

Ing. Petr Tichavský, DSc.
ÚSTAV TEORIE INFORMACE A AUTOMATIZACE AV ČR, v.v.i.
Pod Vodárenskou věží 4, 182 08 Praha 8

Posudek školitele bakalářské práce

Vojtěch Obhlídal: Kanonický rozklad tenzorů násobení polynomů a násobení matic na $GF(2)$

Předložená bakalářská práce se týká problematiky algebraické složitosti operace maticového násobení a násobení polynomů. Složitost těchto algebraických operací je dána hodnotami příslušných tenzorů, které tyto číselné operace popisují jako obecné bilineární funkce. Větší pozornost je věnována násobení polynomů, násobení matic je zmíněno spíše okrajově.

Násobení polynomů se jeví jako snazší úloha než násobení matic. Z teoretického hlediska je znám Toom-Cookův algoritmus, který říká, že složitost násobení roste lineárně se stupněm polynomu, pokud ovšem zanedbáváme složitost násobení koeficientů skalárem. Z praktického hlediska se však tento algoritmus nechová dobře, využívá inverze Vandermondovy matice, která je špatně podmíněná. Motivace práce je nalezení algoritmu pro násobení polynomů které by mělo sice vyšší složitost než Toom-Cookův algoritmus, ale bylo by možné provádět výpočty na okruhu celých čísel. Tato úloha pak vede na úlohu nalezení rozkladu tenzoru násobení na $GF(2)$, což je nejmenší číselné těleso s prvky 0 a 1.

Práce se zabývá možností hledání rozkladu tenzoru na $GF(2)$ pomocí zkoumání splnitelnosti Booleovských formulí, které jsou z rozkladu tenzoru odvozené. V podstatě jsme zjistili, že v současné době existující algoritmy a programy pro splnitelnost Booleovských formulí jsou na hranici toho co lze dosáhnout jinými metodami.

Podarilo se najít jeden nový v literatuře dosud nepopsaný algoritmus pro násobení polynomu stupně 6, který funguje na $GF(2)$, ale bohužel k němu nebyl nalezen odpovídající rozklad na množině celých čísel. Výsledek je tedy spíše negativní, spíše šlo o prozkoumání možností kam až se dá s existujícím software ve složitosti problémů dojít.

Nyní k obsahu práce. V nezbytném úvodu autor poskytuje přehled existujících algoritmů pro násobení polynomů nízkých stupňů - Karatsubův algoritmus a jeho varianty, a další algoritmy. V kapitole 2 autor dává autor motivaci pro zvolený způsob hledání algoritmů pro násobení polynomů přes Booleovské formule a popisuje tuto cestu. Kapitola 3 pak shrnuje dosažené výsledky.

Práce je napsaná poměrně pečlivě. Jedinou výtka kterou bych měl, je spíše k autorovi samotnému než k práci vlastní: k hodnocení A, výborně, bych si představoval větší kreativitu a samostatnější přístup k problematice než pouze přímočaré řešení daného problému pomocí doporučené metody. Pravdou je, že první dvě reference v práci student našel v literatuře a prostudoval samostatně. Chválu zaslouží také schopnost studenta používat nové programové nástroje, a pracovat systematicky.

S ohledem na výše uvedené se domnívám, že předložená práce splňuje požadavky kladené na bakalářské práce a navrhuji klasifikaci B, velmi dobře.

V Praze, 1.8.. 2020

Ing. Petr Tichavský, DSc.
