POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Název: *MDS matice*
Autor: *Šárka Vlášková*

Práce se zabývá studiem MDS matic, kteréžto se využívají v kryptografii. Matice je MDS, pokud je každá její čtvercová podmatice regulární. Ač se jedná o velice jednoduchou definici, konstrukce MDS matic není přímočará a právě tomu se věnuje tato práce. V práci jsou předvedeny tři metody: konstrukce pomocí *Cauchyho matic* (2. kapitola), pomocí *Vandermondových matic* (3. kapitola) a pomocí *sériových matic*, to však pouze pro matice řádu čtyři (5. kapitola). Kapitola 4 pojednává o vlastnostech MDS matic a testovacím algoritmu.

Text práce je z matematického hlediska korektní a práce se celkově dobře čte, množství překlepů odpovídá rozsahu. Stav kontroly na plagiáty v SIS ukazuje celkovou podobnost 26%, Turnitin 24%, což není úplně málo. Prosím autorku, ať toto v rámci obhajoby práce okomentuje.

Konkrétní připomínky

- Důkaz Lemmatu 2.2 jde zjednodušit, místo opakování kroků 1)-3) pro D_1, …, D_{d-2} lze na matici D_1 použít indukční předpoklad, zbytek snadno plyne. Rovněž by bylo záhodno, kdyby znění Lemmatu 2.2 dávalo smysl i pro $d = 1$, k tomu stačí definovat prázdný součin jako 1.
- Formulace Věty 3.4 je zavádějící. V práci je MDS matice zadefinovaná pouze pro čtvercové matice, zpětná implikace Věty 3.4 proto neplatí. V případě čtvercové MDS matice je nutno předpokládat, že $r=s$.
- Pojem „nízká Hammingova váha" v popisu Algoritmu 3 je dosti vágní. Lepší by bylo použít nějaké uspořádání, např. lexikografické.
- V první větě v Sekci 2.4 by bylo vhodné dát do souvislosti *p* a *q*, tj že *q* je mocnina *p*.

Otázky

1. Vysvětlete, proč je počet jedniček v efektivní involuční MSD matici nad F_q, $q = 2^n$, roven d? Tvrdí se, že to plyne z Lemmatu 2.8, ale to jen říká, že d je počet různých prvků v Cauchyho matici.
2. K čemu je zapotřebí znalost počtu aditivních podgrup tělesa F_q? Dejte do souvislosti s počtem MDS matic.
3. Jsou matice zkonstruované v Lemmatech 5.5-5.7 všechny čtvercové MDS matice řádu 4 nad F_q, kde $q=2^n$, nebo jde jen o ukázku některých takových matic? Omezte se na případ, kdy $z_i \in \{1, \alpha, \alpha^2, \alpha + 1\}$.
4. Oceňuji, že je implementace Algoritmů 1, 2 a 4 přiložena k práci. Algoritmus 3 ovšem není naimplementován, proč? Jeví se býti nejzajímavější.

Drobné překlepy

- str 9 nahoře: špatný font pro těleso F_q
- str 14: vezeme → vezmeme
- str 17: úpravy v bodě (ii) ke konci: $= 1$, dle (3) → dle (4)

Závěr

Předloženou práci považuji za kvalitní a doporučuji ji uznat jako bakalářskou práci.

Návrh klasifikace sdělí oponent předsedovi zkušební komise.

Zuzana Patáková
Katedra algebry
29.8.2023