'(\mathrm{p}_i)$ a množinu T_i tak, že $T_i = T_{i-1} \cup \{\mathrm{p}_i\}$ když $e'(\mathrm{p}_i) = 1$ a $T_i = T_{i-1} \cup \{\neg\mathrm{p}_i\}$ když $e'(\mathrm{p}_i) = 0$. Budeme přitom udržovat vlastnost, že každá konečná $T' \subseteq T_i$ je splnitelná nějakým ohodnocením e, které se na množině $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_i\}$ 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 $\mathrm{p}_i \in T_{i-1}$, tak definujeme $T_i = T_{i-1}$ a $e'(\mathrm{p}_i) = 1$.

   Ověřme, že každá konečná $T' \subseteq T_i$ je splněna nějakým ohodnocením e, které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_i\}$ shoduje s e': Jelikož $T' \cup \{\mathrm{p}_i\}$ je konečnou podmnožinou T_{i-1}, je tato množina splněna ohodnocením e, které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_{i-1}\}$ shoduje s e' (podle indukčního předpokladu); navíc nutně platí i $e(\mathrm{p}_i) = 1$.

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

   Ověření, že každá konečná $T' \subseteq T_i$ je splněna nějakým ohodnocením e, které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_i\}$ shoduje s e', se provede podobně jako výše.

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

   (a) každá konečná $T' \subseteq T_{i-1}$ je splněna nějakým ohodnocením e, které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_{i-1}\}$ shoduje s e' a navíc platí $e(\mathrm{p}_i) = 1$,

   (b) každá konečná $T' \subseteq T_{i-1}$ je splněna nějakým ohodnocením e, které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_{i-1}\}$ shoduje s e' a navíc platí $e(\mathrm{p}_i) = 0$.

   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 $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_{i-1}\}$ shoduje s e', platí $e(\mathrm{p}_i) = 0$, a zároveň by existovala konečná $T'' \subseteq T_{i-1}$ taková, že pro každé e splňující T'', které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_{i-1}\}$ shoduje s e', platí $e(\mathrm{p}_i) = 1$. Pak ovšem konečná $T' \cup T'' \subseteq T_{i-1}$ není splnitelná žádným e, které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_{i-1}\}$ shoduje s e', což je spor s udržovanou vlastností (která je zde součástí indukčního předpokladu).

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

I zde pro T_i tedy očividně platí, že každá její konečná množina je splnitelná nějakým ohodnocením e, které se na množině $\{\mathrm{p}_0, \mathrm{p}_1, \cdots, \mathrm{p}_i\}$ 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 $\neg\mathrm{p}_i$. 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 $\{\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_j\}$. Máme tedy $\varphi \in T_j$ a φ je proto splněna ohodnocením e, které se na $\{\mathrm{p}_1, \mathrm{p}_2, \cdots, \mathrm{p}_j\}$ shoduje s e', což v tomto případě znamená, že φ je splněna i ohodnocením e'. □

Axiomatický systém výrokové logiky.

Dosud jsme se zajímali o sémantiku výrokové logiky (význam formulí, pojmy jako je splnitelnost, tautologie, sémantické vyplývání ...). Teď se zajímáme o syntaktické aspekty. Pohovořili jsme o významu tzv. výrokového kalkulu (výrokového počtu) a pustili se do jeho budování.

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

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

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

Dosazením jakýchkoli formulí (výrokové logiky) za (metaproměnné) $\varphi, \psi, \ldots$ do výše uvedených schémat dostaneme konkrétní *axiomy*. Např. dosazením formule $(\neg\mathrm{p} \to (\mathrm{q} \to \neg\mathrm{r}))$ za φ a formule $(\neg\mathrm{r} \to \mathrm{p})$ za ψ ve schématu 1 dostaneme axiom

$$(\neg\mathrm{p} \to (\mathrm{q} \to \neg\mathrm{r})) \to ((\neg\mathrm{r} \to \mathrm{p}) \to (\neg\mathrm{p} \to (\mathrm{q} \to \neg\mathrm{r}))).$$

Cvičení 19 *Demonstrujte, že každý axiom (tedy každá formule, která je instancí uvedených schémat) je tautologie.*

Dále jsme uvedli *dedukční (odvozovací) pravidlo* MP (Modus Ponens):

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

které čteme "z formulí φ a $\varphi \to \psi$ (nad čarou) lze odvodit formuli ψ (pod čarou)". Např. tedy z formulí $(\neg\mathrm{p} \to (\mathrm{q} \to \neg\mathrm{r}))$ a $((\neg\mathrm{p} \to (\mathrm{q} \to \neg\mathrm{r})) \to (\neg\mathrm{r} \to \mathrm{p}))$ odvodíme pravidlem MP formuli $(\neg\mathrm{r} \to \mathrm{p})$.

Cvičení 20 *Demonstrujte, že když φ a $(\varphi \to \psi)$ jsou tatutologie, pak také ψ je tautologie.*

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; také říkáme, že φ je *teorém teorie* T.

Důkazem φ *z* T je jakákoli posloupnost formulí $\varphi_1, \varphi_2, \ldots, \varphi_k$, kde $\varphi_k = \varphi$ a pro každé $i \in \{1, 2, \ldots, k\}$ 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 $j_1, j_2 \in \{1, 2, \ldots, i-1\}$.

Sestavme si důkaz formule $\mathrm{p} \to \mathrm{p}$ z $\emptyset$, tedy ukažme $\emptyset \vdash \mathrm{p} \to \mathrm{p}$, což také píšeme jako $\vdash \mathrm{p} \to \mathrm{p}$. Náš důkaz je posloupnost pěti formulí $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5$, kde:

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

Ukažme ještě, že platí $T \vdash \varphi$, kde $T = \{\mathrm{r}, (\neg\mathrm{q} \to \neg\mathrm{r})\}$ a $\varphi = \mathrm{q}$. To lze prokázat např. tímto důkazem: $((\neg\mathrm{q} \to \neg\mathrm{r}) \to (\mathrm{r} \to \mathrm{q}))$, $(\neg\mathrm{q} \to \neg\mathrm{r})$, $(\mathrm{r} \to \mathrm{q})$, r, q.

Ověřili jsme korektnost axiomatického systému:

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

Cvičení 21 *Dokažte větu o korektnosti indukcí podle délky důkazu; konkrétně ukažte, že pro každý důkaz* $\varphi_1, \varphi_2, \ldots, \varphi_k$ *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* $T \subseteq \mathrm{FML}$ *a* $\varphi, \psi \in \mathrm{FML}$ *platí*

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

Důkaz. Implikace "$\Leftarrow$" je jednoduchá:

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

Implikaci "⇒" dokážeme takto:

Předpokládáme, že platí $T, \varphi \vdash \psi$. Existuje tedy důkaz formule ψ z teorie $T \cup \{\varphi\}$, tj. příslušná posloupnost formulí $\varphi_1, \varphi_2, \ldots, \varphi_k$, kde $\varphi_k = \psi$. Ukážeme indukcí pro $i = 1, 2, \ldots, k$, že $T \vdash \varphi \to \varphi_i$; z toho plyne, že $T \vdash \varphi \to \psi$. 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 22 *Proveďte pečlivě celý důkaz. (V bodě 3 tedy předpokládáme, že např. φ_ℓ je tvaru $\varphi_j \to \varphi_i$, a z indukčního předpokladu plyne, že $T \vdash \varphi \to \varphi_j$ a $T \vdash \varphi \to (\varphi_j \to \varphi_i)$.)*

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

Cvičení 23 *Použijte větu o dedukci k důkazu tvrzení o **tranzitivitě implikace**:*
pokud platí $T \vdash \varphi_1 \to \varphi_2$ a $T \vdash \varphi_2 \to \varphi_3$, tak také platí $T \vdash \varphi_1 \to \varphi_3$.

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

Věta 14 *(o úplnosti). 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 $\varphi = (p \to (\neg q \to r))$ a e, kde $e(p) = 1$ a $e(q) = e(r) = 0$, výraz φ^e označuje formuli $\neg(p \to (\neg q \to r)))$.)

Lemma 15 *Pro každou $\varphi(p_1, \ldots, p_n)$ a každé $e : \mathrm{VS} \to \{0, 1\}$ platí $p_1^e, \ldots, p_n^e \vdash \varphi^e$.*

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 $\varphi(p_1, \ldots, p_n)$ a tedy také ψ je $\psi(p_1, \ldots, p_n)$, postupujeme takto:

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

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

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

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

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

   tak pravidlem MP odvodíme $p_1^e, \ldots, p_n^e \vdash \neg\neg\psi$, tedy $p_1^e, \ldots, p_n^e \vdash \varphi^e$. ((1) dokážeme příště.)

Pro $\varphi = (\varphi_1 \to \varphi_2)$, kde φ je $\varphi(p_1, \ldots, p_n)$ a tedy také φ_1 je $\varphi_1(p_1, \ldots, p_n)$ a φ_2 je $\varphi_2(p_1, \ldots, p_n)$, 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. $p_1^e, \ldots, p_n^e \vdash \varphi_1$ a $p_1^e, \ldots, p_n^e \vdash \neg\varphi_2$. Chceme ukázat, že $p_1^e, \ldots, p_n^e \vdash \neg(\varphi_1 \to \varphi_2)$. Kdybychom věděli, že

$$\boxed{\vdash \varphi_1 \to (\neg\varphi_2 \to \neg(\varphi_1 \to \varphi_2))} \tag{2}$$

   tak pravidlem MP odvodíme. ((2) dokážeme příště.)

□

Cvičení 24 *Dokončete důkaz kompletně za předpokladu, že platí (1) a (2).*

Týden 5

Připomínáme, že jsme Churchovo lemma (Lemma 15) dokázali za předpokladu, že platí (1) a (2), tedy $\vdash \psi \to \neg\neg\psi$ a $\vdash \varphi_1 \to (\neg\varphi_2 \to \neg(\varphi_1 \to \varphi_2))$ (pro všechny formule $\psi, \varphi_1, \varphi_2$). Ukažme si teď platnost těchto našich předpokladů.

Odvození platnosti $\boxed{\vdash \varphi \to \neg\neg\varphi}$**.**

Podle věty o dedukci chceme vlastně ukázat, že platí $\varphi \vdash \neg\neg\varphi$. Při důkazu věty o dedukci nám stačila axiomová schémata (1) a (2). Teď se zřejmě neobejdeme bez schématu (3). Díky tomuto schématu by vlastně stačilo ukázat, že platí $\vdash \neg\neg\neg\varphi \to \neg\varphi$, neboli $\neg\neg\neg\varphi \vdash \neg\varphi$.

Cvičení 25 *Proč z předpokladu* $\vdash \neg\neg\neg\varphi \to \neg\varphi$ *plyne* $\vdash \varphi \to \neg\neg\varphi$ *?*

Obecněji by mělo platit (má-li být náš axiomatický systém úplný) $\neg\neg\varphi \vdash \varphi$ (pro všechny formule φ, tedy speciálně pak platí i $\neg\neg\neg\varphi \vdash \neg\varphi$). Pořád ale není jasné, jak to demonstrovat. Možná nás napadne, že $\neg\neg\varphi \vdash \varphi$ by plynulo z $\neg\neg\varphi \vdash \neg\varphi \to \neg\neg\neg\varphi$.

Cvičení 26 *Proč z předpokladu* $\neg\neg\varphi \vdash \neg\varphi \to \neg\neg\neg\varphi$ *plyne* $\neg\neg\varphi \vdash \varphi$ *?*
(Nápověda. Použijte axiomové schéma (3) a větu o dedukci.)

Všimněme si, že $\neg\neg\varphi \vdash \neg\varphi \to \neg\neg\neg\varphi$ platí právě tehdy, když $\neg\neg\varphi, \neg\varphi \vdash \neg\neg\neg\varphi$. Ale přece obecně by mělo platit $\neg\varphi, \varphi \vdash \psi$ (pro všechny formule φ, ψ); **ze sporného předpokladu bychom totiž měli být schopni dokázat jakýkoli závěr**. Napišme si to ve dvou verzích (verze si odpovídají díky větě o dedukci):

$$\boxed{\neg\varphi, \varphi \vdash \psi} \text{ neboli } \boxed{\vdash \neg\varphi \to (\varphi \to \psi)}.$$

Platnost je jasná díky tomu, že platí $\vdash \neg\varphi \to (\neg\psi \to \neg\varphi)$ (instance axiom. schématu (1)), $\vdash (\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$ (instance axiom. schématu (3)) a dříve dokázané tvrzení o tranzitivitě implikace.

Zvýrazněme, že jsme také ukázali

$$\boxed{\vdash \neg\neg\varphi \to \varphi}.$$

Odvození platnosti

$$\boxed{\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))}. \tag{3}$$

Díky pravidlu Modus Ponens a větě o dedukci máme $\varphi, \varphi \to \psi \vdash \psi$ a tedy $\varphi \vdash (\varphi \to \psi) \to \psi$.

Cvičení 27 *Kdychom tedy měli k axiomovému schématu (3) ještě obměněné schéma ve formě* $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$*, tak bychom byli s demonstrací platnosti (3) hotovi. Proč?*

My ovšem ukážeme, že opravdu platí

$$\boxed{\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)}:$$

Jelikož platí $\vdash (\neg\neg\varphi \to \varphi)$ a $(\varphi \to \psi) \vdash (\varphi \to \psi)$ a $\vdash (\psi \to \neg\neg\psi)$, tak díky tvrzení o tranzitivitě implikace odvodíme, že platí $(\varphi \to \psi) \vdash (\neg\neg\varphi \to \neg\neg\psi)$, a tedy také $(\varphi \to \psi) \vdash (\neg\psi \to \neg\varphi)$ (díky axiom. schématu (3) a Modus Ponens).

Teď jsme tedy kompletně dokončili důkaz Lemmatu 15 a pokračujeme v důkazu věty o úplnosti (Věty 14).

Nejprve si ukážeme, že pro každou tautologii φ (tedy $\models \varphi$) platí $\vdash \varphi$. Podle Churchova lemmatu víme, že pro tautologii $\varphi = \varphi(p_1, p_2, \ldots, p_n)$ platí $p_1^e, \ldots, p_n^e \vdash \varphi$ pro každé pravdivostní ohodnocení e (neboť $\varphi^e = \varphi$ pro všechna e). Speciálně tedy pro každé e platí

$$p_1, p_2^e \ldots, p_n^e \vdash \varphi \quad \text{a} \quad \neg p_1, p_2^e, \ldots, p_n^e \vdash \varphi.$$

Umíme se tak zbavit p_1 v předpokladech a ukázat, že platí $p_2^e, \ldots, p_n^e \vdash \varphi$? Ano, obecněji to ukazuje další tvrzení, známé jako věta o neutrální formuli:

Věta 16 (Věta o neutrální formuli) *Jestliže $T, \varphi \vdash \psi$ a $T, \neg\varphi \vdash \psi$, pak také $T \vdash \psi$. (Opačně je to triviální: jestliže $T \vdash \psi$, pak $T, \varphi \vdash \psi$ a $T, \neg\varphi \vdash \psi$.)*

Důkaz. Nejprve si ukažme fakt, který speciálně zdůrazníme:

$$\boxed{\vdash (\neg\varphi \to \varphi) \to \varphi}. \tag{4}$$

Když totiž použijeme $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$, což už jsme ukázali jako (3), a dosadíme zde za φ formuli $\neg\varphi$ a za ψ formuli φ, dostaneme $\vdash \neg\varphi \to (\neg\varphi \to \neg(\neg\varphi \to \varphi))$. Několikanásobným použitím věty o dedukci dostaneme tedy $\vdash \neg\varphi \to \neg(\neg\varphi \to \varphi)$ (jak?), a díky axiom. schématu (3) a pravidlu Modus Ponens dostaneme (4).

Teď tedy předpokládejme, že platí $T, \varphi \vdash \psi$ a $T, \neg\varphi \vdash \psi$, neboli $T \vdash \varphi \to \psi$ a $T \vdash \neg\varphi \to \psi$. Máme tedy také $T \vdash \neg\psi \to \varphi$ a tudíž $T \vdash \neg\psi \to \psi$ (využitím dříve dokázaného včetně tvrzení o tranzitivitě implikace). Podle (4) platí $\vdash (\neg\psi \to \psi) \to \psi$, z čehož teď vyvodíme $T \vdash \psi$. □

Cvičení 28 *Dokončete teď demonstraci toho, že když platí $\models \varphi$ (φ je tautologie), tak také platí $\vdash \varphi$ (φ je dokazatelná).*

Věta o úplnosti (Věta 14) tvrdí obecně, že když platí $T \models \varphi$, tak také platí $T \vdash \varphi$.

Pokud je T konečná, tedy $T = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$, tak prostě použijeme věty o dedukci (v sémantické a syntaktické verzi): z $T \models \varphi$ plyne $\models \varphi_1 \to (\varphi_2 \to \cdots (\varphi_k \to \varphi) \cdots)$, a tedy podle už dokázaného $\vdash \varphi_1 \to (\varphi_2 \to \cdots (\varphi_k \to \varphi) \cdots)$, a proto $T \vdash \varphi$.

Cvičení 29 *Pro případ, kdy $T \models \varphi$ a T je nekonečná, použijte větu o kompaktnosti a ukažte, že $T \vdash \varphi$.*

Dokončili jsme tak kompletně důkaz věty o úplnosti. Připomeneme-li větu o korektnosti, víme tedy, že platí

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

Cvičení 30 *Podívejte se na **větu o důkazu rozborem případů** (Věta 2.36) v [1] a dokažte ji využitím faktu, že $T \models \varphi$ právě tehdy, když $T \vdash \varphi$.*

Speciálně se ještě podívejme na **větu o důkazu sporem** (2.35 v [1]):

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

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 31 *Jako cvičení si proveďte přímý důkaz věty o důkazu sporem, podobně jako v [1]. (Částečně jsme to již udělali v rámci důkazu věty o úplnosti.)*

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 17 *Pro každou množinu* $T \subseteq \mathrm{FML}$ *platí:*

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

Zmínili jsme i **větu o ekvivalenci** (2.34 v [1]). 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; připomeňte si v této souvislosti sématickou verzi věty o ekvivalenci, tedy Tvrzení 6(2).

Cvičení 32 *Existuje ovšem i přímý důkaz věty o ekvivalenci, můžete 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.

Týden 6

Predikátová logika

Syntaxe predikátové logiky. (Rámcově podle kap. 3.1. v [1].)
Uvedli jsme, co je konkrétní jazyk $\mathcal{J}$ 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 $x, y, z, x_1, x_2, \ldots$ 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 $f, g, h, f_1, f_2, \ldots$ apod.,
- a množinou *predikátových symbolů* (také nazývaných *relační symboly*), obecně typicky značených $P, Q, R, P_1, P_2, \ldots$ apod.;
- každý funkční symbol a predikátový symbol musí mít přiřazenu svou *árnost*, též nazývanou *arita* či *četnost*, což je nezáporné celé číslo.

Funkčním symbolům s aritou 0 (tzv. nulárním funkčním symbolům) říkáme také *konstanty* a typicky je označujeme symbolem c s případnými indexy apod.

> 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 *mluvci* a *clovekZobrazku*. (Pro stručnost jsme tyto symboly psali zkráceně.)

Definovali jsme *termy* a *formule* (v daném jazyce); využili jsme opět strukturální indukci.
Pro jazyk $\mathcal{J} = (\mathcal{F}, \mathcal{R}, \text{AR})$ ($\text{AR} : \mathcal{F} \cup \mathcal{R} \rightarrow \mathbb{N}$) ,jsou *termy* definovány takto:

1. Každá proměnná x je term.
2. Je-li f funkční symbol arity n ($f \in \mathcal{F}$, $\text{AR}(f) = n$) a $t_1, t_2, \ldots, t_n$ jsou termy, pak $f(t_1, t_2, \ldots, t_n)$ je term.

Formule v daném jazyce $\mathcal{J}$ jsou definovány takto:

1. Je-li P predikátový symbol arity n ($P \in \mathcal{R}$, $\text{AR}(P) = n$) a $t_1, t_2, \ldots, t_n$ jsou termy, pak $P(t_1, t_2, \ldots, t_n)$ je formule; je to tzv. *atomická formule*.
2. Jsou-li φ a ψ formule, pak $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$ jsou formule.
3. Je-li x proměnná a φ formule, pak $(\forall x)\varphi$ a $(\exists x)\varphi$ jsou formule.

Cvičení 33 *Uvažujme např. jazyk* $\mathcal{J} = (\mathcal{F}, \mathcal{R}, \text{AR})$*, kde* $\mathcal{F} = \{\boldsymbol{0}, \boldsymbol{1}, +, \cdot\}$*,* $\mathcal{R} = \{=, <\}$*,* $\text{AR}(\boldsymbol{0}) = \text{AR}(\boldsymbol{1}) = 0$ *a arita ostatních symbolů je* 2*. Sestavte několik termů a formulí v daném jazyku. Napište je jednak striktně podle definice (příkladem je term* $+(x, y)$*) a také si připomeňte běžně užívanou infixovou notaci (v níž napíšeme např. term* $+(x, y)$ *jako* $(x + y)$*).*

Sémantika predikátové logiky. (Rámcově 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 $\text{AR} : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}$ je zobrazení určující aritu jednotlivých symbolů, existuje nekonečně mnoho možných realizací, nebo též interpretací. *Realizace* jazyka $\mathcal{J} = (\mathcal{F}, \mathcal{R}, \text{AR})$ je struktura

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

- $U^{\mathbf{M}}$ je neprázdná množina zvaná *univerzum*,
- $\mathcal{F}^{\mathbf{M}} = \{f^{\mathbf{M}} \mid f \in \mathcal{F}\}$, kde pro funkční symbol f s aritou n je $f^{\mathbf{M}}$ funkce typu $(U^{\mathbf{M}})^n \longrightarrow U^{\mathbf{M}}$,
- $\mathcal{R}^{\mathbf{M}} = \{P^{\mathbf{M}} \mid P \in \mathcal{R}\}$, kde pro predikátový symbol P s aritou n je $P^{\mathbf{M}}$ n-ární predikát (neboli relace) na $U^{\mathbf{M}}$, tedy $P^{\mathbf{M}} \subseteq (U^{\mathbf{M}})^n$.

(Výrazem $(U^{\mathbf{M}})^n$ značíme kartézský součin $U^{\mathbf{M}} \times U^{\mathbf{M}} \times \cdots \times U^{\mathbf{M}}$ s n výskyty $U^{\mathbf{M}}$.)

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

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

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 $\{\text{FALSE}, \text{TRUE}\}$).

Cvičení 34 *Definujte hodnoty* $\|t\|_{\boldsymbol{M},v}$ *a* $\|\varphi\|_{\boldsymbol{M},v}$ *strukturální indukcí.*
Ilustrujte pak např. pro jazyk $\mathcal{J} = (\mathcal{F}, \mathcal{R}, \text{AR})$*, kde* $\mathcal{F} = \{\boldsymbol{0}, \boldsymbol{1}, +, \cdot\}$*,* $\mathcal{R} = \{=, <\}$*,* $\text{AR}(\boldsymbol{0}) = \text{AR}(\boldsymbol{1}) = 0$ *a arita ostatních symbolů je* 2*. Jako realizaci jazyka* $\mathcal{J}$ *vezměte strukturu* $\boldsymbol{M}$ *s univerzem* $\mathbb{N} = \{0, 1, 2, \dots\}$ *a standardně realizovanými funkčními a predikátovými symboly.*

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* (neboli *tautologie*); tím se rozumí, že je pravdivá v každé struktuře $\mathbf{M}$ (realizující příslušný jazyk).

Ekvivalence formulí.

Předpokládáme teď, že jazyk $\mathcal{J} = (\mathcal{F}, \mathcal{R}, \text{AR})$ je zafixován. Ekvivalenci $\equiv$, kterou jsme zavedli u výrokové logiky, jsme v případě predikátové logiky přirozeně definovali takto:

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

Tedy $\varphi \equiv \psi$ platí právě tehdy, když formule $\varphi \leftrightarrow \psi$ je logicky platná (neboli tautologie).

Cvičení 35 *Ukažte, že ke každé formuli φ lze sestrojit ekvivalentní formuli φ', v níž nejsou jiné logické spojky než $\neg$ a $\to$ a není v ní kvantifikátor $\exists$. (Takové formule φ' jsou tedy omezeny na logické spojky $\neg, \to$ a kvantifikátor $\forall$.)*

Volné a vázané výskyty proměnných ve formuli. Připomeňme, že formuli chápeme (také) jako konečný řetězec symbolů z příslušné (obecně nekonečné) abecedy. Pokud je v daném řetězci φ, který je formulí, na pozici i symbol, který je proměnnou x, přičemž na pozici $i-1$ není kvantifikátor ($\forall$ nebo $\exists$), tak symbol x na pozici i chápeme jako (jeden konkrétní) *výskyt proměnné* x ve formuli φ.

> Např. ve formuli $(P(c) \wedge (\forall x)(P(f(x,y)) \to (\exists y)Q(g(y,z),x)))$ jsou dva výskyty proměnné x (nikoli 3); dále jsou tam dva výskyty proměnné y a jeden výskyt proměnné z. Jak bylo řečeno dříve, symbol c používáme pro *konstantu* (tj. nulární funkční symbol).

Výskyt proměnné x ve formuli φ je *vázaný*, jestliže je součástí podřetězce $(\forall x)\psi$ nebo $(\exists x)\psi$ řetězce φ, kde řetězec ψ je formulí; příslušný výskyt je tedy součástí podřetězce ψ. *Výskyt proměnné* x ve formuli φ, který není vázaný, je *volný*.

> Ve formuli $(P(c) \wedge (\forall x)(P(f(x,y)) \to (\exists y)Q(g(y,z),x)))$ jsou oba výskyty proměnné x vázané; proměnná y má v této formuli jeden volný výskyt a jeden vázaný výskyt; výskyt proměnné z v této formuli je volný.

Pokud je výskyt proměnné x ve formuli φ vázaný a $(\forall x)\psi$ nebo $(\exists x)\psi$ je nejkratší podřetězec řetězce φ, který obsahuje tento výskyt x (a ψ je formulí), tak říkáme, že tento výskyt x je *vázán* příslušným *výrazem* $(\forall x)$ nebo $(\exists x)$.

> Např. ve formuli $(\forall x)\,((\exists x)P(x) \to R(x,y))$ jsou dva výskyty proměnné x, první je vázán výrazem $(\exists x)$ a druhý je vázán výrazem $(\forall x)$.

Říkáme také, že *proměnná* x je *volná ve formuli* φ, jestliže x má ve φ alespoň jeden volný výskyt (přičemž tam může mít i vázané výskyty).

Uvědomili jsme si, že

> formule $(\varphi \to (\forall x)\psi)$ a $(\forall x)(\varphi \to \psi)$ jsou ekvivalentní, jestliže x není volná ve φ.

Dále např.

> formule $((\forall x)\varphi \to \psi)$ a $(\exists x)(\varphi \to \psi)$ jsou ekvivalentní, jestliže x není volná v ψ.

Cvičení 36 *Promyslete si důkladně a podrobně demonstrujte, proč jsou formule v uvedených dvojicích opravdu ekvivalentní a proč jsou uvedené podmínky o ne-volnosti proměnné x důležité.*

Substituovatelnost termu za proměnnou. Zavedli jsme značení $\varphi(x/t)$ pro formuli vzniklou z φ substitucí termu t za všechny *volné* výskyty proměnné x. Přitom jsme definovali, kdy platí, že *ve formuli φ je term t substituovatelný za proměnnou x*: žádný výskyt proměnné y ve formuli $\varphi(x/t)$, který se v této formuli objevil díky nahrazení konkrétního výskytu x ve φ termem t, nesmí být ve $\varphi(x/t)$ vázaným.

> Např. term $z \cdot x$ není substituovatelný za y ve formuli $y < z \to (\exists x)\, y + x = z$.
>
> Příkladem si také připomínáme běžnou infixovou notaci pro binární funkce a predikáty. (Striktně dle definice bychom měli uvedenou formuli psát $<(y, z) \to (\exists x)\ =(+(y, x), z)$.)

Cvičení 37 *Ukažte, že formule $(\forall x)\varphi \to \varphi(x/t)$ je tautologie (tedy logicky platná), jestliže t je term substituovatelný za x ve φ.*
Je to obecně tautologie i bez uvedené podmínky substituovatelnosti?

Na závěr jsme si uvědomili, že v našem příkladu s mužem na obrázku jsme z uvedených formalizovaných předpokladů vyvodili závěr $Syn(clovekZobrazku, mluvci)$ (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 $Syn(clovekZobrazku, mluvci)$ vyvodit "syntakticky", bez odvolávání se na znalost konkrétní struktury Lidstvo.

De facto jsme tak intuitivně ukázali, že závěr je pravdivý v každé struktuře, v nichž jsou pravdivé příslušné předpoklady a ony vybrané formule (tedy nejen ve struktuře Lidstvo). Navíc je závěr dokazatelný syntakticky z příslušné množiny formulí. V dalších přednáškách postavíme tuto intuici na rigorózní bázi.

Týden 7

Speciální role predikátu rovnosti.

Definici sémantiky predikátové logiky doplníme touto standardní úmluvou: Pokud uvažovaný jazyk $\mathcal{J} = (\mathcal{F}, \mathcal{R}, \text{AR})$ obsahuje (v $\mathcal{R}$) mj. predikátový symbol rovnosti, tedy "=" s aritou dva, říkáme také, že $\mathcal{J}$ je *jazyk s rovností*; v tom případě vyžadujeme u každé struktury $\mathbf{M}$ realizující jazyk $\mathcal{J}$, že realizace symbolu = (tedy binární relace $=^{\mathbf{M}}$) je identita na univerzu $U^{\mathbf{M}}$. Tedy pravdivostní hodnota $\| = (t_1, t_2)\|_{\mathbf{M},v}$ je 1 právě tehdy, když prvky univerza $U^{\mathbf{M}}$ reprezentované termy t_1 a t_2, tj. $\|t_1\|_{\mathbf{M},v}$ a $\|t_2\|_{\mathbf{M},v}$, jsou totožné. (Pochopitelně místo $= (t_1, t_2)$ píšeme většinou $t_1 = t_2$.)

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.

Definovali jsme, kdy je

$$\text{struktura } \mathbf{M} \text{ (pro daný jazyk) } \textit{modelem teorie } T,$$

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.

Cvičení 38 *Ukažte, že* platí $\boxed{P(x) \models P(y)}$, *ale* neplatí $\models P(x) \to P(y)$, *což také značíme takto:* $\boxed{\not\models P(x) \to P(y)}$.

Ukažte, že na druhé straně platí *jak* $\boxed{(\forall x)P(x) \models P(y)}$, *tak* $\boxed{\models (\forall x)P(x) \to P(y)}$.

Uvědomme si, že to tedy **není** tak, že by $T \models \varphi$ znamenalo, že pro každou strukturu $\mathbf{M}$ (realizující příslušný jazyk) a každé ohodnocení v platí, že když $\|\psi\|_{\mathbf{M},v} = 1$ pro každou $\psi \in T$, tak $\|\varphi\|_{\mathbf{M},v} = 1$. (Speciálně např. $\|P(x)\|_{\mathbf{M},v} = 1$ obecně neimplikuje $\|P(y)\|_{\mathbf{M},v} = 1$, ačkoliv platí $P(x) \models P(y)$.)

Cvičení 39 *Vzpomeňme si na sémantickou větu o dedukci pro výrokovou logiku: $T, \varphi \models \psi$ právě tehdy, když $T \models \varphi \to \psi$. Platí tato věta bezpodmínečně i pro predikátovou logiku?*

Sémantickou větu o dedukci pro predikátovou logiku formulujeme takto:

Věta 18 *Pokud je φ uzavřená formule (tj. neobsahuje volný výskyt žádné proměnné), pak $T, \varphi \models \psi$ právě tehdy, když $T \models \varphi \to \psi$.*

Důkaz. "⇒"
Předpokládejme, že $T, \varphi \models \psi$, kde φ je uzavřená formule. Uvažujme libovolně zvolený model M teorie T a zkoumejme hodnotu $\|\varphi \to \psi\|_{M,v}$ pro libovolně zvolené ohodnocení v. Pokud

ukážeme, že $\|\varphi \to \psi\|_{M,v} = 1$, bude prokázáno $T \models \varphi \to \psi$ (jelikož model M a ohodnocení v byly zvoleny libovolně).

Protože φ je uzavřená, hodnota $\|\varphi\|_{M,v}$ je nezávislá na v a je tedy rovna hodnotě $\|\varphi\|_M$. Když $\|\varphi\|_M = 0$, tak $\|\varphi \to \psi\|_{M,v} = 1$. Když $\|\varphi\|_M = 1$, tak M je modelem teorie $T \cup \{\varphi\}$ a podle předpokladu tedy platí $\|\psi\|_M = 1$, tedy $\|\psi\|_{M,v'} = 1$ pro všechna v'. Tudíž $\|\varphi \to \psi\|_{M,v} = 1$.

"$\Leftarrow$"

Předpokládejme, že $T \models \varphi \to \psi$ (zde φ ani nemusí být uzavřená). Uvažujme libovolně zvolený model M teorie $T \cup \{\varphi\}$ a zkoumejme hodnotu $\|\psi\|_{M,v}$ pro libovolně zvolené ohodnocení v; podle předpokladu je $\|\varphi \to \psi\|_{M,v} = 1$. Jelikož pro M nutně platí $\|\varphi\|_M = 1$, tedy i $\|\varphi\|_{M,v} = 1$, vyvodíme, že $\|\psi\|_{M,v} = 1$. Platí tedy $T, \varphi \models \psi$. □

Příklad: teorie grup.

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. $G \models (y \cdot x{=}1 \wedge z \cdot x{=}1) \to y = z$. (Připomněli jsme přitom speciální vlastnost predikátu rovnosti "=".)

Cvičení 40 *Demonstrujte, proč platí* $G \models (y \cdot x{=}1 \wedge z \cdot x{=}1) \to y = z$.

(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*)

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

Cvičení 41 *Připomeňte si argumenty, proč za dané podmínky substituovatelnosti platí* $\models (\forall x)\varphi \to \varphi(x/t)$ *a proč je ta podmínka pro tuto platnost důležitá.*

Dále jsme diskutovali axiomové schéma *distribuce (kvantifikátoru)*

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

Cvičení 42 *Připomeňte si, proč za dané podmínky platí* $\models (\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$ *a proč je ta podmínka pro tuto platnost důležitá.*

Přidali jsme dedukční pravidlo *generalizace*:

$$\text{z } \varphi \text{ odvoď } (\forall x)\varphi, \text{ psáno také}$$

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

Cvičení 43 *Argumentujte, proč platí tato implikace:* $T \models \varphi$ *implikuje* $T \models (\forall x)\varphi$.

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

Cvičení 44 *Definujte pojem $T \vdash \varphi$ analogicky jako v případě výrokové logiky.*

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

Věta 19 *$T \vdash \varphi$ implikuje $T \models \varphi$.*

Cvičení 45 *Argumentujte detailně, proč věta o korektnosti platí.*

Nakonec jsme jen zformulovali tuto podstatnou větu:

Věta 20 (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).

Týden 8

Naším úkolem je dokázat Větu 20, tedy větu o úplnosti pro predikátový počet: pokud platí $T \models \varphi$, pak také platí $T \vdash \varphi$.

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 uvedená 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 $T \nvdash \varphi$ (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 $\models \varphi \to \psi$. Kdyby tedy obecně platilo, že $T, \varphi \vdash \psi$ implikuje $T \vdash \varphi \to \psi$, byl by náš důkazový systém nekorektní. Implikace $T, \varphi \vdash \psi \Rightarrow T \vdash \varphi \to \psi$ ovšem platí v případě, že φ je uzavřená.

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

> Má-li φ volné proměnné $x_1, x_2, \ldots, x_n$, pak $\overline{\varphi} = (\forall x_1)(\forall x_2)\ldots(\forall x_n)\varphi$; pokud je $n = 0$ (tedy φ je uzavřená), pak $\overline{\varphi} = \varphi$. 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 $\overline{\varphi}$ prostě označuje jeden z nich.
>
> Poznamenejme ještě, že někdy se také používá *existenční uzávěr* $(\exists x_1)(\exists x_2)\ldots(\exists x_n)\varphi$; výše definovaný uzávěr $\overline{\varphi}$ je také nazýván *univerzálním uzávěrem.*

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

Cvičení 46 *Dokažte následující větu.*
Věta o uzávěru.
Pro každou teorii T a každou formuli φ (v jazyce teorie T) platí:

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

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

V naší předpokládané situaci $T \models \varphi$ a $T \not\vdash \varphi$ (kterou později přivedeme ke sporu) máme tedy také $T \models \overline{\varphi}$ a $T \not\vdash \overline{\varphi}$. Z předpokladu $T \not\vdash \overline{\varphi}$ ovšem plyne, že teorie $T \cup \{\neg\overline{\varphi}\}$ je bezesporná.

> Intuitivně je vidět, že pokud z T nelze dokázat $\overline{\varphi}$, pak $\overline{\varphi}$ nebude dokazatelná ani po přidání $\neg\overline{\varphi}$ k T; jinými slovy, $T \not\vdash \overline{\varphi}$ implikuje $T, \neg\overline{\varphi} \not\vdash \overline{\varphi}$ (což znamená, že z $T \cup \{\neg\overline{\varphi}\}$ nelze dokázat všechny formule, a tudíž $T \cup \{\neg\overline{\varphi}\}$ je bezesporná).
>
> Obecně totiž platí $\vdash (\neg\overline{\varphi} \to \overline{\varphi}) \to \overline{\varphi}$, podle jednoduché, ale velmi užitečné,
>
> *věty o dosazení do tautologie výrokového počtu*
>
> (což je Lemma 3.42 v [1]); formule $(\neg\overline{\varphi} \to \overline{\varphi}) \to \overline{\varphi}$ vznikne dosazením do tautologie $(\neg\mathrm{p} \to \mathrm{p}) \to \mathrm{p}$ 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 $T, \neg\overline{\varphi} \vdash \overline{\varphi}$, tak by podle věty o dedukci (viz Věta 3.44 v [1]) platilo i $T \vdash \neg\overline{\varphi} \to \overline{\varphi}$ (jelikož $\neg\overline{\varphi}$ nemá volné proměnné); pak ovšem díky $\vdash (\neg\overline{\varphi} \to \overline{\varphi}) \to \overline{\varphi}$ pomocí pravidla Modus Ponens vyvodíme $T \vdash \overline{\varphi}$ — což je spor s předpokladem $T \not\vdash \overline{\varphi}$. Lemma 3.56 v [1] ukazuje obecněji, že
>
> $T \vdash \varphi$ právě tehdy, když $T \cup \{\neg\overline{\varphi}\}$ je sporná.

Cvičení 47 *Promyslete si podrobněji zmíněné Lemma 3.42 a Větu 3.44 v [1] s důkazy. (Větu o dedukci v našem textu najdete jako Větu 23.)*

Předpokládejme teď, že ona bezesporná teorie $T \cup \{\neg\overline{\varphi}\}$ má nějaký model $\mathbf{M}$; v něm je tedy pravdivá každá formule z T a také formule $\neg\overline{\varphi}$. Struktura $\mathbf{M}$ je tedy také modelem teorie T a proto je v ní pravdivá také formule $\overline{\varphi}$ (díky našemu předpokladu $T \models \overline{\varphi}$). Není ovšem možné, aby v $\mathbf{M}$ byla pravdivá jak $\overline{\varphi}$ tak $\neg\overline{\varphi}$. Takže buď $T \cup \{\neg\overline{\varphi}\}$ nemá žádný model nebo případ $T \models \overline{\varphi}$, $T \not\vdash \overline{\varphi}$ (a tedy ani případ $T \models \varphi$, $T \not\vdash \varphi$) neexistuje. Následně ukážeme větu 21 (každá bezesporná teorie má model), z čehož vyplyne, že případ $T \models \varphi$, $T \not\vdash \varphi$ neexistuje, a tedy věta 20 (o úplnosti) skutečně platí.

Věta 21 *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 $T \vdash \neg(\varphi \to \varphi)$ pro nějakou formuli φ. (Připomeňme si, že $\neg(\varphi \to \varphi)$ je vlastně "překladem" formule $\varphi \wedge \neg\varphi$.) Ta druhá definice spornosti je opravdu ekvivalentní té první: pro libovolné formule φ, ψ totiž máme $\vdash \neg(\varphi \to \varphi) \to \psi$ (jelikož $\neg(\varphi \to \varphi) \to \psi$ vznikne dosazením do tautologie $\neg(\mathrm{p} \to \mathrm{p}) \to \mathrm{q}$ výrokového počtu); z toho plyne, že $T \vdash \neg(\varphi \to \varphi)$ 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 $t_1, t_2, \ldots, t_n$ jsou prvky $U^{\mathbf{M}_T}$, pak také řetězec $f(t_1, t_2, \ldots, t_n)$ 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 neprázdnosti, 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]. My se k této problematice ještě vrátíme později.

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 $(t_1, t_2, \ldots, t_n)$ prvků univerza $U^{\mathbf{M}_T}$, tedy pro n-tici uzavřených termů, musíme určit prvek univerza $U^{\mathbf{M}_T}$, který je hodnotou $f^{\mathbf{M}_T}(t_1, t_2, \ldots, t_n)$. Jelikož řetězec $f(t_1, t_2, \ldots, t_n)$ je také uzavřený term (tedy prvek $U^{\mathbf{M}_T}$), přirozeně se nabízí následující interpretace:

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

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 $\{1; f(1,1); f(1, f(1,1)); f(f(1,1),1); f(f(1,1), f(1,1)); f(1, f(1, f(1,1))); \ldots\}$, 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 $\{1; (1\cdot1); (1\cdot(1\cdot1)); ((1\cdot1)\cdot1); ((1\cdot1)\cdot(1\cdot1)); (1\cdot(1\cdot(1\cdot1))); \ldots\}$. 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 $(t_1, t_2, \ldots, t_n)$ uzavřených termů do množiny $P^{\mathbf{M}_T}$ pro n-ární predikátový symbol P (tedy, kdy prohlásíme $P^{\mathbf{M}_T}(t_1, t_2, \ldots, t_n)$ 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 schématům 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 $(t_1, t_2, \ldots, t_n)$ máme

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

Když tedy platí $T \vdash P(t_1, t_2, \ldots, t_n)$, pak platí $P^{\mathbf{M}_T}(t_1, t_2, \ldots, t_n)$; pokud $T \nvdash P(t_1, t_2, \ldots, t_n)$, platí $\neg P^{\mathbf{M}_T}(t_1, t_2, \ldots, t_n)$. Zde připouštíme možnost, že z T nelze dokázat ani $P(t_1, t_2, \ldots, t_n)$ ani $\neg P(t_1, t_2, \ldots, t_n)$. 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 $P(t_1, \ldots, t_n)$, protože v tom případě jsou $t_1, \ldots, t_n$ uzavřené termy a z $T \vdash P(t_1, \ldots, t_n)$ plyne $\|P(t_1, \ldots, t_n)\|_{\mathbf{M}_T} = 1$ 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 $T \vdash \psi$, 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

$$T \vdash \varphi \text{ právě tehdy, když } \|\varphi\|_{\mathbf{M}_T} = 1. \tag{5}$$

To ovšem pro naši teorii T nemusí platit. Můžeme totiž mít $T \nvdash P(t_1, \ldots, t_n)$ a zároveň $T \nvdash \neg P(t_1, \ldots, t_n)$; pak pro $\varphi = \neg P(t_1, \ldots, t_n)$ máme $\|\varphi\|_{\mathbf{M}_T} = 1$ ale $T \nvdash \varphi$. Jistě nás napadne, že v takovém případě lze do T přidat $P(t_1, \ldots, t_n)$ (nebo $\neg P(t_1, \ldots, t_n)$); 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 (5) pro uzavřené formule φ strukturální indukcí.

1. Případ, kdy φ je atomická.
   Podle definice $\mathbf{M}_T$ máme $T \vdash P(t_1, \ldots, t_n)$ právě tehdy, když $\|P(t_1, \ldots, t_n)\|_{\mathbf{M}_T} = 1$ (pro uzavřené termy $t_1, \ldots, t_n$).

2. Případ $\varphi = \neg\psi$.

   - (Pod)případ $T \vdash \psi$ jsme už vyřešili dříve.
   - Když $T \nvdash \psi$, tak z indukčního předpokladu (5) 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 $T \nvdash \psi$ a z úplnosti T plyne $T \vdash \neg\psi$, tj. $T \vdash \varphi$.

3. Případ $\varphi = (\psi_1 \to \psi_2)$.
   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 $\|\varphi\|_{\mathbf{M}_T} = 1$.

   Podívejme se alespoň na případ, kdy $\|\psi_1\|_{\mathbf{M}_T} = 0$ a $\|\psi_2\|_{\mathbf{M}_T} = 1$; tedy $\|\varphi\|_{\mathbf{M}_T} = 1$. Podle indukčního předpokladu platí $T \nvdash \psi_1$ a $T \vdash \psi_2$; díky úplnosti teorie T máme $T \vdash \neg\psi_1$. Jelikož formule $\neg\psi_1 \to (\psi_2 \to (\psi_1 \to \psi_2))$ vznikne dosazením do tautologie výrokové logiky, víme, že platí $\vdash \neg\psi_1 \to (\psi_2 \to (\psi_1 \to \psi_2))$. Dvojnásobným použitím Modus Ponens tedy odvodíme, že $T \vdash (\psi_1 \to \psi_2)$, neboli $T \vdash \varphi$.

4. Případ $\varphi = (\forall x)\psi$.
   Vztah (5) 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

   $$T \vdash (\forall x)\psi \text{ právě tehdy, když } \|(\forall x)\psi\|_{\mathbf{M}_T} = 1. \tag{6}$$

   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)případ, kdy pro nějaký uzavřený term t máme $T \nvdash \psi(x/t)$.
  Podle indukčního předpokladu zde máme $\|\psi(x/t)\|_{\mathbf{M}_T} = 0$, z čehož také plyne $\|(\forall x)\psi\|_{\mathbf{M}_T} = 0$. Protože $T \nvdash \psi(x/t)$, máme také $T \nvdash (\forall x)\psi$ (neboť z $T \vdash (\forall x)\psi$ by díky axiomu konkretizace $(\forall x)\psi \to \psi(x/t)$ plynulo $T \vdash \psi(x/t)$).
  Máme zde tedy $T \nvdash (\forall x)\psi$ a $\|(\forall x)\psi\|_{\mathbf{M}_T} = 0$, což odpovídá dokazovanému vztahu (6).
- (Pod)případ, 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 (6) 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.

> Připomeňme si jeden z běžných postupů, když chceme prokázat, že všechny prvky jisté množiny A mají jistou vlastnost φ, tedy chceme prokázat $(\forall x \in A)\varphi(x)$. Zvolíme si nový symbol, např. c, a prohlásíme, že označuje libovolně zvolený prvek množiny A. Když se nám pak podaří prokázat $\varphi(c)$, tedy, že c má vlastnost φ, tak vyvodíme, že platí $(\forall x \in A)\varphi(x)$. Z toho lze vytušit, že když k teorii T přidáme novou konstantu c a axiom $\varphi(x/c) \to (\forall x)\varphi(x)$ (neboli $(\exists x)\neg\varphi(x) \to \neg\varphi(x/c)$), tak vznikne konzervativní rozšíření teorie T.

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 $T \vdash (\exists x)\varphi \to \varphi(x/c)$.

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 $T \nvdash (\forall x)\psi$; 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 $T \vdash (\exists x)\neg\psi \to \neg\psi(x/c)$. Pak ovšem $T \vdash \neg\psi(x/c)$, a tedy $T \nvdash \psi(x/c)$ (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. □

Týden 9

Vybraná tvrzení (na jejichž užitečnost jsme narazili při důkazu věty o úplnosti).
Připomeňme si, co je (univerzální) uzávěr $\overline{\varphi}$ formule φ, a následující větu:

Věta 22 (Věta o uzávěru.)
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 $(\forall x)\varphi \to \varphi$ je instance axiomu konkretizace (je totiž $\varphi = \varphi(x/x)$), je fakt, že z $T \vdash \overline{\varphi}$ plyne $T \vdash \varphi$, také zřejmý. □

Věta 23 (Věta o dedukci.)
Pro každou teorii T, každou uzavřenou formuli φ (tedy φ bez volných proměnných) a každou formuli ψ platí:

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

Cvičení 48 *Připomeňte si důkaz věty pro výrokovou logiku a ten rozšiřte pro predikátovou logiku. Připomeňte si také, proč je zde uzavřenost φ důležitá.*

> *Řešení cvičení.* Nejprve si všimněme, že z $T \vdash \varphi \to \psi$ triviálně plyne $T, \varphi \vdash \varphi \to \psi$; protože také triviálně platí $T, \varphi \vdash \varphi$, díky pravidlu Modus Ponens vyvodíme $T, \varphi \vdash \psi$.
> Teď předpokládejme $T, \varphi \vdash \psi$. Existuje tedy příslušný důkaz, tedy posloupnost formulí $\varphi_1, \varphi_2, \ldots, \varphi_k$, kde $\varphi_k = \psi$ a φ_i, pro každé $i \in \{1, 2, \ldots, k\}$, je buď axiom (tedy instance jednoho z pěti axiomových schémat hilbertovského kalkulu), nebo prvek množiny $T \cup \{\varphi\}$, nebo plyne z předchozích formulí v důkazu podle pravidla Modus Ponens či podle pravidla Generalizace. Ukažme, že platí $T \vdash \varphi \to \varphi_i$, pro $i = 1, 2, \ldots, k$. Pokud φ_i je axiom, tak z platnosti $\vdash \varphi_i$ a $\vdash \varphi_i \to (\varphi \to \varphi_i)$ (instance axiomového schématu 1) vyvodíme $\vdash \varphi \to \varphi_i$ (podle Modus Ponens), tedy také $T \vdash \varphi \to \varphi_i$. Pokud φ_i je prvek T, tak podobně z $T \vdash \varphi_i$ a $\vdash \varphi_i \to (\varphi \to \varphi_i)$ vyvodíme $T \vdash \varphi \to \varphi_i$. Pokud $\varphi_i = \varphi$, tak využijeme, že platí $\vdash \varphi \to \varphi$ (např. podle věty o dosazení do tautologie výrokového počtu); opět tedy máme $T \vdash \varphi \to \varphi_i$. Pokud φ_i plyne z φ_j a $\varphi_\ell = (\varphi_j \to \varphi_i)$ (pro $j, \ell < i$) podle Modus Ponens, využijeme, že máme $T \vdash \varphi \to \varphi_j$ a $T \vdash \varphi \to (\varphi_j \to \varphi_i)$ podle indukčního předpokladu: protože $\vdash (\varphi \to (\varphi_j \to \varphi_i)) \to ((\varphi \to \varphi_j) \to (\varphi \to \varphi_i))$ (axiomové schéma 2), vyvodíme $T \vdash \varphi \to \varphi_i$ dvojnásobným použitím Modus Ponens. Pokud φ_i plyne z φ_j ($j < i$) podle pravidla Generalizace, tedy $\varphi_i = (\forall x)\varphi_j$ (pro nějakou proměnnou x), využijeme indukční předpoklad $T \vdash \varphi \to \varphi_j$, z něhož také plyne $T \vdash (\forall x)(\varphi \to \varphi_j)$. Připomeneme si, že $(\forall x)(\varphi \to \varphi_j) \to (\varphi \to (\forall x)\varphi_j)$ je instancí axiomového schématu 5 (distribuce kvantifikátoru), pokud ovšem x není volná ve φ. Tady vidíme, proč v podmínkách věty o dedukci uvádíme předpoklad, že φ je uzavřená; v tom případě tedy skutečně vyvodíme $T \vdash \varphi \to (\forall x)\varphi_j$, tj. $T \vdash \varphi \to \varphi_i$. Jelikož $\varphi_k = \psi$, ukázali jsme tak, že $T \vdash \varphi \to \psi$.

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

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 $T \nvdash \varphi$, tak $T \cup \{\neg\varphi\}$ je bezesporná. Jestliže tedy máme pro uzavřenou φ jak $T \nvdash \varphi$ tak $T \nvdash \neg\varphi$, 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 $\varphi_0, \varphi_1, \varphi_2, \ldots$ a definovat teorie $T_0, T_1, T_2, \ldots$ následovně:

- $T_0 = T$ (tedy T_0 je výchozí bezesporná teorie);
- Pokud $T_i \nvdash \varphi_i$ a $T_i \nvdash \neg\varphi_i$, pak položíme $T_{i+1} = T_i \cup \{\varphi_i\}$; jinak $T_{i+1} = T_i$.

Je zřejmé, že pro každé $i = 0, 1, 2, \ldots$ je T_i bezesporná. Pak je ovšem bezesporná i $T' = T_0 \cup T_1 \cup T_2 \cup \cdots$. (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 transfinitní 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 $\bigcup_{\kappa<\lambda} T_\kappa$.) □

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

Věta 25 (Věta o konstantách.)
Přidáme-li k jazyku teorie T nové konstanty $c_1, c_2, \ldots, c_n$, dostaneme rozšíření teorie T, které můžeme označit $T_{c_1,c_2,\ldots,c_n}$. Pro každou formuli φ jazyka teorie T a libovolné proměnné $x_1, x_2, \ldots, x_n$ pak platí

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

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

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

- Nechť $T \vdash \varphi$; vezměme nějaký důkaz $\varphi_1, \varphi_2, \ldots, \varphi_k$ formule φ z T, tedy mj. platí $\varphi_k = \varphi$. Posloupnost $\varphi_1, \varphi_2, \ldots, \varphi_k$ je tedy i důkazem v T_{c_1}. Přidáme formuli $\varphi_{k+1} = (\forall x_1)\varphi$ (použili jsme pravidlo generalizace na φ_k), $\varphi_{k+2} = (\forall x_1)\varphi \to \varphi(x_1/c_1)$ (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 $T_{c_1} \vdash \varphi(x_1/c_1)$.

- Nechť $T_{c_1} \vdash \varphi(x_1/c_1)$ a posloupnost $\psi_1, \psi_2, \ldots, \psi_m$ 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 $\psi_1, \psi_2, \ldots, \psi_m$).

  Z toho plyne $T \vdash \varphi(x_1/y)$, a tedy také $T \vdash (\forall y)\varphi(x_1/y)$. Jelikož $(\forall y)\varphi(x_1/y) \to (\varphi(x_1/y))(y/x_1)$ 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. □

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

Cvičení 50 *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 26 (Věta o variantách.)
Nechť y není volná v ψ a je substituovatelná za x v ψ. Pokud φ' vznikne z φ nahrazením (jednoho výskytu) 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 $\vdash (\forall x)\psi \to (\forall y)\psi(x/y)$:
Díky axiomu substituce máme $\vdash (\forall x)\psi \to \psi(x/y)$. Použitím pravidla generalizace pak odvodíme $\vdash (\forall y)\left((\forall x)\psi \to \psi(x/y)\right)$. Axiomem distribuce a pravidlem modus ponens odvodíme $\vdash (\forall x)\psi \to (\forall y)\psi(x/y)$.

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

> Máme $\vdash (\forall y)\psi(x/y) \to \psi$ (jelikož $\psi(x/y)(y/x) = \psi$) a $\vdash (\forall x)\left((\forall y)\psi(x/y) \to \psi\right)$, a tedy $\vdash (\forall y)\psi(x/y) \to (\forall x)\psi$.

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

Ovšem obecně platí $\vdash \varphi_1 \to (\varphi_2 \to (\varphi_1 \wedge \varphi_2))$, neboť se jedná o dosazení do tautologie výrokového počtu ve formě $\mathrm{p} \to (\mathrm{q} \to (\mathrm{p} \wedge \mathrm{q}))$. □

Cvičení 51 *Promyslete si, jak dokončit důkaz předchozí věty.*

Nápověda. Postupujeme strukturální indukcí.

Když podformule $(\forall x)\psi$ je přímo formulí φ, je φ' rovno $(\forall y)\psi(x/y)$ a demonstraci toho, že platí $\vdash \varphi \leftrightarrow \varphi'$ jsme již provedli.

Když $\varphi = \neg\bar{\varphi}$, tak $(\forall x)\psi$ je podformulí formule $\bar{\varphi}$ a podle indukčního předpokladu víme, že $\vdash \bar{\varphi} \leftrightarrow \bar{\varphi}'$, kde $\bar{\varphi}'$ vznikne z $\bar{\varphi}$ nahrazením podformule $(\forall x)\psi$ formulí $(\forall y)\psi(x/y)$. Využitím věty o dosazení do tautologie výrokového počtu snadno odvodíme, že platí $\vdash \neg\bar{\varphi} \leftrightarrow \neg\bar{\varphi}'$ (neboť $(\mathrm{p} \leftrightarrow \mathrm{q}) \rightarrow (\neg\mathrm{p} \leftrightarrow \neg\mathrm{q})$ je tautologie), a tedy $\vdash \varphi \leftrightarrow \varphi'$.

Postup pro případ $\varphi = \varphi_1 \rightarrow \varphi_2$ je analogický. (Proveďte jej!)

Když $\varphi = (\forall z)\xi$ (a $(\forall z)\xi \neq (\forall x)\psi$), tak $\varphi' = (\forall z)\xi'$, kde ξ' vznikne z ξ nahrazením podformule $(\forall x)\psi$ formulí $(\forall y)\psi(x/y)$. Podle indukčního předpokladu máme $\vdash \xi \leftrightarrow \xi'$, tedy $\vdash \xi \rightarrow \xi'$ a $\vdash \xi' \rightarrow \xi$. Z faktu $\vdash \xi \rightarrow \xi'$ díky pravidlu generalizace odvodíme, že $\vdash (\forall z)(\xi \rightarrow \xi')$. Nyní si stačí uvědomit, že platí $\vdash ((\forall z)(\xi \rightarrow \xi')) \rightarrow ((\forall z)\xi \rightarrow (\forall z)\xi')$, což ukážeme v dalším cvičení. (Zde to předpokládejte a důkaz dokončete.)

Cvičení (neočíslováno). Ukažte, že platí $\vdash ((\forall x)(\varphi \rightarrow \psi)) \rightarrow ((\forall x)\varphi \rightarrow (\forall x)\psi)$.

Nápověda. Víme, že platí $(\forall x)(\varphi \rightarrow \psi) \vdash \varphi \rightarrow \psi$ a $(\forall x)\varphi \vdash \varphi$ (proč?), tedy použitím pravidla modus ponens odvodíme, že $(\forall x)(\varphi \rightarrow \psi), (\forall x)\varphi \vdash \psi$; pravidlem generalizace tedy dostaneme $(\forall x)(\varphi \rightarrow \psi), (\forall x)\varphi \vdash (\forall x)\psi$. Vypadá to, že teď stačí dvakrát použít větu o dedukci a jsme hotovi. To ale lze za předpokladu, že formule $(\forall x)\varphi$ a $(\forall x)(\varphi \rightarrow \psi)$ jsou uzavřené. Pokud nejsou, tak prostě jejich volné proměnné nahradíme novými konstantami; takto upravené formule jsou uzavřené a větu o dedukci lze pro ně použít. Kýžený fakt pro původní formule pak plyne z věty o konstantách. (Promyslete si!)

Cvičení (neočíslováno). Ukažte, že věta o variantách platí i pro existenční kvantifikátor (místo univerzálního).

Nápověda. Stačí ukázat, že když y není volná v ψ a je substituovatelná za x v ψ, tak platí $\vdash (\exists x)\psi \leftrightarrow (\exists y)\psi(x/y)$, neboli $\vdash \neg(\forall x)\neg\psi \leftrightarrow \neg(\forall y)\neg\psi(x/y)$. Víme již, že platí $\vdash (\forall x)\neg\psi \leftrightarrow (\forall y)\neg\psi(x/y)$, takže kýžené odvodíme dosazením do tautologie výrokového počtu (konkrétně do již dříve použité $(\mathrm{p} \leftrightarrow \mathrm{q}) \rightarrow (\neg\mathrm{p} \leftrightarrow \neg\mathrm{q})$).

Všimněme si, že postupem ve výše uvedeném důkazu také snadno odvodíme i tuto větu (kterou lze přirozeně rozšířit na nahrazení více výskytů jejich "ekvivalenty"):

Věta 27 (Věta o ekvivalenci.) *Když φ' vznikne z φ nahrazením (jednoho výskytu) podformule ψ formulí ψ', tak platí $\psi \leftrightarrow \psi' \vdash \varphi \leftrightarrow \varphi'$.*

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 platí $T \vdash (\exists x)\varphi \rightarrow \varphi(x/c)$. Ukážeme teď větu, která se nám hodila pro důkaz věty o úplnosti pro predikátovou logiku; jde o větu 29, před niž předřadíme (pomocnou) větu 28.

Věta 28 (Věta o henkinovské konstantě.)
Je-li $\varphi(x)$ formule jazyka J_T teorie T a je-li $S = T \cup \{(\exists x)\varphi \rightarrow \varphi(x/c_\varphi)\}$, kde c_φ je konstanta, o niž jsme jazyk J_T rozšířili, pak teorie S je konzervativním rozšířením teorie T.

Důkaz. Uvažujme T, φ, c_φ, S tak, jak je uvedeno v předpokladu věty; místo c_φ pišme c. Podle věty o konstantách je teorie T_c (která má oproti T jen jazyk rozšířený o c) konzervativním rozšířením teorie T. Máme ovšem ukázat, že $S = T \cup \{(\exists x)\varphi \to \varphi(x/c)\}$ je konzervativním rozšířením T.

Nechť tedy platí $S \vdash \psi$ pro nějakou (pevně zvolenou) formuli ψ v jazyce teorie T; máme ukázat, že platí i $T \vdash \psi$. Podle věty o dedukci máme

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

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

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

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

$$\begin{gathered} T \vdash (\forall y)\big(((\exists x)\varphi \to \varphi(x/y)) \to \psi\big), \\ T \vdash \big((\exists y)((\exists x)\varphi \to \varphi(x/y))\big) \to \psi, \\ T \vdash \big((\exists x)\varphi \to (\exists y)\varphi(x/y)\big) \to \psi. \end{gathered}$$

Podle *věty o variantách* (pro existenční kvantifikátor) máme $\vdash (\exists x)(\varphi) \to (\exists y)\varphi(x/y)$, neboť y se ve φ nevyskytuje. Užitím Modus Ponens dostáváme $T \vdash \psi$. Takže S je skutečně konzervativním rozšířením teorie T. □

Cvičení (neočíslováno). Doplňte důkaz předchozí věty, tedy ukažte, že

1. $\vdash (\forall x)(\varphi \to \psi) \to ((\exists x)\varphi \to \psi)$, když x není volná v ψ;
2. $\vdash (\exists x)(\varphi \to \psi) \to (\varphi \to (\exists x)\psi)$, když x není volná ve φ.

Nápověda.
1. Díky větě o okvivalenci stačí ukázat, že $\vdash (\forall x)(\neg\psi \to \neg\varphi) \to (\neg\psi \to \neg(\exists x)\varphi)$ (proč?), tedy že $\vdash (\forall x)(\neg\psi \to \neg\varphi) \to (\neg\psi \to (\forall x)\neg\varphi)$; to je ovšem axiom distribuce.
2. Jelikož $\vdash (\forall x)\neg\psi \to \neg\psi$, máme i $\vdash \psi \to (\exists x)\psi$. Dosazením do tautologie výrokového počtu $(p_2 \to p_3) \to ((p_1 \to p_2) \to (p_1 \to p_3))$ odvodíme, že platí
$\vdash (\psi \to (\exists x)\psi) \to ((\varphi \to \psi) \to (\varphi \to (\exists x)\psi))$, a tedy $\vdash (\varphi \to \psi) \to (\varphi \to (\exists x)\psi)$ (užitím modus ponens). Generalizací dostaneme $\vdash (\forall x)\big((\varphi \to \psi) \to (\varphi \to (\exists x)\psi)\big)$, a pak aplikací faktu 1 a pravidla modus ponens dostáváme $\vdash (\exists x)(\varphi \to \psi) \to (\varphi \to (\exists x)\psi)$.

Věta 29 (Věta o henkinovském rozšíření.)
Ke každé teorii existuje její konzervativní rozšíření, které je henkinovskou teorií.

Důkaz. Uvažujme (výchozí) teorii T, označenou také T_0. Ukázali jsme (v předchozí větě), 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 $(\exists x)\varphi \to \varphi(x/c_\varphi)$. Tím vznikne teorie T_1, která je konzervativním rozšířením T_0, jak lze snadno ověřit (uvažte případ $T_1 \vdash \psi$ pro formuli ψ v jazyce J_{T_0} a ukažte, proč platí i $T_0 \vdash \psi$).

Ovšem T_1 nemusí být henkinovská, její jazyk byl oproti T_0 rozšířen a může tak obsahovat nové formule s jednou volnou proměnnou, v jazyce J_{T_1}, které příslušné henkinovské konstanty nemají. Proto uvažujme stejný proces rozšíření T_1, čímž dostaneme T_2, atd. Nakonec pro teorii $T' = T_0 \cup T_1 \cup T_2 \cup \cdots$ snadno ověříme, že je henkinovská a přitom je konzervativním rozšířením teorie T. □

Týden 10

Začneme ještě procvičením práce s kvantifikátory.

Cvičení 52 *Ukažte, že platí*

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

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

Jsou logicky platné i obrácené implikace?

Cvičení 53 *Ukažte, že*

1. $(\forall x)(\varphi \to \psi) \to ((\forall x)\varphi \to (\forall x)\psi)$ *je ekvivalentní s* $((\forall x)(\varphi \to \psi) \wedge (\forall x)\varphi) \to (\forall x)\psi$*;*
2. $(\forall x)(\varphi \to \psi) \to ((\exists x)\varphi \to (\exists x)\psi)$ *je ekvivalentní s* $((\forall x)(\varphi \to \psi) \wedge (\exists x)\varphi) \to (\exists x)\psi$.

(Nápověda. Všimněte si, že $(\mathrm{p} \to (\mathrm{q} \to \mathrm{r})) \leftrightarrow ((\mathrm{p} \wedge \mathrm{q}) \to \mathrm{r})$ *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 schématům se (alespoň) dodají tzv.

axiomy rovnosti:

1. $x = x$;
2. $(x_1 = y_1 \wedge x_2 = y_2 \wedge \cdots \wedge x_n = y_n) \to f(x_1, x_2, \ldots, x_n) = f(y_1, y_2, \ldots, y_n)$, pro každý n-ární funkční symbol f v příslušném jazyku;
3. $(x_1 = y_1 \wedge x_2 = y_2 \wedge \cdots \wedge x_n = y_n) \to (P(x_1, x_2, \ldots, x_n) \to P(y_1, y_2, \ldots, y_n))$, 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 také očekávat formule typu "$x = y \to y = x$" (symetrie relace rovnosti) a "$(x = y \wedge y = z) \to x = z$" (tranzitivita). Uvědomili jsme si ale, že ty se dají odvodit (v našem hilbertovském predikátovém kalkulu) díky axiomům rovnosti 1 a 3.

Cvičení 54 *Ukažte, že v hilbertovském kalkulu s axiomy rovnosti platí* $\vdash x = y \to y = x$.

> *Řešení.* Jednou z instancí axiomu rovnosti 3 je $(x = y \wedge x = x) \to (P(x, x) \to P(y, x))$ pro jakýkoli binární predikátový symbol P v příslušném jazyku. Když za P vezmeme predikát "=", dostáváme instanci $(x = y \wedge x = x) \to (x = x \to y = x)$. Využitím toho, že předchozí formule vznikne dosazením do formule $(p \wedge q) \to (q \to r)$ výrokové logiky a že $((p \wedge q) \to (q \to r)) \to (q \to (p \to r))$ je tautologie výrokového počtu, odvodíme, že platí $\vdash x = x \to (x = y \to y = x)$. Protože $x = x$ je axiom, odvodíme $\vdash x = y \to y = x$.

Cvičení 55 *Zkuste podobně ukázat, že platí* $\vdash (x = y \wedge y = z) \to x = z$.

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) $f : U^n \longrightarrow U$, jestliže z $x_1\rho y_1, x_2\rho y_2, \ldots, x_n\rho y_n$ plyne $f(x_1, x_2, \ldots, x_n)\, \rho\, f(y_1, y_2, \ldots, y_n)$. Relaci ρ chápeme jako *kongruenci vzhledem k predikátu* $P \subseteq U^n$, jestliže z $x_1\rho y_1, x_2\rho y_2, \ldots, x_n\rho y_n$ plyne, že $(x_1, \ldots, x_n) \in P$ právě tehdy, když $(y_1, \ldots, y_n) \in P$.

Z věty 21 (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 $(U', \mathcal{F}', \mathcal{R}')$ sestrojenou 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

$$f'([a_1]_\equiv, \ldots, [a_n]_\equiv) = [f(a_1, \ldots, a_n)]_\equiv;$$

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

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

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 mod 5) a (b mod 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 30 (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 $T' \models \varphi$. □

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

Tvrzení 31
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 30(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. □

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 $(Q_1 x_1)(Q_2 x_2)\cdots(Q_n x_n)\psi$, 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 (formuli ψ se říká *otevřené jádro*, nebo též *matrice* či *matice*, dané formule φ v prenexní formě, přičemž sekvenci $(Q_1 x_1)(Q_2 x_2)\cdots(Q_n x_n)$ se říká *prefix*).

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].)

Poznámka. Převod formule do prenexní formy žádá mj. jeden příklad z druhé zápočtové písemky. Např.: k formuli

$$(\forall x)\big(\neg(\forall y)\neg R(x,y,z) \to \neg(\forall z)R(y,x,z)\big)$$

sestrojte ekvivalentní formuli v prenexní formě. Převedení do ekvivalentního tvaru

$$(\forall x)\big((\exists y)R(x,y,z) \to (\exists z)\neg R(y,x,z)\big)$$

je jasné. Pokud ale teď chceme "vytáhnout" $(\exists y)$ z předpokladu implikace uvnitř závorky před závorku, musíme nejen otočit kvantifikátor ($\exists$ změnit na $\forall$), ale dát také pozor na to, že v závěru implikace, tedy ve formuli $(\exists z)\neg R(y,x,z)$ se y vyskytuje volně! Abychom zamezili svázání volné proměnné, nemůžeme ovšem změnit onen volný výskyt y na (např.) y' – výsledná formule by nebyla ekvivalentní původní formuli! (Je to jasné?) Použijeme tedy variantu (pod)formule $(\exists y)R(x,y,z)$, konkrétně např. $(\exists y')R(x,y',z)$ (použitím "čerstvé" proměnné y', která se dosud v celé formuli nevyskytuje). Ve formuli

$$(\forall x)\big((\exists y')R(x,y',z) \to (\exists z)\neg R(y,x,z)\big)$$

už příslušným vytažením před závorku žádný volný výskyt nesvazujeme, takže formule

$$(\forall x)(\forall y')\big(R(x,y',z) \to (\exists z)\neg R(y,x,z)\big)$$

je opravdu ekvivalentní výchozí formuli.

Při vytažení $(\exists z)$ ze závěru implikace uvnitř závorky před závorku se kvantifikátor nemění, ale opět to nelze přímo udělat kvůli svázání volného výskytu proměnné z v předpokladu implikace. Proto závěr $(\exists z)\neg R(y,x,z)$ nahradíme ekvivalentní variantou $(\exists z')\neg R(y,x,z')$ a pak provedeme "vytažení"; dostáváme tedy formuli

$$(\forall x)(\forall y')(\exists z')\big(R(x,y',z) \to \neg R(y,x,z')\big),$$

která je ekvivalentní výchozí formuli a je už v prenexní formě.

Cvičení 56 *Vyzkoušejte si převod formulí do prenexního tvaru na dalších příkladech, ať jste si jisti, že rozumíte všem nuancím.*

Týden 11

Seznámili jsme se s následujícími důležitými fakty z logiky. (Jde nám teď o pochopení výsledků, byť jejich důkazy nejsou součástí našeho kurzu.)

Nejprve jsme si připomněli základní pojmy teorie vyčíslitelnosti, speciálně pojem *rozhodnutelné množiny* (neboli rekurzivní množiny) a *částečně rozhodnutelné množiny* (neboli rekurzivně spočetné množiny), a obecně algoritmicky (*částečně*) *rozhodnutelného problému*; přitom jsme připomněli i pojem *Turingův stroj*.

Otázky rozhodnutelnosti množin $\mathbf{Taut}_J$, $\mathbf{Sat}_J$, $\mathbf{Prov}_J$, $\mathbf{Proofs}_J$, ...

Položili jsme si otázku, zda pro každý konkrétní jazyk $J = (\mathcal{F}, \mathcal{R}, ar)$, řekněme s konečnými množinami $\mathcal{F}$ a $\mathcal{R}$, je množina tautologií (neboli logicky platných formulí) v jazyce J, tedy množina

$$\textsc{Taut}_J = \{\varphi \mid \varphi \text{ je formule v jazyce } J, \text{ pro niž platí } \models \varphi\},$$

rozhodnutelná. Jelikož díky větě o úplnosti máme $\textsc{Taut}_J = \textsc{Prov}_J$, kde

$$\textsc{Prov}_J = \{\varphi \mid \varphi \text{ je formule v jazyce } J, \text{ pro niž platí } \vdash \varphi\}$$

(Prov ze slova "provable"), tak jsme odvodili, že

množina $\textsc{Taut}_J$ je částečně rozhodnutelná:

jelikož množina důkazů $\textsc{Proofs}_J$ (tj. množina posloupností $\varphi_1, \varphi_2, \ldots, \varphi_k$ splňujících příslušné podmínky) je očividně rozhodnutelná, tak algoritmu, který má mít konečný výpočet pro zadanou formuli φ právě tehdy, když φ je tautologie, stačí systematicky postupně generovat všechny důkazy a zastavit se, pokud našel důkaz pro φ.

Zda je $\textsc{Taut}_J$ rozhodnutelná (nejen částečně rozhodnutelná), závisí na konkrétním $J = (\mathcal{F}, \mathcal{R}, ar)$. Např. když $\mathcal{F}$ je prázdná množina a $\mathcal{R}$ obsahuje pouze predikát rovnosti "=", tak $\textsc{Taut}_J$ je rozhodnutelná.

> Připomeňme, že φ je tautologie právě tehdy, když $\neg\varphi$ je nesplnitelná (tj. nemá model). Dá se snadno odvodit, že formule $\varphi(x_1, x_2, \ldots, x_m)$ v jazyce s pouhým predikátem rovnosti má model právě tehdy, když má model, jehož univerzum má maximálně m prvků. Z toho snadno plyne rozhodnutelnost množiny $\textsc{Taut}_J$ pro zmíněný "chudý" jazyk J.

Připomněli jsem si nerozhodnutelný problém zastavení:

> Halting Problem (HP)
> Instance: Turingův stroj M a jeho vstup w.
> Otázka: Je výpočet M na w konečný?

a intuitivně jsme nahlédli, že pro vhodný (malý) jazyk J lze navrhnout formuli $\varphi_{M,w}$ v jazyce J, která má model právě tehdy, když M, w je pozitivní instancí problému HP. V tom případě tedy máme algoritmickou redukci problému HP na problém příslušnosti k množině

$$\textsc{Sat}_J = \{\varphi \mid \varphi \text{ je formule v jazyce } J, \text{ která má model}\}$$

(SAT ze slova "satisfiable"), z čehož plyne, že SAT_J *je nerozhodnutelná.* Jelikož pro každou formuli φ v jazyce J máme $\varphi \in \text{TAUT}_J \iff \neg\varphi \in \text{SAT}_J$, vyvodíme také, že

TAUT_J je nerozhodnutelná.

> Dokonce stačí použít jediný binární predikátový symbol kromě predikátového symbolu rovnosti a výše uvedená redukce z HP se dá realizovat. Demonstrace tohoto faktu vyžaduje ovšem ještě další technickou práci.

Diskutovali jsme i relativizace výše uvedených množin vzhledem k dané teorii T, tedy množinu formulí "pravdivých v T" (tj. sémantických důsledků množiny T)

$$\text{CONSEQ}(T) = \{\varphi \mid T \models \varphi\},$$

která je podle věty o úplnosti (predikátového počtu) rovna množině teorémů teorie T

$$\text{THM}(T) = \{\varphi \mid T \vdash \varphi\}.$$

Uvědomili jsme si, že zde má smysl diskutovat otázky rozhodnutelnosti jen za předpokladu, že samotná množina T je rozhodnutelná (což implikuje, že $\text{THM}(T)$ je částečně rozhodnutelná).

Otázky rozhodnutelnosti množin $Th(\mathbb{N}, \mathbf{Plus})$ a $Th(\mathbb{N}, \mathbf{Plus}, \mathbf{Mult})$

Uvažme konkrétní strukturu $(\mathbb{N}, \text{PLUS})$, s univerzem $\mathbb{N} = \{0, 1, 2, \dots\}$ a ternární relací PLUS, kde $\text{PLUS}(x, y, z)$ platí právě pro trojice čísel x, y, z splňující podmínku $x + y = z$.

Množinu $Th(\mathbb{N}, \text{PLUS})$, *teorii struktury* $(\mathbb{N}, \text{PLUS})$, definujeme jako množinu těch uzavřených formulí jazyka s jediným predikátovým symbolem PLUS (s aritou 3), které jsou v uvedené struktuře pravdivé. Všimněme si, že tato teorie je bezesporná (má model) a úplná (pro každou uzavřenou formuli φ je buď φ nebo $\neg\varphi$ dokazatelná, dokonce přímo prvkem oné teorie).

Cvičení 57 *Ač zde uvažujeme jen jazyk s jediným predikátovým symbolem, konkrétně s ternárním symbolem* PLUS*, ekvivalentně jsme mohli použít binární funkční symbol "+" a predikát rovnosti "=" a případně doplnit např. konstanty "0" a "1" a binární predikátový symbol "≤", se standardní interpretací ve struktuře přirozených čísel. Např. formuli $x \leq y$ můžeme chápat jako zkratku za formuli* $(\exists z)\text{PLUS}(x, z, y)$*. Promyslete si, jak lze pomocí* PLUS *vyjádřit např. $x = 0$ či $x = 1$.*

Není ovšem zřejmé, zda $Th(\mathbb{N}, \text{PLUS})$ je rozhodnutelná. Tuto otázku vyřešil pozitivně Presburger na konci dvacátých let dvacátého století:

Věta 32 *Množina $Th(\mathbb{N}, \text{PLUS})$ (také zvaná Presburgerova aritmetika) je rozhodnutelná.*

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

V rámci tzv. Hilbertova programu bylo potřeba mj. ukázat, že také $Th(\mathbb{N}, \text{PLUS}, \text{MULT})$ je rozhodnutelná; zde MULT je další ternární predikát kde $\text{MULT}(x, y, z)$ platí právě pro trojice čísel x, y, z splňující podmínku $x \cdot y = z$.

Přesněji bychom měli říci, že šlo o nalezení úplné rozhodnutelné teorie T, pro niž je $(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$ modelem. Díky rozhodnutelnosti T by množina $\textsc{Thm}(T)$ byla částečně rozhodnutelná a díky úplnosti pak i rozhodnutelná (pro každou φ stačí souběžně hledat důkaz pro $\overline{\varphi}$ a $\neg\overline{\varphi}$, kde $\overline{\varphi}$ je (univerzální) uzávěr formule φ).

Následující důležitý (Gödelův) výsledek z třicátých let dvacátého století byl překvapivý:

Věta 33 *Množina* $Th(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$ *není rozhodnutelná.*

Nám už je podstata důkazu nerozhodnutelnosti jasná: ke každému Turingovu stroji M a jeho vstupu w lze algoritmicky sestrojit 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 $Th(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$). 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 práce.)

Gödelovy věty o neúplnosti.

První Gödelova věta o neúplnosti.

Podstatu této věty jsme již viděli výše, zformulujme ji teď více standardně:

Věta 34 *Každá axiomatizace struktury* $(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$*, tj. teorie* T *(predikátové logiky prvního řádu) s příslušným jazykem, která je korektní (tj. všechny její uzavřené dokazatalné formule patří do* $Th(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$*) a rozhodnutelná (tj. existuje algoritmus, který rozhoduje, zda daná formule je prvkem* T *neboli axiomem), je neúplná, což znamená, že existuje formule v* $Th(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$*, která není v* T *dokazatelná (neboli existuje formule, která je pravdivá ve struktuře přirozených čísel, ale není dokazatelná ve výchozím axiomatickém systému).*

Věta 34 sice plyne z věty 33, ale navíc vede k otázce, zda lze pro konkrétní korektní a rozhodnutelnou axiomatizaci T struktury $(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$ sestrojit konkrétní formuli, která je pravdivá (tím myslíme je prvkem $Th(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$), ale není dokazatelná (tedy není v $\textsc{Thm}(T)$). To Gödel ukázal; neformálně řečeno, ukázal způsob, jak zkonstruovat aritmetickou formuli φ, která de facto říká "já jsem v T nedokazatelná". (Detailněji, φ říká "pro formuli s určitým pořadovým číslem neexistuje posloupnost, která by byla jejím důkazem v T", ovšem to pořadové číslo je ve skutečnosti číslem formule φ.) Taková φ je jistě pravdivá, protože jinak by se jednalo o nepravdivou formuli, která je dokazatelná v T, a T by tedy nebyla korektní.

Ve zbytku této části načrtneme určitý "programátorský" postup možného důkazu.

Využijeme výše zmíněnou formuli $\Phi_{M,w}(x)$ a větu o rekurzi (zmíněnou níže), a dále očividný fakt, že pro každou rozhodnutelnou axiomatizaci T existuje enumerátor (Turingův stroj) $\mathcal{E}_T$, který generuje všechny uzavřené formule dokazatelné v T.

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.

Věta o rekurzi. Mějme Turingův stroj M realizující (částečnou) funkci $f_M : \Sigma^* \times \Sigma^* \mapsto \Sigma^*$. (Můžeme si stroj M představit jako dvoupáskový s tím, že jeho vstup má dvě části, první napsanou na první pásce a druhou na druhé pásce.) Pak existuje (lze algoritmicky sestrojit) stroj R realizující funkci $f_R : \Sigma^* \mapsto \Sigma^*$ takovou, že pro všechna $w \in \Sigma^*$ platí $f_R(w) = f_M(w, \langle R \rangle)$, kde $\langle R \rangle$ je kódem stroje R.

Idea důkazu. Připomeňme si nějaké standardní kódování Turingových strojů řetězci v pevné abecedě; stačí abeceda $\{0, 1\}$, přičemž budeme předpokládat, že $\{0, 1\} \subseteq \Sigma$ pro abecedu Σ z předpokladu věty. Kód stroje S označme $\langle S \rangle$; jestliže řetězec u je kódem stroje, tak M_u označuje příslušný stroj.

Snadno si uvědomíme, že pro každý řetězec $u \in \Sigma^*$ lze algoritmicky zkonstruovat Turingův stroj P_u, který počítá se dvěma páskami a po spuštění jen zapíše řetězec u na druhou pásku (řekněme, že případný původní obsah druhé pásky přepíše, přičemž první pásku ignoruje). Navrhněme teď stroj B, který po spuštění pracuje také jen na druhé pásce, jejíž obsah v okamžiku spuštění B označme u: B nejdříve zkontroluje, zda řetězec u je kódem nějakého Turingova stroje, tedy stroje M_u; v kladném případě přepíše druhou pásku kódem $\langle P_u; M_u \rangle$ (znak ";" znamená sekvenční kompozici, po ukončení práce prvního stroje je iniciován druhý stroj). Nyní definujme stroj A jako $P_{\langle B;M \rangle}$, a stroj R jako $A; B; M$.

Stroj R si tedy představujeme jako dvoupáskový s tím, že jeho vstup $w \in \Sigma^*$ je napsán na první pásce (a druhá páska je na začátku prázdná). Nejdříve se tedy spustí A, který na druhou pásku zapíše kód stroje $B; M$. Pak se spustí B, který řetězec $\langle B; M \rangle$ na druhé pásce přepíše řetězcem $\langle P_{\langle B;M \rangle}; B; M \rangle$, což je podle definice $\langle A; B; M \rangle$ a tedy $\langle R \rangle$. Pak se spustí M, který má na první pásce onen původní vstup w a na druhé pásce $\langle R \rangle$. Pokud je jeho výpočet konečný, vydá nakonec $f_M(w, \langle R \rangle)$; takže opravdu máme $f_R(w) = f_M(w, \langle R \rangle)$.

Konkrétně můžeme sestrojit 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"). Spusť 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 $Th(\mathbb{N}, \textsc{Plus}, \textsc{Mult})$), 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 obecněji 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 $\neg\varphi$. (V systému F se automaticky předpokládá algoritmická rozhodnutelnost axiomů.)

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

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

Logické programování (Prolog), rezoluční metoda

Zde se jen letmo dotkneme teoretických základů, více se dočtete v [1] a jinde.

Rezoluce ve výrokové logice. Princip *rezoluční metody* se *u výrokové logiky* dá zachytit následovně:

$$(p \vee \varphi), (\neg p \vee \psi) \models \varphi \vee \psi. \tag{7}$$

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

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

kde $\square$ označuje tzv. *prázdnou klauzuli*, kterou chápeme jako označení kontradikce.

Nabízí se tedy možnost následujícího přístupu k *automatizovanému dokazování* $T \models \varphi$ (rezoluční metodou):

Připomeňme, že $T \models \varphi$ právě tehdy, když je $T \cup \{\neg\varphi\}$ nesplnitelná, tedy vlastně právě tehdy, když platí $T, \neg\varphi \models \square$.

Každou formuli z $T \cup \{\neg\varphi\}$ můžeme převést do konjunktivní normální formy a získáme tak souhrnně množinu klauzulí, jejíž nesplnitelnost máme prokázat. (Připomeňme, že klauzule je disjunkce literálů, kde literál je buď výrokový symbol nebo jeho negace.) Pokud dvě klauzule v této množině obsahují komplementární pár literálů, tedy jedna obsahuje p a druhá $\neg p$, můžeme vytvořit další klauzuli, tzv. rezolventu, podle rezolučního pravidla (7). Postupně se tak snažíme vyvodit kontradikci, tedy prázdnou klauzuli $\square$.

Např. chceme ukázat, že platí $p \to q, q \to r \models p \to r$:

V klauzulární formě je zde $T \cup \{\neg\varphi\}$ množinou klauzulí

$$(\neg p \vee q),\ (\neg q \vee r),\ p,\ \neg r$$

(poslední dvě klauzule vzniknou z $\neg(\neg p \vee r)$). Aplikací rezolučního pravidla např. na klauzule $(\neg p \vee q)$ a $(\neg q \vee r)$ vyvodíme rezolventu $(\neg p \vee r)$ (využíváme komutativity $\vee$) a množinu klauzulí tak rozšíříme na

$$(\neg p \vee q),\ (\neg q \vee r),\ p,\ \neg r,\ (\neg p \vee r).$$

Díky $(\neg p \vee r)$ a p vyvodíme r a máme množinu klauzulí

$$(\neg p \vee q),\ (\neg q \vee r),\ p,\ \neg r,\ (\neg p \vee r),\ r.$$

Nyní užitím r a $\neg r$ rozšíříme množinu o rezolventu $\square$ a máme tedy množinu klauzulí

$$(\neg p \vee q),\ (\neg q \vee r),\ p,\ \neg r,\ (\neg p \vee r),\ r,\ \square,$$

která je očividně nesplnitelná. Nutně tedy i výchozí množina je nesplnitelná, a tedy $p \to q, q \to r \models p \to r$ skutečně platí.

Cvičení 58 *Zformalizujte tyto poznatky*

Karel jel autobusem nebo vlakem.

Jel-li Karel autobusem nebo svým vozem, pak přišel pozdě na schůzku.

Karel nepřišel pozdě na schůzku.

ve výrokové logice a pak rezoluční metodou dokažte, že Karel jel vlakem.

Je zřejmé, že když z množiny klauzulí $\mathcal{C}$ opakovaným použitím rezolučního pravidla vyvodíme $\square$, tak množina $\mathcal{C}$ je nesplnitelná. Opačný směr zřejmý není, tak načrtneme důkaz. Stačí ukázat, že z každé konečné nesplnitelné množiny klauzulí lze odvodit $\square$, protože podle věty o kompaktnosti je nekonečná množina nesplnitelná právě tehdy, když existuje její konečná podmnožina, která je nesplnitelná.

Pro konečné množiny $\mathcal{C}$ ukážeme tvrzení indukcí podle počtu m výrokových symbolů objevujících se v klauzulích v $\mathcal{C}$. V každé klauzuli ovšem nedovolujeme více než jeden výskyt každého literálu, jinak bychom např. z nesplnitelné množiny $\{(p \vee p), (\neg p \vee \neg p)\}$ kýženou $\square$ neodvodili.

Když máme nesplnitelnou $\mathcal{C}$ s jediným výrokovým symbolem p, tak v $\mathcal{C}$ nutně musí být klauzule p i klauzule $\neg p$, takže $\square$ odvodíme. Nechť tvrzení platí pro všechny nesplnitelné množiny klauzulí s nejvýš m výrokovými symboly a uvažujme nesplnitelnou $\mathcal{C}$ s $m{+}1$ symboly; nechť jeden z nich je p.

Soustřeďme se nejprve na ta pravdivostní ohodnocení e, pro něž je $e(p) = 1$. Vypusťme z C všechny klauzule obsahující p a v každé zbylé klauzuli vypusťme literál $\neg p$, pokud se v ní vyskytuje. Vznikne množina klauzulí $\mathcal{C}'$ s nanejvýš m výrokovými symboly, která je nesplnitelná (proč?). Z $\mathcal{C}'$ podle indukčního předpokladu odvodíme $\square$. Když přesně totéž odvození (aplikuj pravidlo rezoluce na tyto klauzule podle tohoto výrokového symbolu, pak na tyto klauzule podle tohoto symbolu, atd.) provedeme v původní $\mathcal{C}$, tak pokud jsme nevyvodili $\square$, tak vyvodíme $\neg p$ (proč?). Když pak provedeme analogické úvahy pro případ $e(p) = 0$, dospějeme k odvození p. Ovšem z odvozených klauzulí p a $\neg p$ odvodíme $\square$.

Týden 12

Herbrandova věta (včetně skolemizace). Ilustrovali jsme na konkrétním příkladu. Uvážili jsme teorii obsahující tyto formule $\varphi_1, \varphi_2, \varphi_3, \varphi_4$:

$$(\forall x)(\exists y)P(y,x),\ P(x,y) \to D(y,x),\ (P(x,y) \wedge D(x,z)) \to D(y,z),\ D(x,y) \to \neg(x=y)$$

(např. lze chápat $P(x,y)$ jako "x je rodičem y" a $D(x,y)$ jako "x je potomkem y").

Usoudili jsme, že platí

$$\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\} \models \varphi_5, \quad \text{kde } \varphi_5 \text{ je formule } (\exists x)(\exists y)(P(x,y) \wedge \neg(x=y)).$$

Demonstrujeme to prokázáním, že množina $\{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \neg\overline{\varphi_5}\}$ je nesplnitelná (kde $\overline{\varphi}$ je univerzální uzávěr formule φ; v našem případě ovšem $\overline{\varphi_5} = \varphi_5$). Víme, že všechny formule můžeme univerzálně uzavřít (v našem případě např. $P(x,y) \to D(y,x)$ je nahrazena formulí $(\forall x)(\forall y)(P(x,y) \to D(y,x))$) a převést do prenexní formy. V našem případě jen přepíšeme $\neg\varphi_5$ jako $(\forall x)(\forall y)(\neg P(x,y) \vee x = y)$.

Existenčních kvantifikátorů se zbavíme tzv. *skolemizací*. V našem případě se $\exists$ objevuje jen ve formuli $(\forall x)(\exists y)P(y,x)$. Zavedeme nový funkční symbol f_1 a místo oné formule napíšeme $(\forall x)P(f_1(x),x)$. Tato formule sice není ekvivalentní původní formuli, ale původní množina formulí je nesplnitelná právě tehdy, když nová množina je nesplnitelná; promyslete si proč. Také zformulujte, jak byste se postupně zbavili všech dalších případných existenčních kvantifikátorů (zaváděním stále nových funkčních symbolů).

Máme tedy prokázat nesplnitelnost jisté množiny formulí v prenexní formě bez existenčních kvantifikátorů. Když zapíšeme jejich otevřená jádra (matrice) v konjunktivní normální formě, dostaneme množinu $\{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5\}$, konkrétně

ψ_1 ... $P(f_1(x),x)$,
ψ_2 ... $\neg P(x,y) \vee D(y,x)$,
ψ_3 ... $\neg P(x,y) \vee \neg D(x,z) \vee D(y,z)$,
ψ_4 ... $\neg D(x,y)) \vee \neg(x=y)$,
ψ_5 ... $\neg P(x,y) \vee x = y$.

Rezoluční metodou vyvodíme prázdnou klauzuli $\square$, když použijeme vhodné instance formulí $\psi_1, \psi_2, \psi_3, \psi_4, \psi_5$ vzniklé substitucemi uzavřených termů (prvků tzv. *Herbrandova univerza*, které již známe) za proměnné; budeme ovšem potřebovat i instance axiomů rovnosti. Zavedeme konstantu c (dostaneme tedy Herbrandovo univerzum $\{c, f_1(c), f_1(f_1(c)), \dots\}$) a z instancí $\boxed{P(f_1(c),c)}$ ($\psi_1[x/c]$) a $\boxed{(\neg P(f_1(c),c) \vee D(c,f_1(c))}$ ($\psi_2[x/f_1(c), y/c]$) vyvodíme klauzuli $\boxed{D(c,f_1(c))}$. Z této klauzule a z instance $\boxed{\neg D(c,f_1(c))) \vee \neg(c=f_1(c))}$ vyvodíme $\boxed{\neg(c=f_1(c)}$. Z instancí axiomů rovnosti vyvodíme $(f_1(c) = c \to c = f_1(c)$ a tedy) $\boxed{\neg(f_1(c)=c) \vee c = f_1(c)}$; dalším použitím rezolučního pravidla pak dostaneme $\boxed{\neg(f_1(c)=c)}$. Použitím $\boxed{\neg P(f_1(c),c) \vee f_1(c) = c}$ (instance ψ_5) vyvodíme $\boxed{\neg P(f_1(c),c)}$. Aplikujeme pak rezoluční pravidlo na klauzule $\boxed{P(f_1(c),c)}$ a $\boxed{\neg P(f_1(c),c)}$ a dostáváme kýženou $\square$.

Jedna z variant prezentace Herbrandovy věty je tato:

Věta 35 (Herbrandova) *Pro uzavřenou formuli φ v prenexním tvaru platí $\models \varphi$ právě tehdy, když existuje konečná výrokově sporná teorie, která obsahuje pouze instance formule $(\neg\varphi)^{OS}$ a instance axiomů rovnosti. (Výrazem $(\psi)^{OS}$ označujeme otevřenou skolemovskou variantu formule ψ).*

Rezoluce v logickém programování. Logické programování je založeno na automatizovaném rezolučním dokazování v predikátové logice, což vyžaduje i tzv. unifikaci termů. Budeme to ilustrovat na jednoduchém příkladu programu v Prologu.
(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.
```

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 $P(y,x) \to D(x,y)$ (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 $(P(z,x) \wedge D(z,y)) \to D(x,y)$, 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, resp. klauzulí (po převodu formulí do klauzulární formy). V našem příkladu ji označíme PROG; je to množina těchto klauzulí:

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

$$\textsc{Prog} \models \textsc{Dotaz}.$$

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

$$\textsc{Prog}, \neg\textsc{Dotaz} \models \square,$$

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.

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

- *rezoluční metodě*, využívající mj. *unifikaci* termů a formulí,
- *hornovských klauzulích* (ty obsahují nejvýš jeden pozitivní literál), které mohou být *definitní* (právě jeden pozitivní literál), neboli *fakty* a *pravidla* [z nichž je tvořen prologovský program], nebo *cílové* [odpovídající dotazům 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).
```

Některé další typy logik.

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 nepřiřazuje 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 $\mathrm{VS} \longrightarrow \mathcal{P}(\mathcal{E})$.

> $\mathcal{P}(\mathcal{E})$ 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 $\mathrm{FML} \longrightarrow \mathcal{P}(\mathcal{E})$ (kde FML je množina formulí výrokové logiky s množinou výrokových symbolů VS). Speciálně pro toto rozšířené

e např. platí $\|\varphi \wedge \psi\|_e = \|\varphi\|_e \cap \|\psi\|_e$ a také $\|\varphi \to \psi\|_e = (\|\varphi\|_e)' \cup \|\psi\|_e$, 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 $\longrightarrow [0,1]$; oborem (pravdivostních) hodnot je tedy interval reálných čísel od 0 do 1. Zde se ovšem naskýtá více rozumných možností, jak definovat např. $\|\varphi \wedge \psi\|_e$ a $\|\varphi \to \psi\|_e$; jednou z možností jsou Gödelovy operace: pro konjunkci definujeme $\|\varphi \wedge \psi\|_e = \min(\|\varphi\|_e, \|\psi\|_e)$ a pro implikaci bude hodnota $\|\varphi \to \psi\|_e$ 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:	Process B:
** noncritical region **	** noncritical region **
$flag_A := true$	$flag_B := true$
$turn := B$	$turn := A$
waitfor	**waitfor**
$(flag_B = false \vee turn = A)$	$(flag_A = false \vee turn = B)$
** critical region **	** critical region **
$flag_A := false$	$flag_B := false$
** noncritical region **	** 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]).

Týden 13

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 $T, \neg\varphi \vdash \neg(\psi \to \psi)$).
3. Věta o korektnosti.
4. Churchovo lemma: pro libovolnou formuli φ, která neobsahuje jiné výrokové symboly než $p_1, \ldots, p_n$, platí $p_1^e, \ldots, p_n^e \vdash \varphi^e$.
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 splněného zápočtu nelze jít na zkoušku;
přihlašování na termíny vypsané v IS STAG (pokud není dohodnuto jinak např. emailem);
zkoušení bude probíhat 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 otázku z okruhu A; pokud bude v rozsahu 1-6 (7-12), vytáhne si druhou otázku z okruhu B z rozsahu 6-12 (1-5);
čas na písemnou přípravu: 30 minut (bez možnosti nahlížení do přinesených materiálů a poznámek); čas na ústní zkoušení: zhruba 30 minut.

Reference

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