Kateřina Teplá: Kerdockovy kódy a okolí

Posudek vedoucího diplomové práce

Z textu diplomové práce je zřejmé, že studentka získala o tématu dobrý přehled. Zpracování je uspokojivé, byť ne vynikající.

V první kapitole se zavádějí dvěma způsoby Kerdockovy kódy. Chybí jasný výklad, které z postulovaných vlastností jsou v práci později dokázány (například minimální vzdálenost je odvozena v kapitole tři). Je zavedena Teichmüllerova množina, ale důkaz jejích vlastností je uveden ve formě nástinu. To je škoda, protože jde o základní strukturní nástroj při práci s okruhem $R = GR(4^m)$. Navíc mi není jasné – a bylo by dobré to během obhajoby vyjasnit – jaká znalost autorce chyběla, aby podala plný důkaz, ne pouze nástin. Věc lze přitom dokázat velmi snadno bez použití jakýchkoliv hlubších tvrzení. Lze se vyhnout i Henselovu lemmatu. (Grupa R^* má řád $2^m(2^m-1)$ a z projekce μ vyplývá, že R^* má jako faktor cyklickou grupu řádu 2^m-1. Z klasifikace abelovských grup proto plyne, že R^* má jedinou abelovskou podgrupu řádu 2^m-1. To je (spolu s nulou) ona hledaná Teichmüllerova množina. Ať α je generátor podgrupy. Odečtením polynomů $x^{2^m-1}-1$ a $\prod(x-\alpha^i)$ dostaneme polynom tvaru $2c(x)$, který je nižšího stupně a má kořeny α^i. Použitím μ zjistíme, že $c(x)=0$. Podobnou úvahou vyplyne, že když $x^{2^m-1}-1 = h(x)q(x)$, tak $h(x)$ i $q(x)$ jsou součiny příslušných kořenových činitelů $(x-\alpha^i)$. Z projekce μ tak dostáváme, že v případě primitivního polynomu $h(x)$ jsou všechny jeho kořeny rovny vhodným α^i, které jsou řádu 2^m-1. Zbytek důkazu je zcela přímočarý.)

Druhá kapitola podává základní vlastnosti symplektických forem nad dvouprvkovým tělesem. Ty jsou pro práci s Kerdockovými množinami základním pracovním nástrojem. V kapitole jsou použity pro výklad ekvivalence Kerdockových množin a ortogonálních rozestření (orthogonal spreads).

Jádro práce je v kapitole 3, která jednak podává (obtížný) důkaz klasické věty o vztahů designů a kódů, jednak ukazuje, jak lze tvrzení zobecnit pro kvaternární kódy.

Závěrečná kapitola 4 se věnuje použitím Kerdockových kódů pro křivé (bent) funkce a pro odolné (resilient) funkce. Souvislosti jsou zajímavé a užitečné. Teorie v kapitole uvedená se netýká Kerdockových kódů jako takových. Po jejím vybudování totiž stačí pouze využít jejich známých vlastností. Z matematického hlediska je tedy jádrem kapitoly 4 jednak výpočet pokrývacích poloměrů Reed-Mullerovych kódů $RM(1,m)$, jednak důkaz ekvivalence odolných funkcí a velkých ortogonálních šiků (large orthogonal arrays).

Jsem přesvědčen, že diplomantka dokazovaným tvrzením v zásadě rozumí. Na druhou stranu na některých místech se nelze ubránit dojmu, že při reprodukci určitých důkazů se nechala příliš vést vzorovým textem a důkaz dostatečně nerozpracovala. Nevím, do jaké míry to byla nepozornost nebo pohodlnost, a do jaké míry látku v určitých detailech ne zcela promyslela.

Během obhajoby bych se rád dozvěděl, jaké má argumenty pro tvrzení v odstavci těsně navazujícím na formuli (1.46) ve vztahu k vektorům $\mathbf{v}^\lambda$. Dále bych se rád dozvěděl podrobné zdůvodnění tvrzení o počtu různých kódových slov v předposlední větě důkazu 1.2.15.

Potíže porozumět textu jsem měl také na stranách 43-47. Důkazu bodu (i) lemmatu 3.3.1 nerozumím. Mluví se v něm o nějakém izomorfismu, zřejmě má jít o izomorfismus ve smyslu multiplikační pologrupy. Jak by tento fakt měl mít vliv na rozdělení hodnot 0 a 2, mi není jasné.

Nerozumím tomu, jak interpretovat symbol $\pm$ ve znění Věty 3.3.3. Následuje komentář k důkazu této věty. Skutečnost, která není na vrcholu strany 45 dokázána, je velmi jednoduchá. Stačí si uvědomit, že když Teichmüllerova množina obsahuje

$\zeta^i \pm \zeta^j$, tak musí obsahovat i příslušný obraz Frobeniovým automorfismem. Srovnáním se čtvercem součtu (nebo rozdílu) pak plyne spor. Považuji za chybu, že toto je řešeno odkazem na externí zdroj. Protože znění věty není jasné, není mi ani jasné, jak se provedou závěrečné úpravy. Prosím, aby poslední věta důkazu byla pečlivě rozvedena. Předpokládám, že z upraveného znění věty bude již důkaz následujícího důsledku zřejmý. Ze současné verze mi to zřejmé nepřijde.

Je samozřejmé, že podrobnosti není možno během obhajoby uvádět do detailů. Proto navrhuji, aby diplomantka ve výše uvedených připadech vypracovala opravené znění písemně a zaslala ho vedoucímu práce, případně i oponentovi, a to s předstihem. Do této kategorie budiž ještě zařazen důkaz letmé zmínky o ekvivalenci kvadratických forem Q a $Q + f$ (vztah (2.9)).

Po matematické stránce je práce kvalitní; chyby mají v zásadě charakter buď drobnosti ve formulacích, nebo nejasnosti v průvodním textu. Zarážející je formulace na straně 22: "In this case, a quadratic form Q is non-singular if and only if the bilinear form β obtained by polarisation is non-singular." V bodu (iii) Věty 2.1.8 je třeba předpokládát, že jde o symplektické formy.

Co se týče angličtiny, tak s frekvencí zhruba dvou a více chyb na stránce je buď uveden vyloženě špatně člen, nebo je použit špatný tvar slovesa ve třetí osobě. Jinak je angličtina slušná. Místo slovesa *divide* by bylo vhodné používat sloveso *partition*, jde-li o rozklad množiny.

V práci nejsou žádné ilustrativní příklady. To považuji za chybu.

Práci doporučuji uznat jako diplomovou a hodnotit ji stupněm .....

Aleš Drápal