Posudek oponenta diplomové práce
Generování polynomů pro číselné síto
Anežky Pejlové

Předložená práce se zabývá metodami výběru vhodných polynomů pro faktorizační algoritmus číselné síto. Volba polynomu je pro efektivitu algoritmu klíčová, jde tedy o dost podstatné téma.

Vlastní práce je rozdělena do šesti kapitol, v první jsou shrnuty základní pojmy, je zde také pečlivěji rozepsán důkaz věty Buhlera, Lenstry a Pomerance o asymptotickém chování de Bruijnovy funkce (Věta 3).

Kapitola 3 pak popisuje algoritmy pro generování polynomů base-m a base-(m, p) metodou, je zde též solidně popsán Kleinjungův algoritmus. Tento algoritmus vygeneruje větší množství polynomů použitelných pro číselné síto. Metodami, jak tyto polynomy ohodnotit z hlediska vhodnosti pro prosívací fázi síta, se zabývá čtvrtá kapitola. Jsou zde představena kriteria označovaná jako 'velikost koeficientů' a 'kořenové vlastnosti'. První z nich aproximuje počet hladkých relací pomocí Dickmanovy funkce (vzorec 4.1). V této části modifikovala autorka přístup z Murphyho disertace tak, aby byl vhodný pro base-(m, p) metodu. Dále je zde velice hezky diskutována volba stupně nelineárního polynomu. Sekci 4.1.3 jsem bohužel moc nepochopil, základní myšlenka je maximalizace přínosu jednotlivých prvočísel ve faktorizační bázi.

Pátá kapitola se zabývá kořenovým sítem, což je metoda, jak vylepšit kořenové vlastnosti bez toho, že by se nějak zásadně změnila velikost koeficientů. Je zde navržena optimalizace kořenového síta (sekce 5.2).

Poslední kapitola diskutuje určité implementační aspekty a obsahuje výsledky experimentu, kdy autorka zjišťuje, jak se lišilo seřazení sady vygenerovaných polynomů pomocí různých přístupů.

Práce je napsána velice hezky a obsahuje řadu zajímavých nápadů. Mám několik nejasností, možná způsobených především nedostatkem času na zpracování posudku. Text obsahuje dále několik drobných chybiček, uvádím alespoň některé.

- str. 5 Do funkce ψ dosazujeme (minimálně ve druhém argumentu) obecně kladné reálné hodnoty, to by měla definice zohledňovat.
- str. 8 Funkce $\sqrt{\frac{\ln x}{\ln\ln x}}$ je rostoucí ještě nezaručuje, že přeroste $\beta^{-1}/(1-\varepsilon)$
- str. 10 Místo $y = L_x[\theta]$ má být $y = L_x[1/2, \theta]$.
- str. 16 nahoře: Bude zobrazení ϕ korektně definováno, když polynom f nebude primitivní?
- str. 17: Ve druhém bodu Věty 10 mají být prvoideály stupně 1.
- str. 22 nahoře: Rozklad $N = f_1(m)f_2(m)$ by nemusel dát hledanou faktorizaci N.
- str. 24, Algoritmus 3.1, krok 7: Podle všeho δ nemusí být celé číslo (viz str 68,69)
- str. 25, Věta 14: Prvočísla $p_1, \ldots, p_l$ asi mají být po dvou různá.
- str. 27: Způsob, jakým se nakládá s p ve jmenovateli, se mi moc nezdá. Konkrétně se mi zdá problematický přechod od (3.5) k následující kongruenci.
- str. 40, dole: asi má být $|c_i| \leq m + p$ (soudě dle Věty 13)
- str. 48, Definice 11: Jaký pravděpodobnostní prostor vlastně uvažujeme, jak si uvednou střední hodnotu představit?
- str. 49 množina $\cup_{i=1}^{k} A_k$ není množina násobků b, ale množina všech soudělných čísel s b v množině D_n.
- str. 49, Definice 13: Co je ϕ a jaká jsou na něj omezení? Tato část práce si asi zasloužila podrobnější rozpracování.

- str. 50: Jak se v důkazu Tvrzení 24 dostane rovnost

$$\sum_{k=1}^{\infty} |\{v \in \mathrm{Im}(\phi) : \pi_{p^k}(v) = 0\}| = \sum_{k=1}^{\infty} |\{w \in \pi_{p^k}(M) : \phi_{p^k}(w) = 0\}| \,?$$

- str. 51: Je význam výrazu nespeciální prvočíslo v Tvrzení 25 stejný jako v Definici 4? Pokud ano, kde je tento předpoklad využit?
- str. 52 b): Zde máme $p|b$, $c \equiv (b/a) \bmod p^k$. Jak se pak vyrovnat s výrazem $c^d f(\frac{1}{c}) \equiv 0 \bmod p^k$.
- str. 53, obrázek 4.7: Je v levém dolním rohu $\mathbb{Z}_{p^k}$ nebo $\mathbb{Z}_{p^k}^l$?
- str. 62: Přijde mi, že odhad složitosti z Lemmatu 29 nezahrnuje, že počet zvednutí násobných kořenů může se zvětšujícím se k růst (viz Lemma 9 (2)).
- str. 71: Vzorce pro výpočet $c_i^{(k)}$ nesedí se vzorci ze str. 70 dole. $c_i^{(0)} = 0$ pro $i > 0$.

Celkově práci považuji za kvalitní a doporučuji uznat jako práci diplomovou.

V Praze, 9. 6. 2016

Pavel Příhoda