Posudek oponenta na diplomovou práci
Veroniky Heglasové
Algebraicko-geometrické kódy a Gröbnerovy báze

Jde o práci svým námětem i způsobem zpracování velmi zajímavou. Studentka ukázala schopnost porozumět většímu počtu nesnadných matematických témat a propojit je funkčním způsobem tak, aby byl patrný aplikační potenciál předložené teorie. S nemalou dávkou smutkut však musím konstatovat, že méně by asi v tomto případě bylo více: práce je zatížena formálními chybami, nejasnostmi a nepřesnostmi v míře, která ji výrazně ubírá na hodnotě. Předvedený výkon si myslím zaslouží uznání a práce by měla být přijata jako práce diplomová. Její hodnocení však musí vzít v úvahu jak nemalý počet chyb při expozici výchozí matematické teorie, tak nepřesný a těžko srozumitelný způsob výkladu algoritmů kapitoly 3, tedy výkladu ústředního tématu práce, vůči kterému ostatní partie stojí ve služebné roli,

Ve zbytku posudku se zabývám výkladem, jaké že konkrétní nedostatky jsem jako oponent v práci nalezl. To je úloha oponenta. Tyto výhkrady, kterých je nemálo, by však neměly zastínit celkově kladný dojem z přístupu k tématu včetně zjevného zvládnutí některých obtížných partií související teorie tak, jak je naznačeno výše.

Angličtina práce je srozumitelná, avšak plná prohřešků proti gramatice tohoto jazyka. Typicky *This extension correspondent to projection ...* místo *This extenstion corresponds to the projection of ....* Ve větách chybívají podměty, *is* se používá v roli *exist* (typicky *there is finitely many places*, členy bývají špatně nebo chybí, umístění čárek je ve sporu s konvencemi jazyka (často bývají před *that*). Nejde o výjimky, ale o konzistentní styl celé práce.

Úvodní část 1,1 je snad nejslabší z celého textu. Vypadá, jako by byla psána nesoustředěně a pod časovým tlakem. Jejím úkolem je podat přehled potřebných pojmů z algebraické geometrie. Podivná (a zjevně nesprávná) je například argumentace na straně 4, která chce vysvětlit, že DVR je lokální okruh s maximálním ideálem. V následujících pasážích autorka nejprve předpokládá, že valuační okruh je diskrétní a pak z toho jakoby odvodí, že všechny valuační okruhy jsou pro F/K diskrétní. Není vysvětleno, co je to $x(P)$ (strana 5 dole). Na straně 8 se předpokládá, že K je algebraicky uzavřené, ale pak se pracuje se situacemi, kdy tomu tak zjevně není. V předpokladu Theorem 1.1.25 (a i jinde) je zaměňováno algebraické a konečné rozšíření. V klíčové definici stopy (strana 11 nahoře) byl opomenut jeden výraz, takže je špatně.

Expozice částí 1.2 a 1.3 je výrazně lepší. Matematických chyb jsem si nevšiml. Většina tvrzení je dokázána ve zjevné (a přiznané) návaznosti na

[Stich09]. K úplnosti má výklad daleko – k tomu by byla potřeba expozice teorie rozšíření v míře daleko větší. Jsou vybrány takové důkazy, které bezprostředně navazují na definici Weilova diferenciálu, nebo vycházejí z P-adického zúplnění. To nepovažuji však za nějaký výraznější nedostatek.

Kapitola 2 je založena na kapitole II zdroje [Stich09]. Je reprodukována se zjevným porozuměním.

Kapitola 3 začíná výkladem Gröbnerových bází. Jeho zhuštěnost mi nevadí. Význam nedefinovaného symbolu v Theorem 3.1.8 jsem si snadno odvodil. Zvládl jsem i definici monomů na straně 31, byť mi dala trochu zabrat – písmeno m je totiž konzistentně používáno jak pro označení monomu, tak jako velikost volné báze. Pochopil jsem i definici uspořádání "position over term", byť i ta je zatížena použitím dříve nedefinovaného označení. S čím jsem si ale neporadil, byla definice Φ na straně 33 nahoře. Zde jsem musel požádat autorko o objasnění. Ukázalo se, že problém je v nedobře popsané akci grupy H. V textu se mluví o akci na množině kódových slov, ale je míněna akce na pozicích. V dané kapitole však nejde o jedinou nejasnost. Nerozuměl jsem tomu, proč se mluví o "term module" $[X]^m$. Slovo "module" sem asi nepatří – takové dohady ovšem čtení velmi znesnadňují. Poté následuje věta "Nonstandard terms correspond to terms and standard terms are used to check parity." Čtenář neví, zda tohle je deklarace nebo něco, co mu má být zřejmé. Další text to bohužel neosvětlí.

S podobnou bezstarostností je zahájen výklad části 4.2 Syndrome decoding. Bez pomoci autorky jsem nebyl schopen porozumět, co myslí generátory $\mathcal{L}(mP_\infty)$. Problémů je tam několik. Jednak nekomentuje skutečnost, že X zde znamená $\{x, y\}$. Dále nekomentuje fakt, že tyto symboly nechápe jako prvky okruhu $K[x, y]$, ale $K[x, y]/(f)$. Konečně považuje za samozřejmé, že báze $\mathcal{L}(mP_\infty)$ je tvořena monomy $x^a y^b$. Mně to samozřejmé nepřijde.

Autorka zjevně nedocenila fakt, že tam, kde se dostává z oblasti v zásadě standardních matematických pojmů do oblasti algoritmické a méně standardní, je nutné věnovat definicím a jejich osvětlení daleko více prostoru. Na rozdíl od odborných článků, ze kterých čerpala, nemůže předpokládat, že čtenář diplomové práce je seznámen s kontextem do podobné hloubky jako čterář příslušného odborného článku. Jejím úkolem právě bylo takový kontext vytvořit. O to se snažila chvályhodným uvedením příkladů. Bohužel cesta k nim je zarubaná, neboť na ní leží mnoho padlých definic a pastí nedovyslovených myšlenek.