Posudek oponenta diplomové práce

Název: Schémata závazků k polynomům více proměnných
Autor: Kateřina Bžatková

Předložená práce prezentuje dva nové návrhy schémat závazků (commitment schemes), které se opírají o nedávnou publikaci Dan Boneh, Justin Drake, Ben Fisch, and Ariel Gabizon: *Efficient polynomial commitment schemes for multiple points and polynomials*. Závazky jsou v případě obou schémat představovány reprezentací evaluace polynomu více neurčitých, který sám tvoří tajnou zprávu, proto je významnou součástí textu rovněž stručný nástin potřebné algebraické teorie.

Text práce je rozdělen do motivačního úvodu, pěti věcných sekcí a stručného závěru. Obsahem první kapitoly je shrnutí potřebných partií komutativní algebry, především charakterizace průniků maximálních ideálů a teorie Gröbnerových bází. Druhá část textu je věnována obecným i speciálně polynomiálním schématům závazků, kromě souvisejících definic jsou (zčásti bez důkazu) vysloveny využívané vlastnosti spolehlivosti a úplnosti schémat (soundness and completness). Třetí a čtvrtá kapitola prezentují samotné návrhy schémat a jejich podstatné vlastnosti. V obou se jako tajné zprávy využívají polynomy více neurčitých nad tělesem prvočíselného řádu a závazek představuje vyhodnocení tohoto polynomu v náhodně zvoleném bodu reprezentované ve vhodné cyklické aditivní grupě. O přijetí závazku rozhoduje otázka náležení ideálu a jeho Gröbnerova báze, zatímco v prvním případě je Gröbnerova báze maximálního ideál daného jednou nulou předem bez výpočtu jasná, v druhém schématu je třeba Gröbnerovu bázi součinu maximálních ideálů najít. Stručná pátá sekce textu diskutuje otázku složitosti předložených schémat ve srovnání s dalšími polynomiálními schématy závazků, jež byly pro předloženou práci inspirací.

Text je napsán přehledně a poměrně čtivě, ačkoli bych v záplavě definic přivítal více (alespoň hračkových) příkladů. Především úvodní teoretické pasáže by si rovněž zasloužily větší pečlivost v detailech, čtenář si některé předpoklady a fakta musí domýšlet, případně pro správné pochopení nahlížet do prací, na než se text odkazuje. Samotné téma se zdá být velice aktuální a ačkoli se návrhy nezdají být příliš vzdálené těm, které zobecňují, jedná se do značné míry o původní a bezpochyby velmi zajímavou práci. Matematická úroveň textu je dobrá a svědčí o autorčině porozumění problematice a o její schopnosti samostatné odborné práce, drobné výtky jsou shrnuty v poznámkách níže. Jazykových a formálních nedostatků obsahuje text množství úměrné jeho délce.

Práce Kateřiny Bžatkové *Schémata závazků k polynomům více proměnných* úspěšně naplnila zadání a doporučuji ji uznat jako diplomovou.

Jan Žemlička
Katedra algebry
7.9.2022

Komentáře:

• s.6, ř. -13 – $\mathbb{F}_{<t}[X_1, \dots]$ (využívané v Corollary 1) by mělo být jasně zavedeno.

• s.7, ř. 7 – V zavedení monoidu $\mathbb{T}^n$ by mělo být o jeho prvcích $x_1^{e_1} \dots x_n^{e_n}$ jasně řečeno, že se jedná o monomy s formálními komutujícími proměnnými x_i.

• s.7 a dále – Přehlednosti by myslím prospělo, kdyby byly proměnné všude značeny symbolem X_i (jako je to v Definicích 4 a 5 a dále počínaje Lemmatem 2) a prvky tělesa symbolem x_i (jak se tak děje od Definice 15).

• s.9, důkaz Lemmatu 2 – Předpokládám, že symboly ρ a r zde značí stejný polynom, navíc formulace *... where r is modulo G* je podivná a zbytečná.

• s.11 a dále – Předpokládám, že by těleso $\mathbb{F}$ zde i všude dále, kde dochází k násobení jeho prvků prvky aditivních abelovských grup G_i, mělo být tělesem prvočíselného řádu. Tedy prvky $\mathbb{F} = \mathbb{F}_p = \{0, 1, \dots, p-1\}$ by měly být jednoznačně reprezentovatelné přirozeným číslem (v opačném případě nevím, co by součiny prvků z $\mathbb{F}$ a $\mathbb{G}_i$ měly znamenat).

• s.12, Definice 14 – podmínka $e(g_1, g_2) = g_t$ je spíše než vyžadovaná vlastnost označením generátorů, samotná podmínka, že obraz dvojice generátorů je generátor, plyne pro grupy téhož prvočíselného řádu z následujících dvou podmínek.

• s.13, Definice 15 – Zavedení množin $\mathbf{srs_i}$ je podivné, má dané značení znamenat, že reprezentujeme v $\mathbb{G}_i$ vyhodnocení všech polynomů f_j na všech prvcích $(x_1^{d_1}, \dots, x_\mu^{d_\mu})$ pro d_k splňující $\sum d_k < Q$?

• s.13, Definice 16 – Odkud se vzala x_i v této definici?

• s.15, ř.3 – Co se míní symbolem $\equiv$ v Definici 18?

• s.19 a 25, bod 1 schémat – Nerozumím zápisu definice posloupností $\mathbf{srs_i}$. Zdá se, že bychom pro výpočty (a v souladu s Definicí 15) potřebovali mít v $\mathbf{srs_1}$ všechny hodnoty $[x_1^{d_1} \dots x_\mu^{d_\mu}]_1$ pro omezený stupeň příslušného monomu a v $\mathbf{srs_2}$ všechny hodnoty $[1]_2, [x_1]_2, \dots, [x_\mu]_2$, což je explicitně zmíněno na s.28 a 29.

• s.19 a 25, bod 3 schémat – Proč není na vstupu Open v souladu s Definicí 8 uveden také polynom f?