V. Švejdar, nabídka témat závěrečných prací
(30. srpna 2013)

Seznam témat

1 Gödelův důkaz úplnosti predikátového kalkulu V roce 1931 vyšel Gödelův článek obsahující převratnou větu o neúplnosti (dostatečně silných axiomatických teorií). Článek je velmi slavný, ale zdaleka ne každý logik jej četl, protože způsoby výkladu mezitím pokročily. Před tímto článkem, v roce 1930, vyšel jiný Gödelův článek obsahující větu o úplnosti (predikátové logiky 1. řádu). Tento dřívější článek je čten ještě méně než článek z roku 1931, pravděpodobně protože byl méně převratný a méně překvapivý. Nějaký důkaz věty o úplnosti je dnes běžnou součástí logických kursů.

Gödelovy články přeložil a opatřil komentáři J. van Heijenoort [4]. České překlady, pořízené se znalostí van Heijenoorta, připravuje Katedra filosofie ZČU v Plzni.

Prostudujte a důkladně promyslete Gödelův článek z roku 1930. Vypracujte svou verzi tak, aby se nic neměnilo na myšlenkách důkazu, ale zároveň tak, aby byly doplněny vynechané podrobnosti, aby bylo použito dnešní značení a aby byl použit nějaký z dnešního hlediska běžnější kalkulus. Rozmyslete si, zda v článku nejsou použity nějaké omezující předpoklady, například na mohutnost jazyka nebo na (ne)přítomnost funkčních symbolů či složených termů. Pokud ano, pokuste se je odstranit. Vyhledejte a alespoň si prohlédněte všechnu literaturu, která je citována v poznámkách pod čarou. Kromě technického aspektu, tj. čitelného důkazu, poskytněte čtenáři představu o situaci v logice těsně před Gödelovými větami.

Kriticky posuďte van Heijenoortův překlad i překlad B. Švandové. Není vyloučeno, že Vaše případné poznámky a návrhy by do plzeňského textu před jeho vydáním ještě mohly být zapracovány. Podle vlastní úvahy zahrňte do své analýzy i další články, zejména Skolemovy nebo Gödelův článek z roku 1931. Uvažujte i o otázce, která ale může být obtížnější, co o problematice úplnosti predikátového kalkulu věděl Skolem a zda Gödel byl první, kdo otázku po úplnosti kalkulu formuloval a vyřešil.

[1] K. Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatsh. Math. Phys.*, 37:349–360, 1930.

[2] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38:173–198, 1931.

[3] K. Gödel. Úplnost a neúplnost. Překlad B. Švandové článků z roku 1930 a 1931, editor L. Dostálová, předmluva V. Švejdar, připravováno, 2013.

[4] J. van Heijenoort. *From Frege to Gödel: A Source Book in Mathem. Logic, 1879–1931.* Harvard University Press, 1977.

2 Modely Robinsonovy aritmetiky Robinsonova aritmetika Q je významnou axiomatickou teorií: je velmi slabá, avšak je podstatně neúplná a podstatně nerozhodnutelná. V této vlastnosti se shoduje s Peanovou aritmetikou. Od Peanovy aritmetiky se liší tím, že je konečně axiomatizovatelná. A ještě důležitějším rozdílem je to, že její nestandardní modely lze sestrojit bez užití náročnějších prostředků, jako je ultraprodukt nebo věta o kompaktnosti.

Pokuste se podrobněji popsat strukturu nestandardních modelů Robinsonovy aritmetiky. K tomuto účelu prostudujte ročníkovou práci [1]. Nevadí, když výsledky této práce po prověření převezmete a vypracujete znovu. Pokud to však uděláte, nedržte se značení a doplňte vysvětlení a motivace. Doplňte také některé historické údaje. Pokuste se uvažovat o problému, zda každý model, ve kterém platí prvních pět axiomů Robinsonovy aritmetiky (nebo jen první tři), lze expandovat do modelu, ve kterém platí všechny. Pokud ne, lze charakterizovat modely, které je možné expandovat? Dle vlastního úsudku se zabývejte i variantami Robinsonovy aritmetiky, například Grzegorczykovou teorií Q- s netotálními operacemi, vzájemnou interpretovatelností těchto variant, nebo Robinsonovou aritmetikou nad intuicionistickou logikou.

Téma spíše bakalářské.

[1] M. Kováč. Modely Robinsonovy aritmetiky. Ročníková práce, Filozofická fakulta Univerzity Karlovy, Katedra logiky, 2004.

[2] V. Švejdar. An interpretation of Robinson arithmetic in its Grzegorczyk's weaker variant. *Fundamenta Informaticae*, 81(1–3):347–354, 2007.

[3] A. Tarski, A. Mostowski a R. M. Robinson. *Undecidable Theories.* North-Holland, Amsterdam, 1953.

3 Pojem interpretace aritmetických teorií Pojem interpretace (jedné axiomatické teorie v druhé) se uplatňuje například při prokazování relativní bezespornosti dodatečných axiomů nějaké teorie. To se ve 20. století týkalo zejména teorie množin. Uplatňuje se i v obecné formulaci První Gödelovy věty (*každá bezesporná axiomatická teorie, v níž je interpretovatelná Robinsonova aritmetika* Q*, je neúplná a nerozhodnutelná*). Existují různé varianty tohoto pojmu, např. parametrické interpretace, vícedimenzionální interpretace, lokální a globální interpretace. Interpretovatelnost může sloužit jako nástroj pro porovnávání síly axiomatických teorií. Od přibližně 70. let minulého století je pojem interpretovatelnosti samostatným předmětem výzkumu. Zamyslete se, jak tento pojem lze účelně definovat, porovnejte různá v literatuře se vyskytující řešení, jak překonat technické obtíže v definici. Vypracujte příklady interpretací týkající se známých teorií. Uvažujte o tom, pro které teorie různé varianty tohoto pojmu splývají a pro které ne. Uvažujte o metodách, jak lze prokázat neinterpretovatelnost. Vezměte v úvahu novější literaturu, například či zejména články A. Vissera.

Téma je možné jako bakalářské i jako magisterské. Pojem interpretace byl definován v knize [3] tématu 2, preprinty článků A. Vissera lze stáhnout z holandské preprintové řady Logic Group Preprint Series, relevantní jsou například čísla 279 a 272.

4 Dělitelnost v okruzích Dělitelnost je primárně zkoumána v oboru přirozených nebo celých čísel. Má ale dobrý smysl ji zkoumat i obecně v okruzích či (raději) oborech integrity. Nejčastěji uvažované obory integrity jsou struktura celých čísel a struktura Q$[x]$ polynomů v jedné proměnné s racionálními koeficienty. V těchto dvou oborech integrity navíc platí Bezoutova věta. Vypracujte vlastní verzi teorie dělitelnosti v oborech integrity (okruzích). Vyhledejte v literatuře různé konstrukce okruhů a uvažujte, jak dělitelnost dopadne v oborech integrity, v níž Bezoutova věta neplatí, a jak takové obory integrity vůbec lze sestrojit. Podle vlastní úvahy věnujte pozornost případně také některým z následujících otázek. Existují užitečné axiomy o dělitelnosti jiné než Bezoutova věta, například distributivita násobení vůči největšímu společnému děliteli? Jaký je jejich vztah k Bezoutově větě? Co lze říci o algoritmické složitosti některých úloh (dělení se zbytkem, čínská zbytková věta) v okruzích jiných než struktura celých čísel, například v okruhu Q$[x]$? Co se v teorii dělitelnosti změní v případě, kdy podkladovou logikou se stane intuicionistická logika místo logiky klasické?

Bakalářské téma, jako magisterské by pravděpodobně bylo možné pouze v případě, kdyby se podařilo zjistit či vyhledat zajímavé a málo známé či neznámé výsledky týkající se poslední ze zmíněných otázek.

5 Aritmetická úplnost modální logiky R Aritmetická interpretace logiky GL (logiky dokazatelnosti) je, jak známo, založena na tom, že modalita nutnosti $\Box$ se překládá na formuli $\mathsf{Pr}_T(x)$, která vyjadřuje formální dokazatelnost v nějaké dostatečně silné axiomatické teorii T a se kterou se pracuje v nějaké rovněž silné teorii S, která může ale nemusí být totožná s teorií T. Logika dokazatelnosti je důležitým nástrojem pro zkoumání gödelovské autoreference, v níž autoreferenční sentence tvrdí něco o vlastní nebo vzájemné dokazatelnosti a nedokazatelnosti.

Modální logika R je rozšíření logiky GL o *rosserovské modality* $\preceq$ a $\prec$, které jsou aplikovatelné pouze na formule začínající modalitou $\Box$. Aritmetickým překladem $(\Box A \preceq \Box B)^*$ modální formule $\Box A \preceq \Box B$ je pak sentence existuje důkaz sentence $\overline{A^*}$, před kterým neexistuje žádný důkaz sentence $\overline{B^*}$, kde A^* a B^* jsou překlady formulí A a B, a analogicky se definuje překlad modální formule $\Box A \prec \Box B$. Logika R je nástrojem pro zkoumání rosserovské autoreference, v níž autoreferenční sentence mohou tvrdit něco nejen o dokazatelnosti a nedokazatelnosti, ale i o tom, že důkaz něčeho (existuje a) je menší než důkaz něčeho jiného.

Modální logika R není tak populární jako logika GL, hlavně asi proto, že rosserovská autoreference je příliš různorodá než aby se dala modelovat jednoduchou modální logikou. Nicméně práce o ní existují, zejména článek od Solovaye a Guaspariho.

Napište vlastní studii o logice R. Převeďte známé práce do dnešního značení a uvažujte, co by šlo zjednodušit či zpřehlednit. Navrhněte (vyhledejte v literatuře) případně i gentzenovský kalkulus pro logiku R. Uvažujte i o variantách logiky R a o jejich vlastnostech.

Magisterské téma. Zadáno panu Holíkovi.

[1] D. Guaspari a R. M. Solovay. Rosser sentences. *Ann. Math. Logic*, 16:81–99, 1979.

6 Historie základních pojmů z teorie rekurzívních funkcí Vývoj té části moderní logiky, která se týká podstatné neúplnosti a podstatné nerozhodnutelnosti axiomatických teorií a jejíž výzkum silně ovlivnil Gödelův článek z r. 1930, je neoddělitelně propojen s vývojem teorie rekurzívních funkcí. Teorie rekurzívních funkcí v podobě soustavy pojmů a tvrzení o nich se dnes ve víceméně stejné podobě učí na různých matematických a informatických fakultách. Čemu je ale obvykle věnována menší pozornost, jsou otázky, jak příslušné pojmy vznikly, kdo je první navrhl, zda se přitom objevilo nějaké zdůvodnění terminologie, kdo koho a jak ovlivnil. Pokuste se zmapovat vývoj základních pojmů z teorie rekurzívních funkcí, jako je (primitivně) rekurzívní funkce či množina, produktivní a kreativní množina, věta o rekurzi, převeditelnost, kompletnost, prosté a hyperprosté množiny. Zároveň se pokuste upřesnit, jaký byl přínos zakladatelů teorie: K. Gödel, S. C. Kleene, A. Church, A. Turing, E. Post, případně další. Existují důležité výsledky, které byly známy ještě před Gödelovým článkem?

Jako východisko použijte literaturu, která je citována v [2] a [1]. Články si prohlédněte a některé prostudujte podrobně. Seznamte čtenáře i s konkrétními myšlenkami a důkazy. Převeďte některé důkazy do dnešní podoby s použitím dnešního značení. Protože všech článků citovaných v [2] a [1] je mnoho a všechny prostudovat nemůžete, stanovte si případně nějaký dílčí úkol, který zpracujete podrobněji. Promluvte také s Annou Horskou, která, než se začala zabývat něčím jiným, určité kroky ve zpracování tohoto tématu už podnikla.

Téma lze považovat za bakalářské i magisterské.

[1] P. Odifreddi. *Classical Recursion Theory.* North-Holland, Amsterdam, 1989.

[2] H. Rogers, Jr. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, New York, 1967.

7 Probabilistické algoritmy pro prvočíselnost Ve zjišťování, zda velká čísla jsou prvočísly, se poměrně dobře uplatňují pravděpodobnostní algoritmy, které při zpracování vstupu n provedou nějaký výpočet s číslem n spolu s nějakým dalším náhodně vygenerovaným číslem nebo s více takovými náhodnými čísly. Známy jsou zejména dva takové algoritmy, Rabinův-Millerův a Solovayův-Strassenův. Prostudujte příslušné články a zpracujte tuto problematiku tak, aby bylo jasné, jaké poznatky z teorie čísel oba algoritmy využívají a jak obtížné tyto poznatky jsou.

Bakalářské téma. Zadáno Natálii Tejkalové.

[1] M. O. Rabin. Probabilistic algorithm for testing primality. *J. of Number Theory*, 12:128–138, 1980.

[2] R. M. Solovay a V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Computing*, 6:84–85, 1977.

8 Fragmenty aritmetiky a princip kolekce V článku [1] se zkoumají vztahy mezi tzv. silnými fragmenty Peanovy aritmetiky, tj. teoriemi, které místo schématu indukce mají následující axiomatická schémata:

$$\mathrm{I}\Sigma_n\colon \quad \forall \underline{y}(\varphi(0,\underline{y}) \mathbin{\&} \forall x(\varphi(x,\underline{y}) \to \varphi(\mathrm{S}(x),\underline{y})) \to \forall x \varphi(x,\underline{y})), \qquad \varphi \in \Sigma_n,$$
$$\mathrm{B}\Sigma_n\colon \quad \forall \underline{y} \forall z(\forall u{<}z\, \exists v \varphi(u,v,\underline{y}) \to \exists w \forall u{<}z\, \exists v{<}w\, \varphi(u,v,\underline{y})), \qquad \varphi \in \Sigma_n.$$

$\mathrm{I}\Sigma_n$ je schéma indukce, avšak omezené na formule složitosti Σ_n. Schéma $\mathrm{B}\Sigma_n$ je schéma kolekce, anglicky *collection schema* nebo *bounding schema*, pro formule rovněž složitosti pouze Σ_n. Označení $\mathrm{I}\Sigma_n$ a $\mathrm{B}\Sigma_n$ se vztahuje jak k axiomatickému schématu, tak k teorii, která vznikne přidáním tohoto schématu k vhodné základní teorii. Je známo, že schéma kolekce (bez omezení na složitost formule) lze použít k ekvivalentní axiomatizaci Peanovy aritmetiky.

Fragmenty Peanovy aritmetiky byly zkoumány v 80. letech minulého století, avšak problém, zda schéma $\mathrm{I}\Delta_n$ (indukce pro Δ_n-formule, tj. pro formule, které lze ekvivalentně psát v Σ_n- i Π_n tvaru) je ekvivalentní se schématem $\mathrm{B}\Sigma_n$, vyřešil T. Slaman [2] až v roce 2004.

Napište vlastní zpracování problematiky silných fragmentů Peanovy aritmetiky tak, aby byl zahrnut i Slamanův výsledek. Konstrukce modelů uvedené v [1] přepracujte s použitím dnešního značení a tak, aby byly dány do souvislosti s konstrukcemi obecné teorie modelů. Podle vlastní úvahy vezměte v úvahu i další schémata (Dirichletův princip), nebo se zabývejte interpretovatelností zkoumaných teorií.

Téma pravděpodobně spíše magisterské.

[1] J. B. Paris a L. A. S. Kirby. Σ_n-collection schemas in arithmetic. V A. Macintyre, L. Pacholski a J. Paris, editoři, *Logic Colloquium '77*, Studies in Logic and the Foundations of Mathematics, str. 199–209. North-Holland, Amsterdam, 1978.

[2] T. Slaman. Σ_n-bounding and Δ_n-induction. *Proc. Amer. Math. Soc.*, 132:2449–2456, 2004.