Posudek oponenta k diplomové práci
Analýza algoritmu SQUFOF
Lukáše Langera

Předložená práce se zabývá faktorizačním algoritmem SQUFOF. Tento algoritmus navržený Danielem Shanksem využívá vztahu třídové grupy kvadratického tělesa a tříd ekvivalence kvadratických forem daného diskriminantu. Algoritmus v určitém směru také rozvíjí algoritmus CFRAC. Práce se proto zabývá řetězovými rozvoji kvadratických čísel a jejich vztahu ke kvadratickým formám, vztahu kvadratických forem daného diskriminantu a ideálů v odpovídajícím rozšíření celých čísel a vztahu těchto ideálů a speciálních mříží v $\mathbb{R}^2$.

Třetí kapitola představuje vlastní algoritmus SQUFOF a jeho různá vylepšení.

V poslední kapitole pak autor prezentuje porovnání výkonu vlastní implementace algoritmu, optimalizované verze SQUFOF implementované v PSIQS Java pacakge a kvadratického síta.

Téma práce považuji za velmi náročné po teoretické stránce, není vůbec na škodu, že se řada technicky obtížných tvrzení uvádí bez důkazu. Za asi největší problém v práci považuju často nedostatečné zavedení klíčových pojmů. V některých případech jsem asi dokázal odhadnout, jak to bylo myšleno v dalších pasážích práce, některá tvrzení jsem však nedokázal pochopit. Tím nechci tvrdit, že chyba je nutně na straně autora, přesto se mi zdá, že práci by prospělo lepší promyšlení, na které aspekty teorie se podrobněji zaměřit. Text obsahuje také vzhledem k rozsahu práce snesitelné množství překlepů, některé uvádím níže.

Práci Lukáše Langera doporučuji uznat jako diplomovou.

V Praze 1. 9. 2016

Pavel Příhoda

Konkrétní připomínky k práci:

- Na straně 7 je kolize značení u x_0 vztah (2.6) a vztah (2.4) a u P_{-1} vztah (2.8) a (2.5). Pak není moc jasné, co se vlastně snaží Věta 1 dokázat.
- str. 8, důkaz b) místo $P_{i-1} = b_{i+1}Q_{i+1} - P_i$ má být $P_{i+1} = b_{i+1}Q_{i+1} - P_i$; konec důkazu c) má asi být P_{i-1} místo P_{-1} a Q_i místo Q_0; důkaz d)e) Je zde předpoklad $Q_i > 0$, který není dokázán.
- str. 9 3. řádek má začínat $b_i(\sqrt{N} + P_i) - P_i$
- str. 9 g) je dle všeho (2.9)
- str. 10 asi má být, že každé x_i lze napsat ve tvaru $\frac{\sqrt{N}+P_{i-1}}{Q_i}$
- str. 10 důkaz tvrzení 2: místo $\frac{b_1B_0+1}{b_1}$ má být $\frac{b_0b_1+1}{b_1}$
- str. 11 V důkazu Věty 4 má být $x_i = \frac{\sqrt{N}+P_{i-1}}{Q_i}$ místo $x_i = \frac{\sqrt{N}+P_i}{Q_i}$; člen $NB_{i-1}^2A_{i-1}^2$ na konci důkazu má být $NB_{i-1}^2 - A_{i-1}^2$.
- str. 15, důkaz Věty 9: Perioda π byla zavedena jako perioda posloupnosti $\{x_i\}$ v důkazu je však využívána jako perioda posloupnosti $\{Q_i\}$.
- str. 15 vzhledem k určitým nejasnostem ve značení (viz první připomínka) není úplně jasné, která čísla tvoří množinu $\mathbb{T}$. Indexy u členů P_i, Q_i dávají asi seskupení prvků $\mathbb{T}$ do posloupností a toto seskupování definuje ekvivalenci na $\mathbb{T}^*$. Vzhledem k tomu, že se jedná klíčové pojmy práce, považuji zde uvedené vysvětlení za nedostatečné.
- str. 19, Definice 7: Nejsem si jistý, jestli zde uvedená definice grupy $PSL_2(\mathbb{Z})$ je standardní. Zde uvedenou grupu bych asi označil jako $GL_2(\mathbb{Z})$.

- v Poznámce na straně 19 má být $(a, b + 2na, an^2 + nb + c) \sim (a, b, c)$.
- Definice 9,10 na straně 19 zdánlivě(?) představují nejednoznačnou definici nejednoznačné formy
- Lemma 11 slibuje něco jiného než je dokázáno
- Lemma 13 na str. 21 by znamenalo, že redukčním operátorem nezredukujeme formu
- Definice 14: Zdá se, že redukované ekvivalentní formy rovnáme do posloupnosti pomocí operátoru ϱ. Pokud je tomu tak, mělo by to být zdůrazněno.
- str. 22 Pokud nebylo jasné, co je vlastně množina $\mathbb{T}$, množina $\mathbb{F}$ asi není pro jistotu definována vůbec.
- str. 22 Δ by mělo být celé číslo, nemůže jít o prvek $\mathbb{T}$.
- str. 22 Proč se v důkazu Lemmatu 15 nedokazuje, že $\Phi_{\mathbb{T},\mathbb{F}}\Phi_{\mathbb{F},\mathbb{T}}$ je identita?
- str. 23 Nepodařilo se mi pochopit druhou část důkazu Věty 16.
- str. 24 Definice 17 - abychom mohli mluvit o grupě, potřebujeme nejen koreknost binární operace, ale také asociativitu skládání a jednotku. Asi mohlo být ověřeno, že třída ekvivalence hlavní formy tvoří jednotku grupy.
- str. 24 V Lemmatu 18 se operuje s pojmem středu symetrie třídy ekvivalence forem. Tento pojem podle mě není v práci zadefinován.
- str. 28 Ve vztahu definujícím $\overline{\xi}$ by mělo být uvedeno, z jakých oborů jsou α, β.
- V důkazu Lemmatu 21 na str. 28 je implikace $s|Q, Q|\mathcal{N}(s\sqrt{N} + P) \Rightarrow s|P$. Zde je mi jasné pouze $s|P^2$, pro $s|P$ lze ale využít jinou argumentaci.
- str. 29 Pokud věta pod důkazem Lemmatu 21 definuje primitivní ideál, mohlo by to být napsáno lépe.
- str. 30 Vektory $\langle \alpha_i \rangle$ by měly být lineárně nezávislé, podobně jako vektory $\langle \beta_i \rangle$. Taky by nebylo od věci napsat, z jakého vektorového prostoru tyto prvky jsou.
- str. 30 V příkladě 10 má místo $\sqrt{133}$ být $\sqrt{113}$.
- str. 35 Ve vztahu (2.30) by mělo místo s^2 být s.
- str. 37 Jak interpretovat relaci $n\mathcal{L} \subseteq \mathbb{Z}[\sqrt{N}]$ v (2.31), pokud je $\mathcal{L} \subseteq \mathbb{Q}[\sqrt{N}] \times \mathbb{Q}[\sqrt{N}]$?
- str. 38 Není mi jasná argumentace v závěru důkazu Věty 24.
- str. 42 Ve výrazu $\frac{L(H_k)L(K_j)s\mu_n\phi_m t}{\lambda_j L(H_1)}$ by asi t mělo být ve jmenovateli.
- Ve třetí kapitole bych uvítal větší provázanost textu s teorií z předešlé kapitoly. Proč je např. možné nalézt i, pro které je Q_i čtverec?
- str. 44 Odkud se vzalo 224 v příkladu na výpočet inverzu odmocniny čtvercové formy?