Posudek oponenta bakalářské práce

Název: Malé kořeny celočíselných polynomů více proměnných
Autor: Dora Todorovová

Shrnutí obsahu práce

Předložená práce se zabývá otázkou hledání kořenů celočíselných polynomů více proměnných s využitím redukované báze mřížky dané koeficienty těchto polynomů. Text sestává z úvodu, závěru a tří věcných kapitol. První část práce připomíná terminologii a základní fakta teorie mřížek včetně zjednodušené verze LLL-algortimus a nastiňuje Coppersmithovu metodu hledání kořenů celočíselných polynomů modulo přirozené číslo. V druhé kapitole je popsán postup na hledání kořenu polynomu dvou neurčitých citovaný z článku Dana Boneha a Glenna Durfee a poté obecný postup převzatý z práce Ellen Jochemszové a Alexandera Maye. Třetí kapitola ilustruje metodu na příkladech lineárního polynomu tří proměnných a kvadratického polynomu dvou proměnných $axy + bx + c$.

Celkové hodnocení práce

Téma práce. Téma práce bylo sice poměrně obtížné, neboť bylo založeno na teorii přednášené až v magisterském studiu. Samotná problematika je ovšem srozumitelná a zajímavá, proto jistě vhodná pro zpracování v bakalářské práci.

Vlastní příspěvek. První dvě kapitoly textu jsou čistě kompilační a vedle učebnice počítačové algebry zpracovávají bez výraznějšího vlastního přínosu části dvou článků. Vlastní studentčinou prací je především stručná třetí kapitola, která aplikuje popsanou metodu.

Matematická úroveň. První dvě části práce obsahují spíše hrubý popis metody bez podrobného zdůvodnění, které by rozšiřovalo argumentaci zpracovaných článků, formulace jsou občas bez nahlédnutí do zdrojových textů obtížně srozumitelné a není zcela jasné do jaké míry argumentaci rozuměla studentka. Občas je navíc nesprávně použita terminologie (viz níže). Aplikační třetí kapitola je ovšem přehledná a svědčí o autorčině pochopení problematiky.

Práce se zdroji. Práce využívá především tří zdrojů. Popis metody obsažený v druhé části práce je občas příliš blízký využívaným článkům, škoda je, že autorka neuvedla alespoň jiné příklady konstruovaných mřížek. Závěrečná kapitola je původní.

Formální úprava. Text se poměrně dobře čte, ačkoli obsahuje nezanedbatelné množství jazykových neobratností a nepřesností. Chybějící čárky znesnadňujé sruzumitelnost některých souvětí.

Připomínky a otázky

1. strana 6: Vynechání důkazu Tvrzení 6 by zasluhovalo nějaký komentář.
2. strana 8: U hodnot příkladu 2.1 by bylo vhodné uvést odkud je bereme, především, co jsou přirozená a co reálná čísla (například pro α nebo m to nemusí být na první pohled čtenáři jasné).
3. strana 10, řádek 1 (a níže): *dimenze* (pod)matice rozhodně není v souladu se standardní terminologií.

4. strana 12 (i jinde): Využití symbolu $\Rightarrow$ ve volném textu není vhodné.
5. strana 12, řádek -10: Proč by mělo být sporné nalezení faktorizace čísla N?
6. strana 14: Ve formulaci Lemmatu 8 není terminologicky vhodné mluvit o *řádu* sloupce.
7. strana 15, konec důkazu Lemmatu 9: Co znamená, že *Vzorec 2.1 zanedbává* $m - mn$?
8. strana 18: Na prvním řádku není dokončena druhá věta.

Závěr

Práce Dory Todorovové „Malé kořeny celočíselných polynomů více proměnných"přes uvedené výhrady splnila zadání a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
1.9.2020