Posudek oponenta bakalářské práce
Srovnání základních algoritmů pro problém diskrétního logaritmu
Michaely Kučerové

Diskrétním logaritmem v cyklické grupě G s generátorem α rozumíme následující problém: Pro dané $\beta \in G$ najdi $x \in \{0, \ldots, |G|-1\}$ tak, aby $\alpha^x = \beta$. Je známo, že problém diskrétního logaritmu nelze v této obecnosti řešit dostatečně efektivně. Pro praktické využití se však vždy musíme omezit na nějakou použitelnou realizaci cyklických grup. V této práci jsou to multiplikativní grupy p-prvkového tělesa a grupy bodů na eliptických křivkách nad konečným tělesem. Pro tyto případy není známo efektivní řešení problému diskrétního logaritmu. Předložená práce vysvětluje některé metody, které lze pro řešení problému diskrétního logaritmu použít. Jsou to baby-step giant-step, Pollardova ϱ-metoda, Pollardova λ-metoda, indexový kalkulus a Pohlig-Hellmanova redukce problému na grupy prvočíselného řádu. U každé metody je ukázán konkrétní příklad, je uvedena (často i dokázána) časová i paměťová složitost. Některé z těchto metod byly naimplementovány a byla změřena jejich složitost z hlediska počtu grupových operací a počtu procesorových instrukcí.

Práce je napsána pečlivě a srozumitelně. Za větší nedostatek považuji kroky 2. a 3. Příkladu 38, které nejsou napsané správně (výsledek ale správný je). Dále mi chybí vysvětlení, jak budeme řešit soustavu kongruencí v Algoritmu 3.5. Pak už jen drobnosti: V Poznámce 17 bych uvedl, proč dává $z^{-1} \bmod d$ smysl, první věta druhé kapitoly je bez vysvětlení slova bezpečný docela odvážná. V Definici 23 bych definoval operaci $-$ explicitně. Pojem paměťové složitosti se mi nezdá dost vysvětlený - podíváme-li se na Fakt 37, má Pollardovo ϱ složitost $O(1)$, přitom s rostoucím d by měla růst i náročnost na uložení jednoho prvku grupy. V Příkladu 30 je rychlejší počítat 5^{-11} jako inverz $5 * (5^{10})$. Výraz $(\bmod p)_i^{e_i}$ na straně 15 má být $(\bmod p_i^{e_i})$, rovnost (3.3) má být $(\beta_j)^{d/p_i^{j+1}} = \alpha^{a_j d/p_i}$. Na straně 22 se v kroku 5 objevuje podmínka $v_j < d$, která v Algoritmu 3.4 chybí.

Celkově práce působí dobrým dojmem, myslím, že autorka problematice rozumí. Práci proto doporučuji k obhajobě s hodnocením *výborně*.

V Praze 5.9. 2011

Pavel Příhoda