Posudek vedoucího na diplomovou práci
Anežky Pejlové nazvanou
Generování polynomů pro číselné síto

Jde podle mého soudu o velmi zdařilou práci, ve které se podařilo představit fázi generování polynomů v algoritmu číselného síta v plném rozsahu. Zvláště oceňuji kritický přístup k mnoha heuristikám, které jsou v používaných algoritmech skryty.

Práce je dobře strukturovaná. První kapitola obsahuje některé matematické výsledky a pojmy, které lze vyložit zcela nezávisle na kontextu číselného síta. Jádrem je technický výsledek, který propojuje výsledky Canfielda, Erdöse a Pomerance o hustotě hladkých hodnot s asymptotickými výsledky vyjádřenými L-notací. Druhá kapitola vykládá hlavní myšlenky jednotlivých fází číselného síta s přihlédnutím k použití nemonických polynomů. Třetí kapitola úspěšně reprodukuje první Kleinjungův algoritmus. Těžiště práce je v závěrečných třech kapitolách. V první z nich je nejprve vyloženo, jak k volbě stupně polynomu lze použít odhad doby běhu algoritmu, což vzhledem k řetězci implikací vedoucího od výtěžnosti polynomu přes množství relací k volbě velikosti prosívací oblasti znamená, že při využití base-(m, p) metody lze volit nižší stupně než při volbě základní base-m metody (viz Tabulka 4.1). Ocenění zaslouží zavedení konceptu přínosového schématu, což je pojem, který umožňuje více rigorózní přístup k takzvaným kořenovým vlastnostem. Pátá kapitola je věnovaná takzvanému kořenovému sítu. Šestá kapitola mi přišla zajímavá jednak informací, že Jedličkovo vylepšení metody největšího spádu se ukázalo jako implementačně přínosné, jednak informací, že řazení podle L^2 normy lze zaměnit řazením podle velikosti koeficientů. To je pozorování, které by mohlo mít docela významný praktický dopad. Je to vlastně vyvrcholení řetězce úvah, které vykládají jednotlivá zjednodušení při stanovování kritéria velikosti polynomu.

Lze si představit, že dalším prohlubováním by z předkládané práce vznikla práce disertační. Tak, jak je práce předložena, je poněkud nevyrovnaná. Některé kroky algoritmu jsou podrobeny pečlivé analýze, někde je analýza nedotažena a někde ani nebyla zahájena. To je ovšem přirozené vzhledem k rozsahu práce diplomové a vzhledem k ambici autorky podat co nejúplnějšího průvodce daným algoritmem.

Práci jsem připomínkoval průběžně, a tato zkušenost mě vede k domněnce, že formálních nedopatření v ní nebude mnoho. Závěrečnou verzi jsem ovšem z hlediska formálních nedopatření podrobnému zkoumání nepodrobil.

Navrhuji, aby práce byla přijata jako práce diplomová a byla hodnocena stupněm *výborně*.

Aleš Drápal

V Praze 1. června 2016