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. Současně měl být alespoň jeden z nich implementován. O implementaci se však v práci žádná zpráva nepodává, takže nelze považovat cíl práce za naplněný.

Vlastní téma práce zaujímá 26 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. Při plnění tohoto chvályhodného cíle se však ukázalo, že i když jde o látku, která by měla být studentce z kurzovních přednášek známa, její přesná a věcně správná prezentace, a také její vhodné strukturování, jí působily značné problémy. V důsledku toho rozsah úvodních kapitol je větší než by vzhledem k tématu práce bylo nutné. Čas strávený nad těmito kapitolami pak zjevně chyběl při zpracování hlavního tématu. I přes velký objem času úvodním kapitolám věnovaný v nich zůstalo množství nepřesností, ba i vyložených chyb.

Tématicky centrální kapitoly jsou celkově vzato kvalitnější, avšak strádají nedostatkem úvah, které by popisované postupy a algoritmy reflektovaly, ať už cestou samostatných rozborů a otázek, nebo cestou měření, která by vycházela z nějaké implementace. V těchto kapitolách jsou navíc také určitá místa, kde jsou buď nepřípustné nepřesnosti, nebo zjevně chybí výklad souvislostí.

Celkovým rozsahem je práce přiměřená, množství látky nastudované a více či méně zvládnuté je nemalé, formální úroveň je vcelku velmi slušná. Pokud by nebyl tak výrazný rozpor mezi zadáním a výsledkem, šlo by snad uvažovat o přijetí práce jako práce diplomové. V dané situaci se však cítím povinován navrhnout komisi opak.

Následují podrobnější připomínky.

Podkapitola 2.1 má nešťastnou strukturu. Lépe bylo začít pojmem modulu a okruhu (kde se potřebuje minimum fakt) a pak přejít k tělesům. Přechod k modulům, jak je nyní na straně 7, druhý odstavec, nelze akceptovat. Najednou se mluví o multiplikativním zobrazení z M do M, aniž by se řeklo, že M je modul. Přitom v předcházejících odstavcích se o M mluví jako o podmnožině okruhu.

Autorka občas vkládá do části označené jako Poznámka fakta zásadního významu. Tak je to i s Poznámkou 2.1. Ta je zvláště nešťastná. Ve svém úvodu označí množinu V, na kterou pak odkazuje explicitně pouze v jednom případě, byť implicitně je V přítomno i v dalších bodech. Dále používá obrat *algebraicky uzavřené v* U, aniž by ho definovala. Jednoznačnost až na T-isomorfismus by bylo vhodné popsat explicitně, aby

bylo zřejmé, co tím autorka míní (mně to v tomto kontextu jasné není). V následujícím bodě pak by mělo jít o rozšiřování T-homomorfismů na T-automorfismus.

Zcela špatně je definice jednoduchého rozšíření na straně 7 nahoře. Nechápu, jak se taková věc mohla stát.

Podobně je nešťastný důkaz Hlavního tvrzení 2.35. Argumenty nahoře na straně 16 nepůsobí přesvědčivě. Pochybuji, že takto lze vůbec argumentovat. I kdyby však taková argumentace možná byla, je to pro vlastní důkaz argumentace zbytečná a svědčí o malé znalosti struktury konečně generovaných beztorzních abelovských grup. (Stačilo si ujasnit, že $\mathbb{Q}^n$ nemůže obsahovat abelovskou grupu ranku (hodnosti) $n+1$.)

Podobně i důkaz Hlavního tvrzení 2.38 nevypadá dobře. Znalost struktury abelovských grup je potřebná k tomu, abychom mohli deklarovat existenci celistvé báze $\beta_1, \ldots, \beta_n$ takové, že existují kladná $d_1, \ldots, d_n$, která splňují, že $d_1\beta_1, \ldots, d_n\beta_n$ je báze ideálu I.

První rovnost v Tvrzení 2.54 není vysvětlena. Vyžaduje Činskou větu o zbytku, což nikde není zmíněno. Bez toho je důkaz neúplný.

Důkazu Tvrzení 2.64 jsem nebyl schopen porozumět.

V kapitole 2 jsou ještě další, méně závažná, nedopatření.

Kapitola 3 je v zásadě vyhovující. Určité formulace ovšem působí lehce vyhýbavě a naznačují, že studentka některým fázím algoritmu číselného síta do detailů nerozumí. Za chybu považuji, že fakt, že polynomy t_i musí být lineární, není vyložen rigorózně, a že není z toho odvozeno nic (nebo alespoň naznačeno) pro rozklad $(a - b\alpha)$ na prvoideály, a to zvláště ve vztahu k normě prvku $a - b\alpha$. Tím je pominuta možnost ukázat podstatnou vazbu této části práce na předcházející kapitolu.

V podkapitole 4.2 není pojem zkosení dostatečně objasněn. Vypadá to, že zkosený interval je totéž jako obdélníkový, jenom je použita jiná metoda volby A a B. Text je v tomto směru zjevně neúplný.

Poznámka 4.4 by měla být spíše tvrzením, a měla by explicitně zmínit (a stručně vyložit), že i $\sup(f)$ je norma. V Definici 4.3 by asi mělo být řečeno, že jde o polynomy stupně nejvýše d.

Podkapitola 4.4.2 nevypadá dobře. Protože jde o diskrétní hodnoty, tak je možné střední hodnotu definovat přes (předpokládané) uniformní rozdělení pravděpodobnosti dělitelnosti prvočíslem p konkrétním vzorcem. V označením zvoleném v textu předložené práce to vypadá tak, že střední hodnota $\mathbf{E}(v_p(F(a,b)))$ závisí na konkrétní dvojici (a,b). Tak to asi míněno nebylo, ale díky chybějící explicitní definici a špatně zvolenému označení není text srozumitelný.

Kapitola 5 vypadá po formální i věcné stránce dobře, byť, jak naznačeno v úvodu posudku, postrádám jakoukoliv reflexi popisovaných algoritmů. Překvapila mě inicializace algoritmu hodnotu $a_d = 0$. Považuji za chybu, že se pracuje se zkosením intervalu s aniž by se vysvětlilo, jak byly zvoleny hodnoty A a B, tedy aniž by se vysvětlilo, jak se k

hodnotě s dojde. Přitom v důkazech tvrzení, které s hodnotou s pracují, není fakt, že jde o zkosení, nutný (alespoň se mi tak zdá). Asi by stačilo v těchto tvrzeních říci, že s je číslo vybrané z určitého intervalu. Poznamenávám, že formule kapitoly 5 jsem nestudoval do detailů, a že tedy je možné, že některá nedopatření mi unikla.

Jsem přesvědčen, že dotáhnout předloženou práci do přijatelné podoby (ba i do velmi kvalitní podoby) je možné v relativně nedlouhém časovém období. Práce je celkem rozumně strukturována a potřebné zásahy budou mít spíše lokální charakter. Nicméně, vzhledem k faktům výše uvedeným, nemohu komisi doporučit, aby práce byla přijata jako práce diplomová, Doporučuji tedy hodnocení stupněm *neprospěla*.

V Praze dne 27. srpna 2013

Aleš Drápal