Posudek oponenta bakalářské práce

Název: Složitost některých faktorizačních algoritmů
Autor: Vilém Štěpánek

Shrnutí obsahu práce

Metoda eliptických křivek (ECM) je jedním z nejpoužívanějších algoritmů pro rozklad velkých čísel. Jejími přednostmi je snadná implementace a přitom příznivá asymptotická složitost. A té složitosti se věnuje tato bakalářská práce. Vychází se z různých odhadů pravděpodobností a z nich se spočte odhad složitosti, který sice není formálně dokonale ověřen, ale souhlasí s daty z praxe. Stejné ověření provedl i student na vlastní implementaci ECM.

Celkové hodnocení práce

Téma práce. Složitost algoritmů je náročné téma, kterému se naprostá většina studentů MMIB vyhýbá. Autor práce se tohoto tématu zhostil se ctí.

Vlastní příspěvek. Práce neobsahuje žádný nový výsledek. Příspěvkem studenta je shrnutí výsledků z různých zdrojů do jednoho celku. Dokázány jsou ovšem jen ty výsledky, které nevyžadují komplikovaný aparát.

Matematická úroveň. Velmi dobrá, student porozuměl i složitějším kalkulacím, na které obvykle studenti nejsou z přednášek zvyklí. Důkazy jsou korektně zformulovány. Připomínku bych měl pouze k obecným algebraickým pojmům jako automorfismus nebo ekvivalence, které jsou definovány ne v základní podobě, nýbrž ve svém důsledku pro eliptické křivky.

Formální úprava. Po formální stránce je práce standardní bakalářské úrovně, tj. není moc čtivá. Definice a věty se hrnou za sebou, aniž by bylo jasné, kam směřujeme, některé věty nedávají gramatický smysl, objevují se typografické chyby. Překlepy ve slovech nejsou. Přiložený program je napsán v absurdní angličtině.

Otázky k zodpovězení u obhajoby

1. Na straně 21 se rozebírají tři možné reprezentace bodů v projektivním prostoru, s tím, že dle následné diskuze se třetí varianta zdá být nejvýhodnější, protože nemusíme počítat inverzy modulo n. Smyslem ECM je ovšem nalézt dělitele čísla n a toho se docílí tak, že v jednu chvíli selže inverze modulo n, neboť chceme invertovat číslo s n soudělné. Pokud tedy body projektivního prostoru reprezentujeme jiným způsobem, jak pak nalezneme dělitele čísla n? Odpověď na tuto zásadní otázku v práci chybí, neboť pseudokód je napsán jen pro zdánlivě nevýhodnou reprezentaci afinní.

2. Na straně 20 se minimum funkce nepočítá, ale rovnou prozradí. Což o to, výpočet je vskutku jednoduchý, ale chtěl bych se ujistit, že vynechání toho kroku nepramení z často vídané alergie na slovo „derivace“ a že student ví, jak naložit s členem $o(1)$, který není konstantní.

Drobné připomínky

- V češtině není zvykem značit mohutnost množiny A jako $\#A$.

- str. 8: Věta „Dále víme, že $E_{a,b}$ je izomorfní s $E_{a',b'}$ znamená, že existuje...“ by šla zajisté zformulovat lépe.
- str. 9 a dál: Zápis „Nechť $\mathcal{S}$ je množina celých čísel taková, že $\forall s \in \mathcal{S}$ platí: $|s-(p+1)| \leq 2\sqrt{p}$“ lze elegantněji vyjádřit pomocí

$$\mathcal{S} \subseteq (p+1-2\sqrt{p}, p+1+2\sqrt{p}) \cap \mathbf{Z},$$

  přičemž nezáleží na tom, zda vezmeme otevřený nebo uzavřený interval, když $\sqrt{p}$ není racionální.
- str. 9: Zápis $\sum_{t,p+1-t\in\mathcal{S}}$ je zmatečný. Přehlednější je třeba $\sum_{t\in\mathcal{S}-p-1}$.
- str. 9: Třetí řádek odspodu má být $p \geq 5$.
- str. 10: Důkaz Tvrzení 18 neplyne z Definice 7, ale z Poznámky 5.
- str. 17: Tvrzení se píše s velkým T jen, když se jedná o název, např. Tvrzení 23. Viz „Náměstí Republiky“ a „toto náměstí“.
- str. 35: Pál Erdős se píše s dlouhou přehláskou. Moje maličkost se píše s háčkem nad c.
- Přiložený program má 1GB (!), z čehož polovinu tvoří spustitelný soubor a polovinu seznam prvočísel (asi).
- Přiložený program nejde spustit z DVD a musí se překopírovat do počítače, což chvíli trvá, vzhledem k monstrózní velikosti.

Závěr

Práce je po vědecké stránce přínosná. Formální chyby jsou pouze drobnějšího charakteru. Proto doporučuji text uznat jako bakalářskou práci.

RNDr. Přemysl Jedlička, PhD.
Katedra matematiky, Technická fakulta, Česká zemědělská univerzita
15. 6. 2016