Posudek vedoucího bakalářské práce

Název: Násobení v konečném tělese charakteristiky 2 a XOR-metriky
Autor: Nikita Edward Carulkov

Shrnutí obsahu práce

Předložená práce porovnává dvojici maticových metrik vyjadřujících výpočetní náročnost násobení regulární maticí nad dvouprvkovým tělesem, které se ukazují být zajímavé v kontextu „lehkovážné" (lightweight) kryptografie v přístrojích s omezenou výpočetní kapacitou, konkrétně pro reprezentaci počítání v konečných tělesech. První *přímá* metrika (*d-XOR-count*) je založena na Hammingově váze, zatímco druhá *sekvenční* metrika (*s-XOR-count*) počítá minimální počet elementárních matic, jejichž součinem je až na permutaci řádků daná matice.

Text je vedle úvodu a závěru rozdělen do dvou kapitol, z nichž první prezentuje známé základní vlastnosti obou metrik. Druhá část práce obsahuje studentovy vlastní výsledky, jednak konstrukci tříd matic, jejichž přímá metrika je menší než sekvenční, a dále nalezení minimálního stupně matice, pro který lze takovou konstruovat realizovat.

Celkové hodnocení práce

Téma práce. Téma práce vychází z článku Lukase Kölsche "XOR-Counts and Lightweight Multiplication with Fixed Elements in Binary Finite Fields", jehož některé výsledky prezentuje a dále rozvíjí a zobecňuje. Zadání bylo studentem podle mého mínění velmi zdařile naplněno.

Vlastní příspěvek. Celou druhou kapitolu textu tvoří studentovy vlastní výsledky, které zesilují a zpřesňují výsledky zpracovaného článku.

Matematická úroveň. Matematická úroveň práce je podle mého mínění velmi dobrá a formulace jsou korektní.

Práce se zdroji. Třebaže první část práce zpracovává známé výsledky, výsledný text na zdrojích není nijak formulačně závislý. Druhá část práce vychází sice z publikované konstrukce, prezentované výsledky jsou ovšem původní.

Formální úprava. Formální náležitosti práce nezasluhují podle mého názoru žádné výtky a jazykových a stylistických nedostatků je v textu velmi málo.

Připomínky a otázky

S připomínkami a otázkami, které jsem vznášel průběžně k pracovním verzím práce, se student úspěšně vyrovnal a ve finálním textu už jsem významnější nedostatky nepostřehl.

Závěr

Práce Nikity Edwarda Carulkova *Násobení v konečném tělese charakteristiky 2 a XOR-metriky* podle mého názoru zcela splnila zadání a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace vedoucí práce sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
21.6.2020