František Polach: Testování identit

posudek vedoucího bakalářské práce

Hlavním přínosem práce je zpracování tří základních článků o složitosti problému testování identit v konečných algebrách. Je podán důkaz, že pro nilpotentní grupy a okruhy je tento problém snadný (ve smyslu teorie složitosti), zatímco pro nenilpotentní okruhy je tento problém obtížný. Jde o poměrně komplikované téma, neboť vyžaduje vhled do základů tří dosti rozdílných oborů: teorie složitosti, teorie grup a teorie okruhů. Student se ho přesto zhostil vcelku úspěšně a výsledkem je hodnotná práce, podávající ucelený výklad zadaného problému.

Mezi negativa předložené práce patří poněkud neobratný sloh, který naštěstí na většině míst neubírá na srozumitelnosti. Vážnějším nedostatkem je, že některá tvrzení jsou spíše okomentována, než dokázána, a zasloužila by podrobnější vysvětlení. Navíc práce obsahuje několik drobných matematických nepřesností. Konkrétní příklady:

1) *Str. 10, naivní algoritmus na řešení problému testování identit.* Autor naznačuje, že má exponenciální složitost a že náleží do třídy co-NP. Toto vysvětlení je poměrně odbyto, přitom na tak jednoduchém příkladě šlo např. jednoduše předvést, co je oním polynomiálně ověřitelným certifikátem. Nedostatečné mi též připadá vysvětlení, proč je velikost vstupu "totéž" jako počet proměnných a proč je výpočet hodnoty p(a) polynomiální. Zasvěcenému čtenáři jsou tato fakta jasná, nováčku v oboru, domnívám se, nikoliv.
2) *Str. 12, důkaz 2.1.* Kde se vzaly identity 1.,2.,3.? Důkaz je celkově dosti zmatený, navíc tatáž písmena u,v v něm značí na různých místech různé věci.
3) *Str. 13, důkaz 2.3.* Procedura převedení polynomu na uvedený tvar by jistě zasloužila obsáhlejší komentář. Navíc je nevhodně zvoleno značení, písmeno s značí na různých místech různé termy. Ve formulaci lemmatu je drobná nepřesnost, množiny S_i je třeba číslovat od nuly.
4) *Str. 13, důkaz 2.4.* Formulace je dosti těžkopádná.
5) *Str. 13.* Tvrzení 2.5 je zformulováno špatně. Formálně přepsáno, student zaměnil formuli (forall sigma)(A <=> B(sigma)) za formuli (A <=> (forall sigma)B(sigma)). Důkaz je správně (dokazuje tu druhou variantu tohoto tvrzení).
6) *Str. 15, důkaz 2.6.* Značení a_n se šipkou je nevhodné, neboť tímto způsobem jsou značeny složky. Dále, formálně vzato, množina T by neměla být vstupem algoritmu, neboť pak by se počítala do velikosti vstupu a složitost by byla jiná.
7) *Str. 17, důkaz 2.7.* Poslední věta by zasloužila pořádné vysvětlení. Dále, vnoření prezentované o pár řádek výše je špatně.
8) *Str. 20, důkaz 3.3.* Tvrzení, že |F'|=O(|F|) by zasloužilo lepší vysvětlení.
9) *Str. 21-24.* Poslední kapitola je celkově dosti těžko čitelná a musím přiznat, že jsem důkazu příliš neporozumněl, mj. díky tomu, že na řadě míst chybějí detaily. Např. důkaz 3.5: proč je T_v(g,h) distributivní? důkaz 3.6: proč to implikuje platnost v BA? důkaz 3.10: "obecně známá" tvrzení (která ani já všechna neznám) měla být samostatně zformulována a uvedeny odkazy.

Přes uvedené nedostatky má předložená práce svou hodnotu. Zpracované články byly poměrně obtížné a rozsah práce není malý. Pozitivem práce je také zanedbatelné množství překlepů a jazykových chyb.

S přihlédnutím k uvedeným faktům navrhuji předloženou bakalářskou práci hodnotit stupněm **velmi dobře.**

David Stanovský

16.6.2006