Oponentský posudek diplomové práce

Autor práce: Bc. Marek Zpěváček
Název: Důkazy bezpečnosti hashovacích funkcí
Vedoucí: doc. Mgr. Pavel Příhoda, Ph.D.

Diplomová práce Marka Zpěváčka prezentuje kompletní důkaz přelomového výsledku Miklóse Ajtaie o redukci Problému přibližně nejkratší báze (SBP_f) v libovolné instanci na Problém krátkého řešení (SIS) publikovaného v roce 1996 spolu se zavedením potřebného matematického aparátu a aplikací teoretického výsledku na popis třídy hashovacích funkcí odolných vůči kolizím.

Text obsahuje vedle motivačního úvodu a stručného závěru tři kapitoly. První kapitola se zabývá teorií mříží, je zde zavedena základní terminologie a soustředěn souhrn nezbytných vlastností, které následně umožnují formulaci algoritmických problémů založených na teorii mříží. Centrální a nejrozsáhlejší druhá část práce je věnována samotnému důkazu Altaiova výsledku, tedy konstrukci pravděpodobnostního algoritmu, který umí efektivně vyřešit problém SBP_f v nejhorším případě pomocí orákula řešícího problém SIS v průměrném případě. Poslední velmi stručná kapitola vysvětluje koncept konstrukce odolných hashovacích funkcí spolu s konkrétním příkladem rodiny funkcí SWIFFT.

Jak již bylo řečeno, hlavním cílem práce bylo doplnění nepříliš matematicky jasného článku Miklóse Ajtaie *Generating hard instances of lattice problems* zveřejněného v Electronic Colloquium on Computational Complexity (a na něj práce odkazuje, nikoli na podstatně stručnější verzi uvedenou v seznamu literatury) o matematicky přesné detaily důkazů. Text se struktury článku a myšlenek důkazů přiznaně drží, avšak důkazy doplňuje, často zásadně, o množství netriviálních detailů. Student se tak pravděpodobně sice opravdu přesvědčil, že Altaiova redukce platí, otázkou je, zda je výsledný text pro čtenáře matematicky srozumitelnější a věrohodnější než původní článek. Je trochu škoda, že student nad rámec sdělení, z kterého důkazu v Altaiově článku předvedený postup vychází, podrobněji nekomentoval nejasnosti původního důkazu a způsob, jak byly v jeho textu odstraněny, čehož si byl jistě dobře vědom. Nejvýznamnějším přínosem práce se zdá být explicitní dopočítání hodnot c_i z hlavní Věty 18 spolu s diskusí ohledně možnosti jejich snížení při omezení výběru n na hodnoty nad jistou dolní mezí. Za užitečné v této souvislosti považuji především přesná označení partií důkazu, které tato zlepšení parametrů c_i umožňují.

Text je sice napsán občas poněkud těžkopádným jazykem (viz například formulace „*Splňuje-li ... matice navíc podmínky, které pro nás nejsou důležité, potom se této úpravě říká ...* na straně 5), avšak množství drobných jazykových nedostatků je přiměřené rozsahu práce a matematické formulace jsou vesměs korektní. V dlouhých technických důkazech jednotlivých tvrzení se čtenář snadno stratí (samotný důkaz hlavní Věty 18 má dvanáct stránek), text se proto příliš dobře nečte, škoda, že se nepodařilo formulace a důkazy rozčlenit na jednodušší pozorování, na nichž se snáze udrží čtenářova pozornost, případně nějak zpřehlednit původní Altaiovo značení (připouštím, že to jistě nebylo snadné a možná ani uskutečnitelné). Výsledný

text ovšem bez pochyby dosvědčuje autorův vhled do zkoumané problematiky a jeho schopnost samostatné odborné práce.

Práce Marka Zpěváčka *Důkazy bezpečnosti hashovacích funkcí* podle mého názoru přes uvedené výtky splnila zadání a doporučuji ji uznat jako diplomovou.

v Praze 4.6.2019 Jan Žemlička

Připomínky:

(1) V definici 14 bychom měli psát

$\lambda_i(L) = \min\{r \in \mathbb{R} : L$ obsahuje i lineárně nezávislých vektorů kratších než $r\}$.

(2) Článek, na nějž se práce odkazuje je

Ajtai, M. (1996). Generating hard instances of lattice problems (Extended abstract + Appendix). Electronic Colloquium on Computational Complexity - Reports Series 1996, TR96-007, https://eccc.weizmann.ac.il/report/1996/007/