POSUDEK DIPLOMOVÉ PRÁCE

Autor práce: Bc. Lukáš Langer
Název: Analýza algoritmu SQUFOF
Vedoucí: Jan Žemlička

Práce Lukáše Langera je věnována algoritmu známému pod zkratkou SQUFOF (Square form factorization), který pro faktorizaci přirozených čísel navrhl Daniel Shanks. Po historické a motivační úvodní kapitole se pokouší nejrozsáhlejší druhá kapitola o podrobnou analýzu fungování algoritmu, která je opřena o velmi netriviální poznatky z algebraické teorie čísel. K tomuto účelu jsou v této části v různé míře podrobnosti postupně představena potřebná fakta o periodických řetězových zlomcích, o kvadratických formách na celých číslech, o ideálech okruhů algebraických celých čísel $\mathbb{Z}[\sqrt{N}]$ a o mřížích ranku 2. Část výsledků je prezentována s důkazem, u části je důkaz s ohledem na očekávaný rozsah práce vynechán nebo nahrazen jeho náznakem. Třetí kapitola obsahuje komentář dvou variant algoritmu SQUFOF a závěrečná část práce srovnává výsledky měření rychlosti studentovy implementace algoritmu SQUFOF s implementací téhož algoritmu a implementací kvadratického síta z dostupných knihoven.

Text nese především kompilační charakter, ovšem vzhledem k obtížnosti a rozsahu potřebné teorie, nešlo o snadný úkol. Nejpodstatnějším studentovým přínosem k tématu je vedle ilustračních příkladů k prezentovaným pojmům především měření na několika implementacích algoritmu SQUFOF a kvadratického síta a komentování naměřených hodnot. Ačkoli je práce napsána poměrně kultivovaně, její čtení neusnadňuje fakt, že se autorovi ne vždy daří srozumitelně zavést potřebnou terminologii, případně jasně vysvětlit deklarované vlastnosti. Podobně ztěžuje porozumění občasné využívání pojmů a konceptů zavedených teprve v následujících partiích. Přesto výsledný text podle mého názoru svědčí o autorově vhledu do zkoumané problematiky a schopnost samostatné odborné práce. Množství zjevných matematických omylů a nepřesností je podle mého mínění přijatelné (výběrový seznam viz níže), škoda jen, že si čtenář ke správnému pochopení často musí domýšlet kontext. Hodnotu a pravděpodobně i srozumitelnost práce by rovněž významně zvýšilo, kdyby se studentu podařilo zpracovat prezentovanou teorii včetně podrobné a úplné argumentace.

Přes uvedené nedostatky práce Lukáše Langera *Analýza algoritmu SQUFOF* podle mého mínění naplnila zadání a doporučuji ji uznat jako diplomovou.

v Praze 31.8.2016 Jan Žemlička

Připomínky a otázky:

- s.6, před (2.1) by stálo za to zdůraznit, že pracujeme s bezčtvercovým přirozeným N;

- s.6-7, myslím, že není šťastné připouštět za x_0 hodnotu jinou než $\sqrt{N}$;

- s.11, důkaz Věty 4 s využitím vztahu z [Rie85, A8.12 a A8.13] není příliš poctivý;

- s.15, *Poznámka* mluví o dosud nezavedených pojmech forma a střed symetrie;

- s.16, co znamená formulace ,,pokud se oba společně vyskytují v rozvoji řetězového zlomku" v definici $\mathbb{T}^*$?

- s.16, formulace ani důkaz Lemmatu 10 není srozumitelný: co například znamená ,,x_0 můžeme redukovat" nebo ,,vrátíme se zpět k standardnímu zápisu pro b_r"?

- s.16, Co ilustruje Příklad 6?

- s.17, místo ,,zobrazení není jednoznačné" bychom měli říct zobrazení není jednoznačně určené,

- s.18, ve výrazu $ad - bc = \pm 1$ chybí rovnítko;

- s.19, co má tvrdit Lemma 11? (z důkazu se zdá, že tvrzení k/Δ);

- s.20, to, že jsou formy f a $p(f)$ ekvivalentní nepatří do definice. A odkud to vlastně víme?

- s.21, Lemma 13 je ve zjevném rozporu s následným komentářem (redukce neredukované formy by nebyla redukovaná);

- s.21, Definice 14 obsahuje a vyžaduje několik (netriviálních) tvrzení;

- s.22, Proč stačí v důkazu Lemmatu 15 dokázat $\Phi_{\mathbb{F},\mathbb{T}}\Phi_{\mathbb{T},\mathbb{F}} = id$ (a nepotřebujeme obráceně $\Phi_{\mathbb{T},\mathbb{F}}\Phi_{\mathbb{F},\mathbb{T}} = id$)?

- s.25, odkud víme, že je forma z Definice 18 jednoznačně určená?

- s.29, odkud víme, že jsou zobrazení $\Phi_{\mathbb{F},\mathbb{I}}$ a $\Phi_{\mathbb{I},\mathbb{F}}$ (respektive $\Phi_{\mathbb{T},\mathbb{I}}$ a $\Phi_{\mathbb{I},\mathbb{T}}$) vzájemně inverzní?

- s.43 stálo by za to podrobněji vysvětlit, z čeho plyne korespondence skládání forem a násobení ideálů.