Posudek vedoucího bakalářské práce

Název: Rychlé násobení v tělese $GF(2^n)$
Autor: Marek Bajtoš

Shrnutí obsahu práce

Předložená práce se zabývá otázkou efektivní reprezentace násobení v konečném tělese charakteristiky dva použitelné v zařízeních s omezenou výpočetní kapacitou. K tomuto účelu je v textu nejprve zavedena a diskutována maticová prezentace prvků zkoumané třídy těles nad dvouprvkovým tělesem, která umožňuje provést výpočet násobení daným prvkem s využitím minimálního možného počtu operací sčítání v prvotělese, tedy operací XOR. Jádrem práce je druhá kapitola textu, která srozumitelně prezentuje několik nedávných výsledků o reprezentovatelnosti prvků tělesa s násobením realizovatelným malým počtem binárních sčítání.

Celkové hodnocení práce

Téma práce. Téma práce bylo kompilační, od studenta vyžadovalo především porozumění odbornému článku, jeho zpracování, doplnění o netriviální detaily či příklady a zařazení do kontextu známé teorie konečných těles a lineární algebry. Téma bylo podle mého mínění vhodné pro zpracování v bakalářské práci pro obor Matematické metody informační bezpečnost.

Vlastní příspěvek. Hlavním zdrojem textu byla jediná stať z konferenčního sborníku, pro jejíž pochopení bylo třeba nastudovat některé pokročilejší partie z maticové algebry. Studentův hlavní přínos spočívá kromě několika ilustračních příkladů především v uceleném a dobře srozumitelném sepsání poznatků z teorie konečných těles, která se zdá být užitečná pro implementaci kryptografických algoritmů v zařízeních se zásadně omezenou výpočetní kapacitou. Nezanedbatelná část doplněné teorie zahrnuje důkazy, některé z důkazů snazších tvrzení jsou výsledkem studentovy samostatné práce (například důkaz Lemmatu 1.21).

Matematická úroveň. Matematická úroveň práce je uspokojivá a formulace jsou vesměs korektní. Přinejmenším nesrozumitelně ovšem občas působí některé komentáře, které v textu zřejmě nedopatřením zůstaly z pracovních verzí (například komentář za Větou 1.1).

Práce se zdroji. Ačkoli je práce kompilací, která sleduje strukturu hlavního zpracovávaného článku, díky doplnění argumentace a sjednocení terminologie s využitím další literatury není výsledný text na zdrojích formulačně závislý.

Formální úprava. Formální náležitosti práce nezasluhují žádné podstatnější výtky. Jazykových nepřesností je v textu množství přiměřené jeho rozsahu a text je přes některé nepříliš šťastné formulace, jejichž zamýšleným účelem bylo zřejmě usnadnit čtenářovo pochopení problematiky, poměrně čtivý.

Připomínky a otázky

S připomínkami a otázkami, které jsem vznášel průběžně k pracovním verzím textu, se student úspěšně vyrovnal. V předložené verzi práce jsem postřehl jen dva nedostatky:

1. strana 8: Vzhledem k tomu, že matice 0×0 v textu zřejmě nejsou uvažovány, mělo by být Lemma 1.19 formulováno nikoli pro nenulové, nýbrž pro nekonstantní polynomy.

2. strana 17: V důkazu Věty 2.4 je místo zavedeného značení $\mathbb{F}_2[A]$ využíváno nedefinované značení $\mathbb{F}_2(A)$.

Závěr

Práce podle mého názoru práce Marka Bajtoše Rychlé násobení v tělese $GF(2^n)$ splnila zadání a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace vedoucí práce sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
23.1.2018