Posudek oponenta k diplomové práci
Podpůrné algoritmy číselného síta
Adély Skokové

Číselné síto je v současnosti asymptoticky nejrychlejší (veřejně) známý algoritmus pro číselné faktorizace. Algoritmus sestává z několika fází, v podstatě každá z nich se může stát úzkým hrdlem algoritmu, pokud by byla implementována bez nějaké další optimalizace. Předložená práce se zabývá optimalizací volby polynomu, který je použit pro konstrukci číselného tělesa.

Text je rozdělen do pěti kapitol, krátkého úvodu, shrnutí potřebných pojmů z algebraické teorie čísel, stručného popisu jednotlivých fází číselného síta a dvou kapitol věnovaných volbě polynomu, zejména dvěma algoritmům T. Kleinjunga.

Práce je převážně kompilačního charakteru, je docela dobře logicky rozčleněná, obsahuje minimum překlepů. Bohužel obsahuje poměrně značné množství nepřesností, případně nepřesvědčivých důkazů.

Kapitola 2 obsahuje látku probíranou ve standardních kurzech na MFF UK, proto si myslím, že měla být pojata podstatně stručněji a raději bez důkazů. Nebudu ji proto hodnotit podrobněji.

Kapitola 3 je docela dobrá, ale tvrzení 'součin hlavních ideálů nemusí být hlavní ideál' (str. 28) v kontextu komutativních okruhů neplatí, na straně 29 má být místo $y^d f_i(x, y) = F_i(x, y)$ asi $y^d f_i(x/y) = F_i(x, y)$.

Kapitola 4: V Tvrzení 4.1 máme determinant matice $\mathbf{M}$ stupně $d+1$, determinanty menších matic jsou proto stupně d. V matici $\mathbf{M}$ má být vpravo dole $a+ba_d$. V Tvrzení 4.2 vypadla absolutní hodnota. Pojem zkosení intervalu není dostatečně vysvětlen, také by nebylo špatné říct něco k tomu, jak velký by měl prosévací interval být. Problematická je pasáž 4.3.1 o hodnocení koeficientů. Mělo by být zdůvodněno, proč $\sup(f)$ existuje. Dále se ukazuje, že $\sup(f, s)$ je norma. V důkazu trojúhelníkové nerovnosti mi není jasné, co se stane, pokud stupeň $f + g$ bude menší než stupeň f i stupeň g. Následující část 4.3.2 jsem moc nepochopil, ale možná není chyba na straně autorky.

Kapitola 5 je klíčová část práce, podle mě mohla být rozebrána podrobněji. Zejména orientace ve značení na straně 51 a 52 je docela obtížná. Zde by bylo žádoucí uvést konkrétní příklad. V Tvrzení 5.2 na straně 48 dole se argumentuje asi nějakou heuristikou, důkaz je přinejmenším nejasný. Dále aplikace Tvrzení 5.2 v Tvrzení 5.3 je problematická, někam se vypařil předpoklad o nabývání supnormy v j-té souřadnici. Důkaz Tvrzení 5.4 vzbuzuje pochybnosti. Kongruence $p_i \equiv 1 \pmod{d}$ způsobuje, že $x^d - 1$ bude mít v $\mathbb{Z}_{p_i}[x]$ právě d kořenů. Tento fakt není v důkazu zmíněn, vypadá to jako bychom předpoklad mohli nahradit $d < p_i$, pak by ale tvrzení neplatilo. Dále by nebylo špatné vysvětlit, v čem spočívá přínos druhého Kleinjungova algoritmu proti prvnímu.

Celkově práce nepůsobí špatným dojmem, většinu chyb by nemělo být těžké opravit. Věcných chyb či nepřesností je ale přece jenom trochu moc. Pokud by součástí řešení byla implementace a třeba nějaké experimenty se vstupními parametry, daly by se výše uvedené nedostatky odpustit. Na kompilační text jsou logicky nároky poněkud vyšší, předloženou práci proto nedoporučuji uznat jako diplomovou.

Ve vlaku, 6. 9. 2013

Pavel Příhoda