Posudek školitele na disertační práci

Verification of Mathematical proofs
Mgr. Petra Pudláka

Dokazování matematických vět počítačem, tedy konstrukce důkazů různých i nematematických tvrzení z dané množiny předpokladů, je dnes již zavedená disciplina, která má bohaté teoretické zázemí i mnoho praktických aplikací.

Byla vytvořena řada velmi výkonných programů, například *OTTER*, *Isabelle, LINTaP, Spass* nebo *Vampire*, které používájí různých metod strojového dokazování nebo jsou zaměřeny na určitý typ logických systémů. Nejčastěji se setkáváme se strojovými dokazovači pro predikátovou logiku I. řádu, její speciální fragmenty a jejich rozšíření (například různé typy výrokových modálních logic). Takové systémy jsou většinou plně automatizované. Dokazovače pro logiky vyšších řádů jsou častěji interaktivní.

Uživatel má tedy na výběr řadu systémů, které může použít. Zde ovšem problém konstrukce (nebo ověřování) důkazů nekončí. I ten nejvýkonnější systém se může zahltit množstvím odvozených tvrzení, které může být způsobeno příliš velkým počtem axiomů, nevhodnou strategií, opakovaným odvozováním neužitečných tvrzení a podobně.

Předložená práce se zabývá do hloubky třemi z uvedených problémů. První část je věnována přípravné fázi dokazování, efektivní úpravě formulí logiky I. řádu do tvaru klauzulí. Je navržena, implemenována a testována efektivní transformace formulí predikátové logiky I. rádu do konjunktivních normálních tvarů, které jsou obvyklým vstupem pro systémy odvozování.

Druhá část práce je věnována samotnému procesu odvozování, hledání rychlejších a kratších důkazů, pomocí algoritmicky generovaných lemmat. Vytvořený plně automatizovaný program analyzuje důkaz a mezi mnoha podobnými odvozenými tvrzeními, hledá ty, která nejvíce přispěla na cestě k důkazu dané doměnky. Lemmata jsou hodnocena podle několika kriterií a po výběru nejužitečnějších, je sestrojený důkaz většinou radikálně zjednodušen vypuštěním nadbytečných kroků, použitým k důkazům již nepotřebných pomocných tvrzení. Navržený algoritmus, metody hodnocení a výběru lemmat obsahují řadu pozoruhodných myšlenek. Originální je již samotné východisko, které dává přednost dokazování konečné množiny domněnek před dokazováním jenom jediné.

Tato metoda je testována na několika teoriích, fragmentu Teorie množin v podání již zavedeného standardu TPTP, odvozování Booleovských vlastností množin v pojetí znalostní báze Mizar, na Meredithově axiomatizaci výrokové logiky jediným (komplikovaným) schematem axiomů a na modální výrokové logice S5.

Zatímco předchozí dvě části byly založeny na syntaktických metodách, třetí část práce je věnována sémantické analyze problému a výběru vhodných premis z většinou velké (případně potencionálně nekonečné) množiny předpokladů. Zde je využita metoda kontroly modelů v optimálním pravděpodobnostním algoritmu prohledávání potencionálních důkazových stromů. Důkaz optimálnosti algoritmu se opírá o hluboké výsledky z teorie složitosti.

V poslední kapitole jsou uvedené metody použity k detailní analýze vztahů modálních výrokových logik, která je předmětem tzv. Modal Logic Challenge vyhlášené G. Sutcliffem. Autor vychází z modálního systému $S1^0$ a vyšetřuje vztahy mezi modálními logikami S1, S2, S3, S4, S5, K, T a řadou jejich ekvivalentních axiomatik. Jde o tři desítky formálních systémů, jejichž vzájemné vztahy jsou až na několik málo případů navrženým algoritmem detailně rozebrány.

Předložená práce obsahuje víc než dostatek původních myšlenek a originálních postupů, které jsou realizovány v programech, a úspěšně testovány na současných standardech (benchmarks) i na dalších obtížných úlohách. Práce je zpracována přehledně po formalní stránce zcela vyhovujícím způsobem.

Mám zato, že jde o velmi kvalitní práci, kterou doporučuji přijmout jako prací disertační a na jejím základě udělit Mgr. Petru Pudlákovi titul PhD.

V Praze 2. října 2006