Natálie Tejkalová, *Probabilistické algoritmy pro prvočíselnost*

(V. Švejdar, posudek vedoucího na bakalářskou práci, září 2013)

Předložená práce obsahuje popis dvou historicky důležitých a přitom i dnes prakticky použitelných algoritmů pro prvočíselnost, Solovayova-Strassenova z r. 1977 a o něco pozdějšího Rabinova-Millerova. Oba algoritmy jsou podrobně vysvětleny a jsou podány důkazy jejich korektnosti. Závěrečná Kapitola 5 je pokusem podat obecnější informaci o pravděpodobnostních třídách ve výpočtové složitosti a o praktickém a případně filosofickém významu pravděpodobnostních algoritmů a náhodnosti vůbec.

Je známo, že důkaz korektnosti některých algoritmů závisí na nedokázaných hypotézách, nebo v jiných případech na dokázaných avšak obtížných výsledcích z teorie čísel. Jedním z motivů, proč zadat tuto práci, bylo zjistit, jak obtížné je matematické pozadí obou probíraných algoritmů. Na tuto otázku práce dává poměrně přesvědčivé odpovědi. Všechna potřebná teorie čísel je zvládnutelná i na školní (bakalářské) úrovni. Na druhé straně, bez mírně obtížnějších výsledků a úvah, jako je Gaussovo lemma nebo Eisensteinův obdélník, nebo cykličnost grupy $\Phi(p)$ pro p prvočíslo, se pravděpodobně obejít nelze.

Na několika místech bych uvítal podrobnější informaci o tom, co je autorčin vlastní přínos a co je převzato z literatury. Takovou otázku vzbuzuje například věta "náš důkaz se nejvíce inspiruje důkazem uvedeným v . . . " na str. 24. Velmi oceňuji, že autorka ukazuje fungování pravděpodobnostních algoritmů na konkrétních a ne tak malých číslech. I tady bych ale rád věděl, co autorka spočítala sama a jak. Například na str. 22 je vyjmenováno 16 "lživých" parametrů, které dají nesprávný výsledek při zpracování čísla 91 Rabinovým-Millerovým algoritmem. Našla je autorka sama?

Na dalších několika místech práce ja patrná určitá terminologická neustálenost. Místo "vyčíslitelná množina" na str. 32 a "parciálně rekurzivní funkce" na str. 33 bych doporučil *rekurzívní množina* a *částečně rekurzívní funkce*. Podobně "stupeň" na str. 19 má být *řád*. Na téže straně se zdá, že se autorka zbytečně vyhýbá termínu *cyklická grupa*, ačkoliv jinde jej používá.

Kapitola 5 poskytuje čitelnou úvodní informaci o pravděpodobnostních třídách ve výpočtové složitosti. Její aktuálnost nedokáži posoudit, ale zdá se, že lepší by bylo tuto kapitolu pojednat méně do šířky a s konkrétními příklady algoritmů a úloh. Turingovy stroje s orákulem, nedeterministické Turingovy stroje a vlastně Turingovy stroje vůbec lze považovat pro daný kontext za celkem zbytečné.

Práce je psaná dobrým jazykem, s velmi malým množstvím překlepů a téměř bez pravopisných chyb. Stylistickou úroveň velmi oceňuji, je dobře, že se autorka pokusila formulovat i neformální vysvětlení a někdy i vlastní názor. Na druhé straně

k formě a typografii lze mít dvě poměrně silné výhrady. Není jasné, jaký bibliografický styl byl použit k formátování seznamu literatury, a vzniká podezření, že žádný. Práce se doslova hemží nevhodnými řádkovými lomy. Přitom problematiku dělení řádků v matematickém režimu a víceřádkové rovnice lze považovat za obtížnější, avšak například neslabičné předložky na koncích rádků by šlo snadno odstranit.

Autorka udělala pěkný kus práce při promyšlení řady netriviálních důkazů a shromáždila poměrně obsáhlou relevantní literaturu, která není zmíněna v zadání práce. Z těchto důvodů a přes výhrady zmíněné výše navrhuji klasifikaci *výborně*.

V Praze 14.9.2013 doc RNDr Vítězslav Švejdar CSc