Oponentský posudek diplomové práce

Jaroslav Kotil: Goppa kódy a jejich aplikace

Předložená práce se zabývá samoopravnými Goppovými kódy a jejich aplikací pro postkvantové kryptosystémy: McEliecův a velmi podobný Niederreiterův kryptosystém.

Práce podává velmi pěkný a ucelený přehled tématu. U Goppa kódů jsou odvozené základní vlastnosti a tyto kódy jsou interpretovány jednak jako alternantní kódy a jednak jako reziduální kódy algebraicko geometrických kódů. Jsou rozebrány speciální zajímavé vlastnosti binárních a divokých Goppových kódů a je ukázán efektivní dekódovací algoritmus založený na rozšířeném Euklidově algoritmu. Dále jsou pak diskutovány kryptosystémy založené na obtížnosti problému dekódování vzhledem k náhodnému lineárnímu kódu a možné útoky na ně.

Ačkoliv jde převážně o fakta dostupná v literatuře, seznam literatury je velmi dlouhý (přes 40 položek) a podle slov autora bylo nutné doplnit a zpřehlednit různé důkazy.

Dojem z této jinak velmi pěkné práce kazí ne zcela pečlivé zpracování. Jedna obecná výtka směřuje k citacím, kdy autor pro ten který důkaz odkazuje do monografií bez přesnějšího určení, kde se dané tvrzení najde. Dále text obsahuje více nepřesností, které ho činí obtížněji srozumitelným:

1. Závěr důkazu věty 1.23 je trochu odbytý, protože obecný prvek kódu C' je tvaru $c' = c + \beta y$, kde $c \in C$ a $\beta \in \mathbb{F}_q$.

2. Na stránce 16 uprostřed by se $x \in F$ spíše dalo reprezentovat jakožto funkce $F \to \overline{K}$. Těleso $\mathcal{O}_P/P$ je závislé na místě P, ale vždy lze nějak vnořit do algebraického uzávěru tělesa K.

3. Poznámka 1.11 na str. 20 je matoucí. Eliptické křivky odpovídají funkčním tělesům rodu 1, zatímco racionální funkční těleso je rodu 0.

4. Technicky vzato je problém faktorizace (str. 22) subexponenciální, protože číselné síto potřebuje cca. $\mathcal{O}(e^{\sqrt[3]{x}})$ kroků, kde x je počet bitů faktorizovaného čísla.

5. Na str. 24 je obecně P ideál pouze, pokud je g ireducibilní. Jednoduchý protipříklad v opačném případě: Nechť $R = \mathbb{Z}$ a $g = 6$. Pak $2, 3 \in P = R \setminus S$, ale $2 + 3 \in S$.

6. Polynomy f ve znění tvrzení 2.4 (str. 28) nemohou být monické. Proč tomu tak je, je dobře vidět z důkazu, konkrétně z toho, že polynom $d(x)$ daný rovností na str. 29 bude těžko obecně monický.

7. Definice syndromového polynomu $S(x)$ na str. 36 je matoucí. Mělo být z kraje řečeno, že podíl $r_i/(x-\alpha_i)$ uvažujeme modulo $g(x)$.

8. Ve znění lemmatu 2.13 (str. 39) mělo být předpokládáno $s(x) \neq 0$ a též měla být zdůrazněna jednoznačnost i.

9. Na str. 40 mi pro obecný bezčtvercový polynom $g(x)$ není zdaleka jasné, proč existuje k $S(x)$ inverze modulo $g(x)$. Nutný a postačující předpoklad je, že $\mathrm{NSD}(S, g) = 1$, což se zdá být jasné pouze v případě, že $g(x)$ je ireducibilní.

10. U tvorby klíčů na str. 42 a 44 by matice S a P nejspíš měly být nad tímtéž tělesem jako kód C.

11. Vypovídací hodnota druhé poloviny obrázku 3.1 na str. 49 je velice omezená, protože zlepšení od Leona a Sterna nebyla vysvětlena.

Nakonec uvádím nalezené překlepy:

1. Poslední řádek na str. 5 není v zavedeném značení správně zapsán.

2. V matici G na str. 13 nahoře má být v dolním řádku v exponentech $k-1$ místo $n-k-1$.

3. Na str. 19: $\mathrm{Ker}(\mathrm{ev}) = \{f \in \mathcal{L}(\mathcal{G}) \mid \ldots$

4. Na str. 26 na 4. řádku odspoda má být $\sum_{j=1}^{t} x^{t-j} \left(\sum_{k=1}^{j} g_{t-k+1} \alpha^{j-k} \right)$.

5. Na str. 32 nahoře je $f' = \sum_{i=1}^{n} c_i \prod_{j \neq i} (x - \alpha_j)^{c_j}$.

6. Na str. 33 jde o $[8, 2, 5]_2$ Goppa kód.

7. Na str. 36 dole: $\deg \sigma(x) \leq \frac{t}{2}$.

8. Na str. 37 v algoritmu 1, kroku 1 jsou chybně inicializovány polynomy u_0, u_1, v_0, v_1.

9. Špatné nerovnosti u $\mathrm{wt}(e)$, $\deg\alpha(x)$, $\deg\beta(x)$ na str. 40.

10. Na str. 53: $m_r G_r$

I přes uvedené nedostatky je předložená práce velice zajímavá a prokazuje dobré porozumění tématu.

Práci **doporučuji uznat jako diplomovou** a hodnocení příkládám na zvláštním listě.

V Praze dne 16. 8. 2013 RNDr. Jan Šťovíček, Ph.D.