Posudek vedoucího na diplomovou práci
Adély Skokové: Podpůrné algoritmy číselného síta

Cílem práce mělo být popsat dva důležité, byť ne centrální, algoritmy používané v číselném sítu. Z nich byl popsán pouze jeden. Vzhledem k rozsáhlosti problematiky tuto redukci považuji za vhodnou. Součástí řešení je i implementace Kleinjungova druhého algoritmu pro hledání polynomů. Tato implementace se stala součástí programového vybavení, které realizuje algoritmus číselného síta a které je vyvíjeno na katedře algebry.

Vlastní téma práce zaujímá 30 stran, tedy čtvrtou a pátou kapitolu. Tomu předchází kapitola o potřebných pojmech a poznatcích z komutativní algebry a hrubý popis číselného síta. Jejich přítomnost v práci vyplynula ze snahy autorky vlastní téma práce organicky začlenit do kontextu. Rozsah druhé kapitoly (o potřebných pojmech komutativní algebry) je o něco větší než by bývalo nutné – to však vyplynulo z kontaktu s vedoucím práce, kdy se zdálo být žádoucí upevnit porozumění autorky právě těm potřebným základním pojmům. To se snad podařilo, nicméně analýza tématu provedená v hlavních kapitolách neukazuje na to, že by toho bylo bývalo opravdu využito.

Úvodní kapitoly jsou pěkně napsány a s malým počtem chyb. jde spíše jenom o drobnosti, byť některé dosti překvapivé (vzhledem k zvolenému způsobu zápisu by skalární násobení mělo být chápáno jako $R \times M \to M$; raději podmoduly než modmoduly; T-izomorfismus U do U nemusí obecně vzato být automorfismus; druhá část Poznámky 2.4.6 nedává smysl – správně má být, že průnik ideálu a celých čísel obsahuje právě jedno prvočíslo, protože tento průnik je vlastní prvoideál celých čísel).

Druhá polovina práce je kvalitou výrazně slabší. Autorka reprodukuje popisy algoritmů a jen výjimečně přidává něco vlastního. Z implementace i celkového popisu je patrné, že jádru problematiky dobře rozumí. Téměř nikde však nevyužije možnosti vyložit smysl tvrzení nebo fakt, které jsou v původních článích uvedeny bez důkazů. Čtenář diplomové práce často nepozná. zda se za nějakým takovým tvrzením nebo faktem skrývá jednoduché pozorování nebo heuristický ohad nebo něco, co je podloženo experimenty a měřeními.

Například na straně 35 je definována Dickmanova funkce ρ, je uvedena její souvislost s odhadem frekvence hladkých hodnot a pak je řečeno, že hodnotící funkcí polynomu $F(x, y)$ může být dvojný integrál přes danou oblast hodnoty $\rho(\log|F(x, y)|/\log b)$ bez toho, že by bylo vyloženo, že jde vlastně o spojitou aproximaci součtu pravděpodobností, že $F(a, b)$ je hladké číslo, tedy o odhad počtu hladkých hodnot v dané oblasti. (Zde nejde o míru přesnosti použití termínů teorie pravděpodobnosti, ale o sdělení, že je tady nějaká velmi přímočará souvislost.)

Podobně třeba popis kořenových vlastností (část 4.3.2) působí dojmem, že je psán bez hlubšího porozumění.

Podobné nedostatky jsou i v kapitole páté. Někdy se promítají i do částí, jež si kladou nárok na formální korektnost. Například při výkladu (m, p)-adického rozkladu (str. 45) kde jde o nalezení čísel a_i, čteme, že nejprve definujeme rekurzivní parametry r_i. Ovšem definice r_i používá a_{i+1}. Není to nic, co by po chvíli studia nebylo možno pochopit – ve skutečnosti se postupně určují $r_d, a_d, r_{d-1}, a_{d-1}, \ldots$. Ovšem tak, jak je to napsáno, je to špatně.

Obecně není snadné rozhodnout, kde u autorky šlo o neporozumění a kde o nešikovné vyjádření. Během vedení práce jsem došel k názoru, že většinou jde spíše o to druhé, a z toho vycházím i při návrhu známky. Nicméně podobných míst je v práci více. Například v důkazu Tvrzení 5.5.4 je klíčovým faktem, že $x^d \equiv 1 \bmod p_i$ má právě d řešení, a tudiž pokud pro nějaké a má $x^d \equiv a \bmod p_i$ alespoň jedno řešení, je takových řešení právě d. O nic jiného v důkazu nejde. Nicméně je velmi obtížné takovou úvahu za textem důkazu vidět. Navíc v závěru jde o rutinní aplikaci Čínské věty o zbytku, což by mělo být pro autorku samozřejmost. Místo toho podává úvahu, která vlastně skrývá důkaz Čínské věty o zbytku pro daný konkrétní příklad.

V páté kapitole jsou i nepříjemná formální nedopatření. Například na straně 41 chybí, že $f_1(m)$ a $f_2(m)$ jsou kongruentní nule modulo N.

Kladu si otázku, zda a_d z Tvrzení 5.3.1 má skutečně být prvočíslo.

Celkovým rozsahem je práce přiměřená, množství látky nastudované a více či méně zvládnuté je nemalé, formální úroveň je vcelku velmi slušná, a to i po jazykové stránce (jenom na okraj – před *než* se doporučuje psát čárku pouze tehdy, jde-li o uvedení vedlejší věty v souvětí).

Vzhledem k faktům výše uvedeným doporučuji, aby práce byla přijata jako práce diplomová. Doporučuji hodnocení stupněm *dobře*.

V Praze dne 27. května 2015

Aleš Drápal