Posudek oponenta bakalářské práce

Název: Konstrukce MDS matic
Autor: Lukáš Belza

Shrnutí obsahu práce

Práce se zabývá metodami konstrukce tzv. MDS matic, tj. matic A typu $k \times m$ nad (většinou konečnými) tělesy takových, že řádky matice $(I_k \mid A)$ generují MDS kód ve smyslu algebraické teorie samoopravných kódů. Pěkná ekvivalentní charakterizace takovýchto matic je uvedena a dokázána v práci jakožto věta 5: Matice je MDS, právě když má všechny minory nenulové. Autor se poté zaměřuje převážně na metody konstrukce čtvercových MDS matic malých řádů (konkrétně 3 a 4) speciálního tvaru (tzv. cirkulantní matice) a na závěr doplňuje velice stručný nástin významu MDS matic v kryptografii.

Celkové hodnocení práce

Téma práce. Téma považuji za vhodné pro bakalářskou práci – z teorie využívá převážně lineární algebru, ale umožňuje ji aplikovat a zkoumat ze zajímavé perspektivy.

Vlastní příspěvek. Příspěvek autora spočívá v doplnění a rozvedení důkazů z literatury a vlastním bádáním nad charakterizací cirkulantních MDS matic malých řádů, což považuji za odpovídající úrovni bakalářské práce.

Matematická úroveň. Práce je sepsána pečlivě a srozumitelně, matematická úroveň je dobrá. Vytkl bych určitou nevyrovnanost v podrobnosti důkazů – některé argumenty jsou rozebrány do posledního detailu a doplněny příkladem, zatímco jinde jsou ne zcela samozřejmé kroky vydávány prostě za fakt. Více k tomu níže.

Práce se zdroji. Nemám námitek.

Formální úprava. Formální úprava práce je z mého pohledu plně vyhovující.

Připomínky a otázky

Nejprve uvádím připomínky k důkazům, konkrétně k místům, které by podle mě zasloužily doplnit:

1. Důkaz věty 5, str. 4 a 5 – věta o rozvoji determinantu podle sloupce se používá na matici B opakovaně a formulka pro vztah determinantů matic B a M by vzhledem k úrovni detailů v okolním textu zasloužila vlastní lemma.

2. Důkaz lemmatu 12 na str. 9 – to, že pro cirkulatní matici A platí $A^T = TAT$, by určitě chtělo vysvětlit. Je totiž klíčové, že matice je opravdu cirkulantní, tudíž překlopení podle vedlejší diagonály ji nemění. Pro obecnou čtvercovou matici A se totiž A^T a TAT liší přesně o překlopení podle vedlejší diagonály. Ve finále mi přijde, že rovnost $A^T = TAT$ je na důkaz srovnatelně obtížná jako znění lemmatu 12 samotného.

3. Důkaz lemmatu 17 na str. 13 – chybí vysvětlení, proč přesně existuje $n \in \mathbb{N}$ takové, že $M^n = I_d$.

Nakonec ještě několik méně podstatných připomínek a otázek:

4. Druhý odstavec v části 1.1 na str. 3 je mírně nepřesný. Např. $[n, k, d]$ kód není *určený* trojicí n, k, d. Jinými slovy, existuje typicky hodně různých kódů se stejnou trojicí parametrů n, k, d.
5. Str. 5, řádek 11 – chybí složené závorky, $i \in \{1, \ldots, p\}$.
6. Konec prvního odstavce na str. 7 – spíš bych psal „skript o konečných tělesech“.
7. Ve znění tvrzení 23 na str. 19 označuje tentýž symbol n dvě různá čísla.
8. Poslední dvě věty části 2.2.1 na str. 26 tak, jak jsou, trochu matou (byť jim v kontextu předchozího textu rozumět je).
9. Otázka k příkladu pod lemmatem 29 na str. 26 – je bloková konstrukce vhodná k tvoření ne nutně cirkulatních MDS matic? Konstrukce s Vandermondovými maticemi o kousek dál, počítám, také zřídka kdy dá za výsledek cirkulatní matici.
10. Poslední věta před tvrzením 31 (str. 27) – požadavek na ortogonalitu nejde splnit u cirkulatních *MDS* matic (přidal bych „MDS“).
11. Přelom str. 27/28 – písmeno k se používá ve dvou různých významech, což trochu mate.
12. Poslední vzorec na str. 29 – proč by měly zmizet druhé mocniny, tj. proč např. $(a_0 + a_2)^2 = a_0 + a_2$?
13. Str. 30/31 – to, že čísla místo na poznámky pod čarou odkazují na body na další straně, je velice účelné, ale poněkud nezvyklé a nebylo by špatné čtenáře předem varovat, aby nepropadal panice, že vysvětlení chybí.
14. Str. 31, poznámka 4 – vysvětlení rozdílu mezi aktivními a pasivními S-boxy mi přijde zestručněné až do té míry, že neplní účel (tj. neznalý čtenář si tu informaci musí dohledat jinde).

Závěr

Práci považuji za zdařilou a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

doc. RNDr. Jan Šťovíček, Ph.D.
Katedra algebry MFF UK
3. 2. 2021