Posudek vedoucího práce Filipa Kucky

Vítězslav Kala

13. června 2023

Bakalářská práce Filipa Kucky se věnuje zpracování zobecnění algoritmu RSA v číselných tělesech a zejména jeho reformulaci pomocí mřížek.

Jeho práci na tématu značně ztěžoval fakt, že výchozí článek (Zheng–Liu) je napsaný velmi nepřehledně až místy nekorektně, takže student musel doplňovat velkou řadu detailů a zpřesňovat různá tvrzení a definice. Přitom musel samostatně vypracovat řadu (spíše jednoduchých, ale ne zcela triviálních) důkazů.

Do jisté míry se mu to povedlo v tom smyslu, že výsledná práce je nepochybně lepší než původní článek, ale bohužel i tak má poměrně daleko ke korektnímu matematickému textu.

Práce je plná drobných chyb a nepřesností, včetně velkého množství překlepů a gramatických chyb. Jako jeden příklad zde např. uvedu, že hned v úvodu je zmiňován „RSA ploblém“.

Zásadnější jsou ale tyto nejasnosti v práci a chyby v důkazech (zmiňuji zde jen ty významnější):

1. Str. 4, komentář za větou 1.1.7. Obecně nemůžeme brát jako celistvou bázi $1, \theta, \dots, \theta^{n-1}$. Toto také mělo být vysvětleno (ale není) v kapitole 4, kde se pracuje za silného předpokladu, že $\mathcal{O}_K = \mathbb{Z}[\theta]$.

2. Důkaz lemmatu 1.1.8 není kompletní. Na závěr důkazu je také třeba zdůvodnit, proč $\mathbb{Z} \cap P \neq \mathbb{Z}$.

3. Poznámka 1.2.5 obsahuje vlastnosti týkající se ortogonální báze B^* (např. to, že jistá množina pokrývá celé $\mathbb{R}^n$), které nejsou vůbec očividné, a tedy by si zasloužily důkaz.

4. Důkaz věty 2.2.1, str. 11: není vysvětlený přechod od $\varphi(Q)$ k $\varphi(A)$ v exponentu a s tím související změna čísla k za jiné číslo.

5. Důkaz věty 2.3.1, část (1). Uvedený argument nedokazuje surjektivitu zobrazení ψ.

6. Důkaz věty 2.3.1, část (3). Je škoda, že důkaz není uvedený, tento důkaz není až tak složitý (jde jen o použití čínské zbytkové věty).

7. Str. 13, řádek 4 od konce. Rozhodně není pravda, že „ide iba o viacnásobné použitie klasického RSA“, protože násobení ve číselném tělese neprobíhá po složkách (jak je ve zbytku práce správně diskutované).

8. Důkaz tvrzení 2.4.2. Argument na začátku důkazu nedokazuje bijektivnost daného zobrazení (ta je ale očividná z definice).

9. Toto není vyloženě chyba, ale v celé kapitole 3 není potřeba předpokládat to, že prvek θ je celistvý.

10. Definice 3.2.4. V tuto chvíli nevíme, že násobení $\odot$ je asociativní, takže je třeba specifikovat uzávorkování v definici $f^{\odot n}$.

11. Úplný konec důkazu lemmatu 3.3.1. Tento argument nedokazuje surjektivitu zobrazení H^* (ta je ale jasná z definice).

12. Lemma 3.5.1, část 5. Zde je třeba předpokládat, že $m_\theta \nmid f$.

13. Lemma 3.5.1, konec důkazu části 3. Proč se v poslední rovnosti rovná $t_f(H)$ příslušnému součinu matic?

14. Věta 4.2.1. Zde použité značení $M_{\mathbb{Z}}^*$ nebylo definované. Dále, proč jsou v důkaze zmíněná zúžení skutečně bijekcemi?

15. Začátek sekce 4.3. Zobrazení Φ_q by si zasloužilo pořádnou definici.

16. Poslední řádek znění lemmatu 4.3.2. Co se zde myslí uvedeným součtem mřížek?

17. Lemma 4.4.1 a podobné úvahy by lépe zapadly do sekce 1.2, kde by vysvětlily, jak funguje báze B^*.

18. Důkaz věty 4.4.2 obsahuje několik chyb: Jednak zdůvodnění týkající se konečnosti $\mathbb{Z}^n/\mathcal{L}$ nefunguje, protože ne každá mřížka odpovídá nějakému ideálu. Dále uvedený argument nedokazuje surjektivitu zobrazení ψ.

19. V lemmatu 4.4.4 má nejspíš být, že danou množinou reprezentantů je $\tau^{-1}(S_{\alpha,\beta})$.

Práce také obsahuje některé neformální komentáře, které nedávají příliš dobrý smysl. Např.:

20. Str. 7. „Bez tejto podmienky by sme si museli celistvú bázu pre každé $\mathcal{O}_K$ vypočítat zvlášť.“

21. Str. 11. „V obecnom RSA je množinu reprezentantov $\mathbb{Z}/N\mathbb{Z} = \{0, \ldots, N-1\}$, čo je zároveň jediná možnosť.“

22. Str. 26. „V praxi teda nemáme žiadne obmedzenia a môžeme šifrovať slová ľubovoľnej dĺžky.“

Celkově je kapitola 3 v poměrně dobrém stavu a (vedle gramatických chyb) obsahuje jen pár zásadnějších problémů. Také kapitola 2 obsahuje jen relativně snadno opravitelné nedostatky. Naopak 4. kapitola a zejména sekce 4.4 není příliš dobrá. Konkrétně důkaz věty 4.4.2 (viz bod 18 výše) by stál za důkladné vysvětlení během obhajoby práce.

Práce obsahuje velkou řadu problémů. Zároveň ale její vypracování i do současného stavu zdaleka nebylo triviální. V případě zdárného průběhu obhajoby bych tedy doporučil práci přijmout jako bakalářskou práci a hodnotit ji známkou *dobře*.

Vítězslav Kala

Katedra algebry
MFF UK
Sokolovská 83
186 75 Praha 8

vitezslav.kala@matfyz.cuni.cz
https://www.karlin.mff.cuni.cz/~kala/web/