Posudek vedoucího diplomové práce
Prosívání ve faktorizačních algoritmech
Samuela Staška

Cílem práce bylo porozumět (často heuristickým) argumentům používaným při odhadu složitosti kvadratického a číselného síta do té míry, že bude možné provést podobný odhad pro víceméně libovolný faktorizační algoritmus, který bude nějak implementovat prosívací fázi. Takový algoritmus vždy bude záviset na několika parametrech, které je potřeba vhodně nastavit. Doufal jsem, že studiem několika konkrétních případů bude možné v ideálním případě navrhnout obecný postup, který by tyto parametry nastavil.

Primárně tedy nešlo o studium a vylepšování známých výsledků o složitosti kvadratického a číselného síta, takový cíl se mi zdál příliš ambiciózní. Nicméně nastudování základních přístupů k těmto odhadům bylo nutnou podmínkou pro zvládnutí práce.

V první kapitole autor poměrně detailně zpracoval složitost kvadratického síta podle knihy Crandall, Pomerance *Prime numbers, a computational perspective*. Samostatně se pak pokusil diskutovat varianty MPQS a variantu kvadratického síta s jedním velkým prvočíslem. Sám pak navrhl variantu MPQS s jednoduchou inicializací polynomů. V této variantě se podrobně zabýval problémem opakujících se hladkých relací, které představují problém pro lineární fázi algoritmu. Vzorce odvozené na straně 19 se ukázaly být příliš komplikované pro stanovení parametru c, který je třeba pro inicializaci algoritmu. Autor na základě experimentů na výpočetně dostupných datech navrhl alternativní metody volby tohoto paramteru. Byl také schopen vysvětlit některé 'anomálie' v datech na str. 21 - 24. Experimenty ukazují že by navržená varianta mohla při srovnatelné délce prosívacích intervalů poskytnout více unikátních hladkých relací než standardní kvadratické síto. Tento fakt se bohužel nepodařilo prokázat.

Druhá kapitola je věnována číselnému sítu. Opět je proveden odhad složitosti základního algoritmu podle článku Buhler, Lenstra, Pomerance: Factoring integers with the number field sieve a je diskutováno doplnění o kvadratické charaktery z hlediska složitosti. Hlavní náplň kapitoly pak je podrobnější výpočet složitosti variant z Coppersmithova článku *Modifications to the number field sieve*. Coppersmitova metoda byla dále zkoumána v modifikaci, kdy je část výpočtu paralelizovaná (2.3.3). Tím, že se měnila část algoritmu, která nemá asymptoticky dominantní složitost, nedojde k vylepšení odhadu složitosti. Autor ale dokázal kvantifikovat přínos paralelizace.

Závěrečná část je věnována randomizovanému číselnému sítu. Tento algoritmus, který pubikovali Lee a Venkatesan v Journal of Number Theory v roce 2018, představuje variantu, pro kterou je možno stanovit rigorózně složitost v průměrném případu. Původní článek je poměrně dlouhý a komplikovaný, úkolem autora bylo vystihnout hlavní rozdíl proti klasickému číselnému sítu a přiblížit hlavní myšlenky rigorózního důkazu složitosti. Nad rámec tohoto zadání byla v kapitole 2.4.3 provedena randomizace Coppersmithovy metody, která nebyla v originálním článku detailně rozpracovaná.

Celkově jsem s prací autora spokojen, Samuel zvládl pochopit poměrně

obtízné téma do té míry, že byl schopen samostatně navrhnout parametry pro různé varianty číselného síta, což byl hlavní cíl. Problémy, na které jsem poukázal, byl schopen samostatně odstranit. Bohužel jsem si nevšiml problému při kvantifikaci přínosu varianty s velkým prvočíslem (str. 12), kde nejspíš byl započítán přínos pouze jednoho velkého prvočísla.

Práce je napsána srozumitelně, ale není členěna standarním stylem tvrzení - důkaz. Což je při používání heuristických argumentů, či různých zjednodušování výrazů ve výpočtech asi na místě, ale čtenář se pak v textu hůře orientuje.

Přestože autor provedl samostatně řadu netriviálních výpočtů, je celkový charakter práce spíš kompilační. To je částečně též způsobeno zadáním tématu, kdy jsem si od některých modifikací číselného síta sliboval víc, než mohly reálně nabídnout.

Z výše uvedených důvodů navrhuji předloženou práci uznat jako práci diplomovou.

V Praze, 29. 1. 2023,

Pavel Příhoda