Posudek oponenta bakalářské práce studentky Sáry Vyhnalové

Tomáš Vávra

Bakalářská práce *Solovay-Strassenův test prvočíselnosti* se zabývá pravděbodobnostními testy prvočíselnosti. Práce je rozdělena na tři kapitoly. V první kapitole, plně čerpající z literatury, studentka popisuje Solovay-Strassenův test založený na jisté identitě Legendrova symbolu. Druhá kapitola se zabývá výpočtem pravděpodobnosti, že přirozené číslo je prvočíslem, pokud test neselhal v daném počtu případů. První část druhé kapitoly čerpá z literatury, ve druhé části ale studentka přidá vlastní výpočet pravděpodobnosti za předpokladu, že zkoumané číslo není dělitelné danou množinou prvočísel.

Třetí kapitola obsahuje největší přínos autorky. Prvně je představen kvartický symbol, což je zobecnění Jacobiho symbolu v okruhu $\mathbb{Z}[i]$, a jeho vlastnosti. Provočísla tvaru $3 \mod 4$ zůstávají v $\mathbb{Z}[i]$ prvočiniteli, a proto pro ně bylo možno odvodit test analogický Solovay-Strassenovu. Nutno poznamenat, že tvrzení potřebná ke konstrukci testu založeném na kvartickém symbolu odvodila a dokázala studentka sama a nejsou triviální. Oceňuji, že je v celé práci jasné, jaké výsledky jsou převzaté a jaké originální.

Je škoda, že přestože se jedná o téma velmi praktické (pravděpodobná prvočísla se používají při šifrování metodou RSA), nepíše studentka nic o motivaci.

Chyb je v práci minimální množství, mám jen pár drobných připomínek.

- Na konci důkazu tvrzení 14 je uvedeno $|Ab_0| \geq |B|$ namísto $|Ab_0| \leq |B|$.
- V sekci 2.1 je pravděpodobnostní funkce zobrazení do **otevřeného** intervalu $(0, 1)$?
- Vnořené pozorování i s důkazem v rámci jiného důkazu (jako např. v tvrzení 31) mi přijde nešťastné.

Během obhajoby budu mít na studentku dva dotazy:

1. Jak si vede test založený na kvartickém symbolu v porovnání se Solovay-Strassenovým testem?
2. Máte nápad, jak se vypořádat s prvočísly tvaru $1 \mod 4$?

Protože nedostatky práce považuji za minimální vzhledem k dosaženým originálním výsledkům, navrhuji ji uznat jako bakalářskou a ohodnotit známkou *výborně*.

V Praze dne 12. 6. 2019

Ing. Tomáš Vávra, PhD.