Posudek oponenta bakalářské práce

Název: Aplikace Groebnerových bází
Autor: Marie Skalová

Shrnutí obsahu práce

Práce se zabývá automatizací dokazování planimetrických tvrzení pomocí převedení problému do řeči polynomiálních rovnic a použití Gröbnerových bází. Metody jsou ilustrovány na řešených cvičeních.

Celkové hodnocení práce

Téma práce. Téma práce i jeho zpracování považuji za přiměřené a zadání za splněné.

Vlastní příspěvek. Kromě přehledu (většinou bez důkazů) potřebné teorie považuji za hlavní příspěvek autorky podrobné řešení cvičení, často s pomocí softwaru Sage.

Matematická úroveň. Text je povětšinou dobře srozumitelný a logicky členěný. Úroveň je pro formát bakalářské práce přijatelná, byť výsledek místy působí uspěchaně. Výhrady mám k závěru kapitoly 2.2 a různé méně závažné připomínky k řadě dalších míst, podrobněji níže.

Práce se zdroji. K práci se zdroji nemám připomínky.

Formální úprava. Celkově v pořádku, byť výsledek budí trochu dojem dokončování ve spěchu (např. připravené, ale nakonec neuvedené porovnání efektivity různých metod výpočtu na konci důkazů věty 14 na str. 22 a věty 15 na str. 24, kde jsou místo počtu iterací tři tečky).

Připomínky a otázky

Hlavní věcnou připomínku mám k závěru kapitoly 2.2 pod definicí 15, což zahrnuje zvlášť vysvětlení zcela klíčové definice 16. Tady dle mého názoru není text moc srozumitelný a definice 16 není zapsána formálně správně. Aspoň v mém případě světlo do celé věci vneslo až pečlivé přečtení několika citovaných stránek z monografie Cox-Little-O'Shea. Problém je způsoben poměrně nešťastným pokusem zkrátit text předlohy.

Předně v definici 16 má být specifikováno, že $W_1, \ldots, W_p$ jsou *přesně* ty komponenty z jednoznačného rozkladu V na ireducibilní komponenty, na kterých jsou proměnné $u_1, \ldots, u_n$ algebraicky nezávislé. Existence a jednoznačnost tohoto rozkladu, které jsou zrovna tady dost potřeba, aby definice dávala dobrý smysl, mimochodem nejsou v práci (hodily by se do kap. 1.1) pořádně vysvětleny.

Odstavec těsně nad definicí 16, který začíná větou „Z předchozího výkladu plyne …,“ zase argumentačně fauluje. Co přesně tady „z předchozího výkladu plyne“? To totiž objasňuje až vynechaná část kap. 6.4 z monografie. Odpovídající termín v definici 16 je v originále totiž, že „the conclusion g *generically* follows from the hypotheses“, což by se přeložilo, že „závěr g *v obecném případě* plyne z předpokladů“. Obecným případem se tady myslí volba parametrů $u_1, \ldots, u_n$ tak, aby nebyly nulou polynomu c z Proposition 8 na str. 300 v monografii (nuly c jsou ty speciální, degenerované případy, kde závěr nemusí platit). Tím pádem se vlastně ukazuje, že postup z Cox-Little-O'Shea je obecnější než ten jednodušší alternativní ze skript kolegů Barta a Stanovského—v postupu ze skript musíme identifikovat degenerované případy předem, zatímco v práci nepopsaná část postupu z Cox-Little-O'Shea nám najde i to, které případy jsou degenerované.

Uznávám, že odstavec výše mohl být oprávněně uznán nad rámec práce, ale v tom případě by redukce materiálu kolem klíčového pojmu určitě zasloužila precizněji vedený řez.

Nakonec uvádím méně závažné připomínky:

1. Osobně preferuji, když mají tvrzení a definice jednu číselnou řadu, protože to usnadňuje navigaci v textu.
2. V první odrážce definice 9 je více překlepů. Co je A—patrně množina těch monočlenů, u kterých má f nenulový koeficient?
3. Možná by pojem báze ideálu mohl být někde definován. V daném významu se ten pojem až na Hilbertovu větu o bázi moc nepoužívá a vysvětlen je vlastně až ve znění věty 6 na str. 6.
4. Definice 13 zavádí zbytek po dělení polynomů více proměnných jako výstup následného algoritmu a v popisu algoritmu zas jen stručně je, že bude vracet zbytek po dělení polynomů více proměnných, což trochu zavání definicí kruhem (byť to tak není). Dále je vztah s větou 7 bezprostředně nad tím nechán implicitně k rozmyšlení laskavému čtenáři. I když jde o celkem přímočarou věc, pořád si myslím, že tahle pasáž na pomezí str. 6 a 7 by zasloužila napsat pečlivěji.
5. Str. 7, krok algoritmu 1.c.i má být: **if** $\mathrm{LT}_>(f_i) \mid \mathrm{LT}_>(p)$ **then**:
6. Str. 14, řádek 13 zdola: přesněji by *redukovaná* Gröbnerova báze toho ideálu měla být $\{1\}$.
7. Str. 14, řádek 5 zdola: předpokládám, že se máme podívat na *ireducibilní* rozklad množiny V (ten pojem měl být někde vysvětlen).
8. Důkaz Lemmatu 10 na str. 15, rovnost „$\mathrm{Ker}(\phi) = \langle x_1 - f \rangle$“: Jak přesně se dokazuje ekvivalence

   $h(f, x_2, \ldots, x_n) = 0 \iff h(x_1, \ldots, x_n) = 0$ nebo $h(x_1, \ldots, x_n) = \tilde{h} \cdot (x_1 - f)$ pro nějaké $\tilde{h} \neq 0$?
9. Důkaz věty 9, popis struktury na str. 16: Podle toho, co se dál skutečně dokazuje, soudím, že v prvních dvou krocích má být místo $I_1 \cap I_2 \cap I_3 = \mathrm{Rad}(I)$ spíš $J_1 \cap J_2 \cap J_3 = \mathrm{Rad}(J)$. Dál by taky neškodilo na začátku důkazu jasně vysvětlit, že úkrok přes okruh racionálních čísel je tam proto, že se používají výpočty v Sage a ty samozřejmě lze provést jen pro okruh polynomů s racionálními koeficienty místo reálných.
10. V druhém odstavci na str. 19 bych úplně neřekl, že „tato množina je rovna $\mathbf{V}(I \cup \{h_{m+1} \cdot x_{n+1} - 1\})$.“ Když už nic jiného, zmiňovaná množina je podmnožina $\mathbb{A}^n_K$, zatímco

   $$\mathbf{V}(I \cup \{h_{m+1} \cdot x_{n+1} - 1\}) \subseteq \mathbb{A}^{n+1}_K.$$

   Vysvětlení dále v odstavci je přesnější.
11. Důkaz věty 13 na str. 20: Vzorec s cosiny neodpovídá znění věty, říká spíš, že čtverec cosinu *dvojnásobku* obvodového úhlu je roven čtverci cosinu středového úhlu.
12. Str. 22, důkaz věty 14: Jelikož ideál množiny W_1 obsahuje polynom b_1, rovnost $b_1 = 0$ je pro body W_1 nejen povolena, jak se v práci píše, ale přímo vynucena. To je to, o co nakonec jde!
13. Str. 24, druhý důkaz věty 15: Totéž co v předchozím bodě, jen ještě o poznání více nepřesné. Polynomy c_2 a b_1 v Gröbnerových bázích pro W_1 a W_3 uvedeny nejsou a mám pochyby, jestli v daných ideálech vůbec jsou. Pro aplikaci metody ale stačí jen nenulový polynom v proměnných b_1, c_1, c_2 v ideálech W_1 a W_3 (aby tyto proměnné byly algebraicky závislé na daném W_i). Takové polynomy se z uvedených bází sice vykoukat dají, ale záhadou mi zůstává, proč to není nijak vysvětleno. Navíc celý problém, proč se takové polynomy v Gröbnerových bázích neobjevují přímo, je podle Theorem 2 na str. 116 v Cox-Little-O'Shea nejspíše způsoben pouze nevhodnou volbou monomiálního uspořádání.

Závěr

Práci doporučuji uznat jako bakalářskou práci.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

doc. RNDr. Jan Šťovíček, Ph.D.
Katedra algebry MFF UK
20. 8. 2020