Posudek oponenta diplomové práce
Cryptographic application of codes over Galois rings
Bc. Marka Marko

Předložená práce studuje kódy nad konečnými uniseriálními okruhy, zejména nad Galoisovými okruhy. Kódem se rozumí podmodul konečně generovaného volného modulu. Na těchto kódech není uvažovaná klasická Hammingova metrika, ale takzvaná 'cardinal rank distance', která se počítá z velikosti podmodulu okruhu, který nad prvookruhem generují souřadnice kódového slova.

Speciání pozornost je věnována tzv. Gabidulinovým kódům, to jsou kódy odvozené z vhodného slova pomocí generátoru grupy automorfismů daného Galoisova okruhu. V závěru práce je představen kryptosystém GPT, což je analogie McElieceho kryptosystému založená na Gabidulinových kódech.

Práce se zabývá aplikací poměrně náročné části teorie okruhů v teorii kódů. V úvodu by mohlo být podrobněji rozebráno, zda kódy nebo kryptosystém mají nějakou výhodu oproti klasickým lineárním kódům.

Text je velmi dobře strukturovaný, autor se snaží průběžně vysvětlovat, k čemu bude dokazované tvrzení dobré. Přestože se jedná převážně o kompilační práci, autor prezentuje vlastní, vesměs konstruktivní, přístup k dokazovaným tvrzením. V několika důkazech v závěru práce jsem se bohužel ztratil (viz podrobnější komentář níže), jinak jsou ale důkazy psány pečlivě a srozumitelně. Práce též obsahuje větší množství původních příkladů.

Práce s literaturou je v pořádku, ve 3. kapitole bych ale uvedl též relevantní zdroj [6].

Celkově si myslím, že práce splnila zadání a doporučuji ji uznat jako práci diplomovou.

V Praze, 1. 9. 2024

Pavel Příhoda

Konkrétní připomínky k práci:

- Většinu výsledků v kapiltolách 2 a 3 lze formulovat s předpokladem, $S \subseteq R$ je rozšíření konečných uniseriálních okruhů s maximálními ideály pS a pR přičemž R je volný S-modul ranku r. Hlubší vlastnosti Galoisových okruhů se uplatňují hlavně v kapitole 4.
- Claim 13, první odstavec důkazu: Každý konečný okruh je noetherovský.
- Claim 26: M je pravděpodobně podmodul R^m
- Theorem 48: Byl definován rank matice nad S?
- Corollary 49: Smithova normální forma X by měla mít rozměry $k \times l$. Navíc by měla jít najít s koeficienty v S.

- Sekce 3.2: Poznámku, že $rk(a)$ je vlastně $\log_{|S|}(|\sum_{i=1}^{m} Sa_i|)$ by bylo lepší dát hned za Definici 52. Jednak jde o bezsouřadnicový pohled, také je ihned vidět, že kódové slovo s minimální váhou musíme hledat v soclu daného kódu.
- Theorem 54: Bude tvrzení za 'Futhermore' platit pro $x = (1, p, 0, \ldots, 0)$?
- str. 39 dole: Nad jakým okruhem je $\overline{\omega}$ modulový homomorfismus?
- Theorem 61, 2.: Proč je rank kódu $\mathcal{D}$ roven l?
- Corollary 62, 2.: Není zdůvodněno, proč F je volný.
- str. 46, ř. 4: Tvrzení, že λ je homomorfismus těles mi není jasné. Charakteristika p zaručuje slučitelnost se sčítáním, ale proč by mělo platit $\lambda(1) = 1$?
- Definice 69: Mělo by být ujasněno, zda je $F(X)$ prvek $\mathrm{End}_S(R)$ nebo je to polynom. Oba pohledy mají svá pro a proti. V práci se dále uvažuje $F(X)$ jako endomorfismus. V tom případě je potřeba velké opatrnosti při definici stupně. Množina $\mathrm{End}_S(R)$ je konečná, a proto jeden endomorfismus může mít nekonečně mnoho různých vyjádření ve tvaru $\sum_{i=0}^{d'} f_i \tau^i(X)$.
- Lemma 74, Claim 75: Zde nerozumím argumentaci - přijde mi, že je využíváno tvrzení typu, že monický linearizovaný polynom může poslat jednotku R bud' na jednotku R nebo na nulu, které mi není jasné.