Posudok oponenta bakalárskej práce Filipa Kucky

Sára Šůstek Vyhnalová

6. 6. 2023

Predmetom práce Filipa Kucky je kryptografický algoritmus RSA na číselných telesách a jeho následné prepojenie so štruktúrou mriežok.

Táto práca je založená na článku od Zheng a Liu, ktorý je veľmi stručného formátu a v krátkom rozsahu popisuje rôznorodé neľahké matematické koncepty. Zameranie bakalárskej práce na rozšírenie a podrobnejšie spracovanie dôkazov a teórie uvedenej v článku, považujem za vhodné.

Práca obsahuje veľké množstvo gramatických chýb, preklepov a chýbajúcej interpunkcie, o čom svedčia napríklad chyby aj v samotnom abstrakte, napr.

- práca sa zaoberá algoritmom RSA popísaného - správne: RSA popísaným,
- mreižok má byť mriežok,
- venujeme sa dôkazu okruhovému izomorfizmu - správne: okruhového.

Celkovú štruktúra práce a členenie na kapitoly považujem za prehľadné, oceňujem postupné nabaľovanie teórie s vyústením do finálneho algoritmu v závere práce. Negatívnou výnimkou v štruktúre je jedine prvá kapitola, ktorá by si zaslúžila rozčlenenie viet a definícii do viacerých podsekcií a pridanie motivácie a komentárov, ktoré by čitateľa uviedli do kontextu, na čo konkrétne vety využijeme. Kapitola je, žiaľ, v stave Definícia - Veta - Veta, a tak dokola.

Pozitívne vnímam priložené príklady, ktoré nenásilnou formou ilustrujú definície, napr. príklad 3.2.3, príklad 3.2.5 a príklad v sekcii 5.2. Čitateľnosť dôkazov sa naprieč prácou rôzni. Celkovo za najkvalitnejšie spísanú považujem kapitolu 3.

Čo považujem za väčší nedostatok, je, že síce autor v úvode popísal, ktoré dôkazy sú vlastnou prácou, ale prevzaté vety nie sú dostatočne odcitované. V celom texte (s výnimkou prvej kapitoly) sa len zriedka objavil nejaký odkaz na zdroj danej vety a dôkazu. Napr. dôkaz Lemy 2.4.3 je len prekladom z pôvodného článku, ale nikde v kapitole to uvedené nie je. Medzi zmesou vlastných dôkazov a prevzatých sa orientácia čitateľa znižuje.

Mimo gramatických chýb sa v práci vyskytlo aj väčšie množstvo matematických nepresností, vyberám niektoré z nich:

1. S prvkom θ sa pracovalo nejednotne, napr. na str. 7 sa θ vyskytla bez zadefinovania, v sekcii 3.1 je uvedené, že θ je celistvý prvok (nad $\mathbb{Z}$), v kapitole 3.5 je $\theta \in K$ a neuvádza sa, že by šlo o celistvý prvok.
2. Vo vete 1.1.8 chýba uvedenie vzťahu medzi A a $\{\alpha_1, \ldots, \alpha_n\}$ ako $\{\alpha_1, \ldots, \alpha_n\} \subset A$.
3. Určité komentáre medzi vetami v prvej kapitole by si zaslúžili byť sformulované ako samostatné tvrdenia aj s odkazom na dôkaz, norma by mohla tiež byť súčasťou definície. Definíciu si zasluhuje aj pojem polootvorená množina z Poznámky 1.2.5.
4. V príklade 1.1.24 je uvedené, že $2 = (1+i)^2$ v $\mathbb{Z}[i]$. Rozklad $2 = -i(1+i)^2$.
5. Celkový pricíp dôkazu vety 2.2.1 je neprehľadný (hlavne jeho začiatok), v dôkaze sa vyskytol aj pojem najmenší spoločný deliteľ.
6. V práci sa vyskytujú nevhodné formulácie: pred vetou 2.3.1: ostáva bez dôkazu, pretože ide o zložitejšie tvrdenie (a nikde nie je uvedený odkaz na zdroj, kde by to bolo dokázané). Ďalej v dôkaze Lemy 3.3.2: pretože v indukčnom predpoklade vektor e_k nikdy nie je vektor e_n. Občas sa vyskytuje slovo "vidíme", kde by sa viac hodilo "z definície máme"a pod.
7. V rovnosti (2.2) na str. 13 nie sú popísané prvky α_i.

8. Chýba mi zdôvodnenie existencie bázy z A (odkaz na vetu 1.1.8.?)

9. Dôkaz v leme 3.3.1 je zakončený vetou H^* je surjektívne, pričom argument dokazoval iba vlastnosť prosté. Ďalej v Leme 3.3.3 uzátvorkovanie pri násobení matice a vektoru $H(e_k)$ znižuje prehľadnosť, pričom $H^*(e_k)$ je správne uzátvorkované.

10. Niektoré kroky v leme 3.4.3 by si zaslúžili dovysvetlenie. V predposlednom riadku je duplicitne $xt_a(x)$.

11. Sekcia 4.3 a práca s faktorokruhmi: v zobrazení v definícii 3.4.1 sa polynóm $m_\theta(x)$ vôbec nevyskytuje, v sekcii 4.3 sa síce vyskytuje, ale stále nie vo forme ideálu $(m_\theta(x))$.

12. Ako definujeme $\varphi(\alpha, \beta)$ v sekcii 4.5?

13. Kapitola 5: v kryptografickom algoritme správne definujeme verejný a súkromný kľúč (v jednotnom čísle), pričom každý z nich sa môže skladať z viacerých prvkov. V príklade na str. 33 je namiesto j uvedené v zátvorke i. Predposledný odsek na str. 33 nie je zrozumiteľný: "by sme si zvolili čísla", ale autor v ďalšej vete uvádza, že "pre tento prípad platí", akoby nešlo o možnosť voľby.

- Obecná poznámka k úprave a slovenčine: v definíciach chýba zvýraznenie pojmu pomocou *emph*, zjednodušila by sa tým čitateľnosť. Správne po slovensky je pomocné tvrdenie nazývané lema v ženskom rode, v práci sa to autorovi striedalo s českým označením lemma.

Predkladám k obhajobe bod 11. - dovysvetliť správnu interpretáciu oboch zobrazení vo vzťahu k faktorokruhu a naviac prosím o prehľadné odprezentovanie idey dôkazu vety 2.2.1 (bod 5).

Vzhľadom k tomu, že zameranie práce bolo zložitejšie a pokrývalo veľké množstvo netriviálnej teórie, ktorú si študent musel naštudovať, a keďže žiadnu nepresnosť nepovažujem za mimoriadne závažnú, odporúčam prácu prijať, aj napriek nedostatkom, ako prácu bakalársku. Návrh známky predložím predsedovi komisie pre obhajobu.