# Oponentní posudek diplomové práce

Práce „Prosívání ve faktorizačních algoritmech“ od Samuela Staška je převážně kompilační práce, ve které se diplomant zabývá složitostí faktorizačních algoritmů, konkrétně kvadratického síta a číselně-teoretického síta. Oba algoritmy mají původ v osmdesátých letech a autor se zabývá povětšinou verzemi těchto algoritmů, které byly známy již na začátku devadesátých let. Čestnou výjimkou je randomizované číselné síto z roku 2018, což je teoretický algoritmus, jehož výhodou je, že umožňuje rigorózně počítat průměrnou složitost číselného síta – v dřívějších verzích totiž teoretické postupy obvykle počítaly vágně definované „typické případy“.

Výpočty, které student v práci předvedl, jdou nad rámec standardního učiva, což znamená, že se musel naučit velice obtížnou část matematiky. To, že diplomant těm výpočtům rozumí, se ovšem neblaze projevuje tím, že se během výpočtů nedovolává explicitně na vztahy, ze kterých vychází, takže čtenář (který se obvykle v problematice orientuje hůře) často tápe, jak se při výpočtu přešlo z jednoho výrazu ke druhému.

Nejzajímavější se jeví sekce 1.3, ve které diplomant navrhuje vlastní vylepšení kvadratického síta. To vylepšení je implementačně jednoduché a student počítá, při jaké volbě parametrů dojdeme k nejlepším výsledkům. Ukazuje se ovšem, že přesný výpočet je otřesně komplikovaný a že je potřeba něco zanedbat. Tím, že je návrh teoretický a zkušenost z praxe chybí, není jasné, které parametry a jak lze zanedbat, proto student nabízí dvě sady odhadů, jednu pesimistickou a jednu optimistickou. Na několika příkladech se ukazuje, že ta optimistická varianta je skutečnosti blíže; tedy, alespoň tak je to v práci prezentováno. Bohužel, občas ty naměřené hodnoty leží mimo interval mezi optimistickým a pesimistickým odhadem, což by měl diplomant při své obhajobě ozřejmit.

Shrnutí: práce přináší shrnutí vysoce netriviálních výsledků, stejně jako nové vlastní výsledky. Proto doporučuji práci přijmout jako práci diplomovou.

### Drobné chybičky

- Strana 7: Písmeno $M$ se objevuje ve dvou různých významech (Meisselova-Mertensova konstanta a poloměr prosívacího intervalu), což je matoucí.
- Strana 7: Rozvaha podle diplomanta „naznačuje“, jak volit parametr $M$. Nemohl by autor čtenáři skutečně prozradit, jak jej volit? Není zde důvod udržovat čtenáře v napětí, nečteme detektivku.
- Strany 6 a 10: Používá se $\pi_B \approx \frac{B}{\ln B}$, což je sice notorieta, ale sluší se ji zacitovat explicitně.
- Strana 16: Potřebujeme odhadnout $\sum 1/i$ zdola, nikoliv zhora, takže ve skutečnosti dostaneme $k \leq \exp(c)$, což je asymptoticky podobné.
- Strana 17: Z $|I_{\exp(c-1)}| \geq d$ po dosazení $|I_{\exp(c-1)}| = \frac{2M}{c\exp(c-1)}$ dostaneme $c\exp(c) \leq \frac{2M}{d}$, takže odkud se vzalo $d-1$?

- Strana 17: Hodnota $u_c$ odhaduje pravděpodobnost, že je hodnota $x_c$ hladká, nikoliv to, co je v textu napsáno.
- Strana 36: Slušelo by se dodat nějaký odkaz na metodu eliptických křivek.
- Strana 36: Vzhledem k tomu, že ve znění věty je $N$ proměnnou volnou a $n$ vázanou, bylo by přehlednější formulovat poznámku pro $N \to \infty$.
- Strana 43: Slovo „částkových“ neznám.
- Strana 43 a několikrát dále: To, že jsou dané hodnoty optimální, není vidět, takže je potřeba napsat, odkud se vzaly, zda z nějakého softwaru anebo z literatury.
- Strana 52: generováním, nikoliv vygenerováním
- Strana 64 modifikace snížily

doc. RNDr. Přemysl Jedlička, Ph.D.