Posudek oponenta k diplomové práci
Podpůrné algoritmy číselného síta
Adély Skokové

Číselné síto je dnes asymptoticky nejrychlejší známý (nekvantový) algoritmus pro faktorizaci složeného čísla. Implementace jednotlivých fází síta má zásadní vliv na běh celého algoritmu. Předložená práce se zabývá úvodní fází, volbou polynomů se kterými bude dále algoritmus pracovat.

Po úvodní kapitole následuje stručný přehled pojmů a vět z algebraické teorie čísel, které algoritmus číselného síta využívá. Třetí kapitola pak obsahuje hrubý popis celého faktorizačního algoritmu. Těžiště práce je pak v kapitolách 4 a 5, které popisují, jak poznat, že vygenerované polynomy jsou vhodné pro prosívací fázi a jsou detailně popsány 2 algoritmy Thorstena Kleinjunga pro generování polynomů. Druhý algoritmus byl využit při rekordní faktorizaci RSA 768. Proti předchozí verzi, byla práce doplněna o implementaci druhého Kleinjungova algoritmu, kterou autorka testovala na číslech o velikosti 110 a 120 cifer, nalezené polynomy byly srovnávány Murphyho funkcí α.

Práce je po formální a jazykové stránce napsána velmi dobře, větší množství překlepů se vyskytuje až v samém závěru práce (sekce 5.6.1). Je dále třeba uvést, že oblast faktorizačních algoritmů má blíže k experimentálním přírodním vědám než k formálně přesné matematice (C. Pomerance v článku *A Tale of Two Sieves* zmiňuje H. Lenstru, kterému rigorózní teoretické úvahy o faktorizačních algoritmech připomínají 'pig in the rose garden'), není proto jednoduché napsat na takové téma práci, která by byla matematicky zcela korektní.

Přesto si myslím, že alespoň v rámci druhé kapitoly mohla být autorka zcela precizní. Kapitola však obsahuje řadu drobných nepřesností a nedostatků, uvedu jen některé, protože druhá kapitola není pro algoritmy páté kapitoly zásadní.

- V Příkladu 2.2.12 se uvádí $O_K = \mathbb{Z}[\frac{1}{2}, \sqrt{c}]$, což je poněkud v rozporu s Příkladem 2.2.6, kde je uvedeno, že $\mathbb{Z}$ je celistvě uzavřený.
- V důkazu Hlavního tvrzení 2.3.5 chybí důkaz faktu, že existuje baze $\{\beta_1, \ldots, \beta_n\}$, pro kterou bude platit $O_K \subseteq \oplus_{i=1}^{n} \beta_i \mathbb{Z}$, což je v důkazu nejtěžší krok.
- Pokud na straně 25 hledáme lineární kombinaci řádků matice $\mathbf{M}$, která dá nulový vektor, neřešíme soustavu $\mathbf{M}\mathbf{x}^T = 0$ ale soustavu $\mathbf{x}\mathbf{M} = 0$.

Argumenty kapitol 4 a 5 jsou spíše heuristické, přesto si myslím, že autorka se mohla pokusit některé věci vysvětlit lépe. Podle mého názoru k implementování Kleinjungova algoritmu bylo potřeba daleko lepší pochopení látky než je předvedeno v textu páté kapitoly.

- Z textu není jasné, zda vzorce na straně 35 nahoře Dickmanovu funkci určují. Uvedené ohodnocení pomocí vzorce s integrály mohlo být nějak okomentováno, co ten integrál vlastně počítá?
- Ze vzorce pro $\sup(f)$ na str. 36 by pro $f = x$ by $\sup(f)$ pro $d \geq 3$ neexistovalo.
- V Tvrzení 5.5.1 se vyskytuje izolovaně slovo Necht'. Možná tam chybí předpoklad, který by osvětlil úvahu na straně 49 nahoře.
- V Tvrzení 5.5.3. má asi být u definice $a_{i,max}$ v exponentu $i - \frac{d}{2}$.
- Popis algoritmu na straně 52 mi přijde nesrozumitelný. Podle všeho potřebujeme hodnoty $a_{d-1,(1,\ldots,1,j,1,\ldots,1)}$, pomocí nich definujeme $e_{i,j}$ a pomocí $e_{i,j}$ nakonec definujeme $a_{d-1,\mu}$. Pokud je tomu tak, jak získáme hodnoty $a_{d-1,(1,\ldots,1,j,1,\ldots,1)}$?
- Jaký je význam poznámky v prvním odstavci na straně 53?
- U výsledků na straně 63 se uvádí, že velikost posledních dvou koeficientů už neodpovídá velikosti m, což je hezky vidět zejména na druhém polynomu. Není mi jasné, jak je to s koeficientem u x^2. Tvrzení 5.6.1. dává odhad pro koeficient u x^3.
- Bylo by jistě zajímavé a čtenářsky atraktivní uvést, zda došlo k nějakému zásadnímu zrychlení implementace číselného síta na přiloženém CD po změně algoritmu pro volbu polynomu.

- Způsob důkazu Tvrzení 5.5.4. zdá se mi poněkud nešt'astným.

Matematická úroveň předloženého textu je slabší, za zásadní ale považuji naimplementování algoritmu a provedené měření. Práci proto považuji za přínosnou a doporučuji uznat jako diplomovou.

V Praze, 5. 6. 2015

Pavel Příhoda