Posudek oponenta bakalářské práce

Název: Maticový přístup ke konstrukci kvadratických APN funkcí
Autor: Zuzana Rezková

Shrnutí obsahu práce

Práce Zuzany Rezkové je věnována reprezentování a následně konstrukcím skoro perfektních nelineárních (APN) vektorových booleovských funkcí, tj. kryptograficky užitečných funkcí F splňujících pro každé a, b, kde $a \neq 0$, podmínku $|\{x \in \mathbb{F}_2^n \mid F(x) + F(x+a) = b\}| \leq 2$. Základní využívanou myšlenkou je maticová reprezentace homogenních kvadratických APN funkcí. Text je rozdělen vedle motivačního úvodu a stručného závěru do čtyř částí. Zatímco první z nich čtenáře uvádí do teorie booleovských funkcí, obsahuje nejrozsáhlejší druhá kapitola detailní souhrn výsledků článku Yuyin Yu, Mingsheng Wang, Yongqiang Li „A matrix approach for constructing quadratic APN functions". V návaznosti na druhou kapitolu popisuje originální třetí část textu reprezentaci kvadratických APN funkcí pomocí jejich algebraické normální formy a poslední kapitola předkládá příklady prezentovaných konstrukcí.

Celkové hodnocení práce

Téma práce. Téma práce bylo obtížné, ale velmi aktuální a zajímavé, a proto vhodné pro zpracování v bakalářské práci. Zadání práce bylo studentkou podle mého mínění velmi úspěšně naplněno.

Vlastní příspěvek. Zatímco první polovina práce je velmi dobře zpracovanou kompilací, která vysvětluje a doplňuje nejasná místa zpracovávaného článku, druhá polovina sestává z několika vlastních výsledků a předvedení maticových konstrukcí na příkladech.

Matematická úroveň. Matematická úroveň práce je vysoká, formulace jsou korektní a dobře srozumitelné.

Práce se zdroji. Text se primárně opírá o jeden článek, na němž zjevně není formulačně závislý. Jádro práce navíc spočívá v původních výsledcích a aplikaci konstrukcí.

Formální úprava. Formální náležitosti práce nezasluhují žádnou výtku. Text je napsán velmi čtivě, jazykových a stylistických nepřesností jsem zaznamenal zanedbatelné množství.

Připomínky a otázky

1. strana 11: V důkazu Corollary 16 není třeba dokazovat slučitelnost zobrazení L_a s násobením skalárem, to plyne pro každý vektorový prostor nad tělesem prvočíselného řádu už ze slučitelnosti s grupovou operací (nad tělesem $\mathbb{F}_2$ je to navíc v podstatě triviální).

Závěr

Text Zuzany Rezkové „Maticový přístup ke konstrukci kvadratických APN funkcí"je podle mého názoru velmi pěkný a bezpochyby splnil zadání. Práci proto doporučuji uznat jako bakalářskou.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
1.9.2020