Institute of Mathematics of the AS CR, v.v.i.
Žitná 25, 115 67 Praha 1
Czech Republic

Posudek doktorské disertační práce

Some problems concerning lengths of proofs pana *Mgr. Pavla Hrubeše.*

11. listopadu 2007
Praha

Doktorská práce Mgr. Hrubeše je z tzv. důkazové složitosti, oblasti patřící jak do matematické logiky tak do teorie výpočetní složitosti. Tři nejdůležitější výsledky (viz níže) autor již publikoval (práce [9, 10, 11]). Nicméně nejedná se o soubor prací, protože disertace podává u dvou výsledků z části zjednodušené důkazy.

Hlavní výsledky jsou dle mého názoru tři: (1) příklad teorie, pro niž tzv. Kreiselova hypotéza neplatí, (2) spodní odhad na délky důkazů v několika modálních výrokových logikách a (3) totéž pro intuitionistickou výrokovou logiku.

Kreiselova hypotéza je (dosud nedokázané) tvrzení z teorie důkazů aritmetiky prvního řádu. V teorii důkazů je známá, ale poněkud na okraji zájmu. Důvodem pro to asi je, že budí spíše dojem kuriozity než zásadního problému. Nicméně v průběhu třiceti let z prací několika autorů vyplynulo, že se vlastně jedná o otázku jak efektivně (v kolika krocích v závislosti na délce termu) je možné dokázat platné rovnosti mezi uzavřenými termy. To je otázka, která je zajímavá a dotýká se více oborů.

Mgr. Hrubeš ukázal, že v aritmetice, jejíž jazyk je rozšířen o odčítání, lze dokázat v konstantním počtu kroku všechny rovnosti tvaru $\overline{m} \cdot \overline{n} - \overline{m \cdot n}$. Z toho již známým argumentem Yukamiho (využívajícího Diofantickou definici vhodné r.e. množiny) plyne, že pro takovou teorii Kreiseova hypotéza neplatí.

Výsledky (2) a (3) se týkají složitosti výrokových důkazových systému. Základním problémem v této oblasti je, existuje-li důkazový systém, v němž by šlo dokázat všechny výrokové tautologie krátkým (jehož délka je omezena polynomem v délce dokazované tautologie) důkazem. Při vhodně obecné definici pojmu "důkazový systém" (podané Cookem a Reckhowem) je tato otázka ekvivalentní otázce, je-li třída výpočetní složitosti NP uzavřena na doplněk. To je jeden z fundamentálních problému teorie výpočetní složitosti. Značná část výzkumu se soustředí na dokazování spodních odhadů pro konkrétní důkazové systémy (to má i své vlastní důvody). Problém dokázat spodní odhad pro nějakou neklasickou logiku (z nichž intuitionistická logika a různé modální logiky zaujímají výsadní postavení) byl otevřen mnoho let a řada badatelů na něm pracovala. Mgr. Hrubeš tyto problémy vyřešil. Použil známé metody tzv. feasible interpolation; o to se ale již dříve pokusilo několik autorů a teprve Mgr. Hrubeš našel velice pěkný způsob, jak tuto metodu konkrétně aplikovat. V disertaci dokonce podává elegatní zjednodušení původních důkazů (publikovaných v pracích [10, 11] a v disertaci naznačených v sekcích 3.1.1 a 4.1.1).

V části 4.3.2 by stálo za úvahu použít k formalizaci ve výrokovém počtu překlady z omezené aritmetiky (zkoumané konstrukce jsou v ní formalizovatelné přímočaře). Myslím, že by tak mohlo jít formalizovat i konstrukci z [24], což je zmíněno jako otevřený problém.

Práce je napsána pečlivě (narazil jsem jen na překlepy v indexech k a $k+1$ ve definici formulí *Clique* a *Color* na str.32-33). Moje drobná výtka k formální stránce disertace se týká jen zbytečné úspornosti prezentace. Ve všech částech práce je méně odkazů k literatuře, než je vhodné. Například v Part I. chybí zmínka o (dle mého názoru důležitých) výsledcích Farmera a dalších o teoriích, které mají v jazyce funkční symboly četnosti nejvýše 1. Tamtéž by bylo na místě alespoň zmínit věty o tzv. speed-up jevu (počínaje Gödelem a dále Parikh, Statman, Orevkov a řada dalších), které vedly k definici některých pojmů použitých později v pracech o Kreiselově hypotéze. Jiným příkladem podobné citační úspornosti jsou chybějící citace na práce, v nichž byly definovány některé pojmy zásadní pro Part II; jako příklad uvedu jen chybějící citaci na známý článek Cook-Reckhow, v němž jsou definovány základní pojmy důkazové složitosti. Navíc i v částech, kde odkazy k literatuře jsou, by bylo dobré zmínit některé detaily explicitně. Například v úvodu Part I. čtenáři nezbývá než vydedukovat (z komentáře o pracích jiných autorů či ze seznamu axiomů), jaký je vlastně přesně jazyk PA. Nebo na str.53 jsou zmíněny dřívější interpolační věty jiných autoru, ale není ani naznačeno, v čem se lišily a proč nešly též použít k nepodmíněným spodním odhadům. Tato úspornost prezentace komplikuje život čtenáři, ale všechny použité výsledky ostatních autorů jsou citovány, kde je to potřeba.

Na závěr bych ještě rád učinil pár poznámek k úvodu disertace (str.1 - 3). Oceňuji fakt, že se autor pokouší o určitý filosofický nadhled a dává téměř metafyzickou interpretaci problémům, jejichž speciální případy pak v disertaci studuje. Nicméně si (laicky) myslím, že jednak filosofie jazyka je subtilnější, než je naznačeno uvedenými příklady, a jednak že zmíněné problémy nelze chápat jen jako otázky o efektivnosti definic. Například fakt, že "dobrou" mírou složitosti důkazu je jeho délka, není vubec samozřejmý a

Tel.: +420-222 090 711
Fax.: +420-222 211 638
E-mail: mathinst@math.cas.cz
www: http://math.cas.cz
Bank Connection: ČNB Praha
Account No: 696230110/0710
Company Identif. No: 67985840
Tax Identif. No: CZ67985840

Institute of Mathematics of the AS CR, v.v.i.
Žitná 25, 115 67 Praha 1
Czech Republic

do jisté míry proti intuici a zkušenosti. Ještě k poslední části úvodu (Proof complexity and computational complexity). Nemyslím, že by computability theory přišla s přesnou definicí toho, co je to algoritmus (ale přišla s přesnou definicí toho, co je to algoritmicky vyčíslitelná funkce). Řešení problému (**) by implikovalo řešení (*) jen kdyby bylo negativní. S posledním odstavcem nesouhlasím vůbec. Jedním z mála aktivních programů (t.j. kde se něco děje a v němž participuje více jak pět lidí) mířícím na P versus NP problém je důkazová složitost (idea dokázat různost P a NP přes důkazovou složitost je tzv. Cookův program). Je pravda, že některé metody důkazové složitosti využívají výsledky či metody výpočetní složitosti (zrovna jako využívají kombinatoriku, algebru, t. representací a další). Např. metoda náhodných částečných ohodnocení byla vypůjčena z obvodové složitosti (kde si ji zase vypůjčili z logiky) - zpátky jsme ale vrátili nové a obecnější důkazy různých tzv switching lemmas (Woods či Razborov). Nebo v disertaci použitá metoda feasible interpolation vede ke spodním odhadům poukazem na spodní odhad pro velikost tzv. monotonních obvodů. Lze ovšem myslím docela dobře soudit, že teprve použitím ve feasible interpolation dostaly tyto odhady nějaký opravdový význam.

Shrnutí. Výsledky, kterých Mgr. Hrubeš dosáhl, jsou velice zajímavé a zejména spodní odhad pro intuitionistický výrokový počet ihned zaujal řadu lidí v oboru. Důkazy těchto výsledků sledují strategie vymyšlené již dříve jinými autory, ale Mgr. Hrubeš je využil s velkou invencí a elegancí. Podle mého názoru se jedná o vynikající doktorskou práci, která ve svrchované míře dokazuje talent Mgr. Hrubeše k samostatné tvůrčí vědecké práci v matematice. Dopuručuji, aby disertaci úspěšně obhájil.

P.S. V části Acknowledgements by místo ... *for introducing me to the problem of Kreisel's conjecture* ... bylo přesnější ... *for introducing me to Kreisel's conjecture, his PhD project at the time* ... .

Tel.: +420-222 090 711
Fax.: +420-222 211 638
E-mail: mathinst@math.cas.cz
www: http://math.cas.cz
Bank Connection: ČNB Praha
Account No: 69623011/0710
Company Identif. No: 67985840
Tax Identif. No: CZ67985840