Posudek oponenta na diplomovou práci

Filip Lorenc: CRC-kódy

Cílem práce je pochopit nedostatky, co se týče nedetekovaných chyb přenosu, u síťového komunikačního protokolu CAN FD, což je novější verze protokolu CAN (Controller Area Network). Protokol se dle slov autora používá ve velké míře v automobilech.

Z matematického hlediska jde o studium vlastností určitého typu lineárních samoopravných kódů, konkrétně krácených cyklických kódů. CRC-kód je název pro takovýto kód spolu s konkrétní přirozenou metodou kódování odpovídající tomu, kdybychom u obecného lineárního kódu používali generující matici ve standardním tvaru (tj. k odesílaným zprávám přidáváme kontrolní bity).

Zajímavý je ovšem samotný předmět studia, který je v běžných učebnicích dosti opomíjen. A sice jaké přesně vlastnosti mají takovéto samoopravné kódy vzhledem k chybám synchronizace, tj. když je z odesílané zprávy jeden bit odebrán nebo je do ní vložen jeden náhodný bit navíc. K tomuto problému se autor dostane přirozenou cestou při studiu konkrétních potíží s původním návrhem protokolu CAN FD a spočítá (za vcelku standardních předpokladů) pravděpodobnost, že takováto chyba nastane. Ukáže se, že tato pravděpodobnost závisí pouze na délce zprávy a počtu kontrolních bitů, ale už nikoliv na tom, jak konkrétně kontrolní bity počítáme (tj. jaký CRC-polynom zvolíme). Mezi další přínosy práce patří i návrh optimalizace u implementace dlouhých CRC-kódů pro běžně používané počítače.

Práce je rozsahem poměrně dlouhá, ale to je dáno tím, že autor vše důkladně vysvětluje. Čte se velice dobře a v úvodních částech mi přišla možná pomalejší, než bylo nutné (což je samozřejmě dost subjektivní). Matematicky je práce korektní a pečlivě zpracovaná. Uvádím jen několik nepříliš podstatných připomínek a překlepů:

1. Vzorec pro LSbF řazení by měl být $u(x) = \sum_{i=0}^{n-1} u_{n-i-1} x^i$.

2. Polynomiální kódy podle def. 1.2.3 musí obsahovat aspoň jeden nenulový vektor. Toto poněkud nepřirozené omezení postupem času bez komentáře zmizí (např. v tvrz. 1.3.5).

3. Podobný případ drobné nekonzistence má původ též v def. 1.3.1, kde byly cyklické kódy zavedeny bez předpokladu linearity, ale dále se tato obecnost nikde nepoužívá. Čili pak by bylo striktně vzato nutné všude psát „lineární cyklický kód“, což postupem času také potichu vymizí, např. hned v důsl. 1.3.4.

4. Poslední pozorování na str. 12: vzorec pro počet cyklických kódů bych si spíš představoval ve tvaru $\prod_{i=1}^{k}(e_i + 1)$.

5. Na str. 16 uprostřed by měl být polynom $a(x)$ stupně nejvýše $k - 1$ místo $n - 1$.

6. Lemma 2.2.4 je trochu neobratně formulované, jako by to, že $G = \mathbb{F}_{q^m}^*$ je grupa, nebyl známý fakt, ale předpoklad lemmatu.

7. Poznámka 3.1.8 by asi měla končit slovy „každý CRC-kód vznikl zkrácením nějakého cyklického kódu“.

8. Pozorování na str. 62/63: Bylo by dobré zdůraznit, že *každé* řešení té druhé soustavy musí končit $s - r$ nulami (protože tohle je potřeba si uvědomit následně v důkazu důsl. 4.2.11). A také je lepší věty nezačínat matematickým symbolem.

9. Překlep v pozorování na str. 67: i-tice má být $u_{j-1}, \ldots, u_{j-i}$.

10. První věta na str. 75: Všechny prvky $\mathbb{F}_{128}^*$ *mimo* 1 jsou primitivní.

Končím ještě zvědavým dotazem: Jak konkrétně si mám v praxi představit vícekrát zmíněnou „analýzu vlastností CRC-kódů hrubou silou“?

Práce rozhodně **doporučuji k obhajobě** a návrh hodnocení sdělím přímo komisi.

V Praze dne 14. 6. 2021 doc. RNDr. Jan Šťovíček, Ph.D.