Posudek vedoucího diplomové práce

Název: Kryptografické využití kódů nad Galoisovými okruhy
Autor: Marek Marko

Galoisovy okruhy, které jsou v předložené práci zavedeny jako lokální komutativní okruhy charakteristiky p^n a mohutnosti p^{nr} pro nějaké prvočíslo p, představují přirozené zobecnění pojmu konečného těles a nabízejí se jako zajímavá abeceda v obecnější verzi teorie lineárních kódů. Klasické kryptografické využití lineárních kódů představuje McElieceův kryptosystém, jehož variantu využívající kódy s metrikou danou hodností matic reprezentující kódová slova namísto standardní Hammingovy metriky publikoval v devadesátých letech Ernst Gabidulin.

Práce Marka Marko je motivována nedávnými pracemi, které Galoisovy okruhy využívají při zobecněnování Gabidulinovy varianty McElieceova kryptosystému, a primárně se zabývá algoritmickým přístupem při budování třídy kódů vhodných právě pro tuto kryptografickou aplikaci.

Samotný text sestává ze čtyř kapitol. První kapiotola detailně prezentuje konstrukci a popis obecného Galoisova okruhu pomocí Taichmüllerových množin, což následně umožní efektivní algoritmické uchopení kódů zavedených nad těmito okruhy. Druhá část textu se věnuje právě těmto kódům, zavedeným jako podmoduly konečně generovaných volných modulů nad Galoisovými okruhy. Třebaže jsou jejich mnohé vlastnosti známy dokonce v obecnějším kontextu modulů nad Frobeniovými okruhy je většina předvedených důkazů algoritmizovatelných a proto snadno využitelných při práci s konkrétní reprezentací těchto kódů. Třetí kapitola práce se zabývá kardinálně hodnostní metrikou (cardinal rank metric), která je zobecněním hodnostní metriky nad tělesem, jež v Gabidulinově konstrukci nahrazuje Hammingovu metriku. Závěrečná část textu se věnuje popisu protokolu zobecněné Gabidulinovy verze McElieceova schématu pro kódy s maximální vzdáleností danou kardinálně hodnostní metrikou a důkazu korektnosti tohoto schématu. Součástí práce je rovněž historický úvod, závěr a obsáhlý seznam použité notace.

Ačkoli práce vychází z několika nedávných článků, je primárně kompilační a nový návrh kryptosystému tudíž neobsahuje, je její podstatná část výsledkem samostatné studentovy práce, neboť na rozdíl od většiny využívané literatury nevychází z obecného teoretického popisu Frobeniových okruhů. Místo toho pracuje s algoritmickým uchopením užší třídy Galoisových okruhů, která využívá jejich prezentaci popsanou v první kapitole. Kromě toho autor vytvořil velké množství příkladů jednak ilustrujících vlastnosti využívaných struktur a především podobu prezentovaných schémat.

Text práce je napsán matematicky pečlivě, velmi dobrou angličtinou a přes některé značně technické partie se dobře čte. Až na tvrzení charakterizující Galoisovy okruhy (Theorem 10), důkaz žádného podstatného aspektu předvedené teorie nevynechává. Po formální stránce nemohu výslednému textu nic podstatného vytknout a drobné nedostatky, kterých jsem si v pracovních verzích práce povšiml, autor opravil. K předložené práci už tudíž nemám žádné matematické ani jazykové připomínky a domnívám se, že prokazuje autorovu schopnost samostatné odborné práce.

Z výše uvedených důvodů nepochybuji o tom, že předložená práce *Kryptografické využití kódů nad Galoisovými okruhy* úspěšně naplnila zadání a doporučuji ji uznat jako diplomovou.

Jan Žemlička
Katedra algebry
24.8.2024