FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

UNIVERZITA KOMENSKÉHO
V BRATISLAVE

DIPLOMOVÁ PRÁCA

2004 Peter Novotný

FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
UNIVERZITY KOMENSKÉHO V BRATISLAVE
KATEDRA ALGEBRY A TEÓRIE ČÍSEL

DIPLOMOVÁ PRÁCA

Využitie Gröbnerových báz na dôkazy viet elementárnej geometrie

DIPLOMANT: PETER NOVOTNÝ
ŠKOLITEĽ: RNDR. JAROSLAV GURIČAN, CSC.

BRATISLAVA 2004

Čestné vyhlásenie:
Čestne vyhlasujem, že predkladanú prácu som vypracoval samostatne pod odborným vedením školiteľa len s použitím uvedenej literatúry.

. . . . . .
Peter Novotný

Poďakovanie

V prvom rade sa chcem poďakovať môjmu školiteľovi Jaroslavovi Guričanovi za čas, ktorý mi venoval, za pomoc pri riešení otázok spojených s diplomovou prácou a za užitočnú literatúru, ktorú mi poskytol. Ďakujem ďalej spolubývajúcim za ich asistenciu pri odstraňovaní softvérových problémov a tolerantný prístup. A významná vďaka patrí aj mojej rodine a priateľke za ich neustálu materiálnu a duševnú podporu a spoluprácu pri odstraňovaní štylistických a gramatických chýb.

Abstrakt

Touto diplomovou prácou predstavujeme teóriu Gröbnerových báz v okruhoch polynómov viacerých premenných. Popisujeme základné vlastnosti redukcie, dôvod existencie a algoritmus na nájdenie bázy. Ukazujeme rôzne aplikácie teórie, pričom dôraz kladieme na jej využitie pri dokazovaní viet elementárnej geometrie pomocou výpočtovej techniky. Účinnost' tejto metódy prezentujeme na riešení úloh medzinárodných matematických olympiád.

Obsah

Kapitola 1

Úvod

Niet pochýb o tom, že polynómy hrajú v matematike dôležitú rolu. Môžeme ich chápať ako funkcie na ľubovoľnej množine, na ktorej sú definované operácie sčítania a násobenia – z mnohého spomeňme ich využitie v analýze (Taylorov polynóm funkcie jednej či viacerých premenných) a v numerickej matematike (Čebyševove polynómy). Takisto ale vystupujú ako samostatná štruktúra. Pomocou polynómov sa tak napríklad dajú charakterizovať všetky konečné polia. Účinne sa aplikujú v teórii kódovania a pri symbolických výpočtoch.

Problémy, ktoré sa týkajú priamo polynómov alebo úlohy, ktoré je možné na polynómy transformovať, sa často dajú formulovať v reči *polynomických ideálov*. Aby sme toto nahliadli, pozrime sa na takúto veľmi jednoduchú úlohu.

Príklad 1.1. Máme k dispozícii neobmedzené množstvo mincí v hodnotách a a b korún (a a b sú prirodzené). Platíme s nimi v obchode, pričom vydať nám môžu tiež iba mincami v hodnotách a a b. Ktoré všetky obnosy možno takto zaplatiť?

Zrejme každý obnos S, ktorý možno zaplatiť, sa musí dať vyjadriť v tvare

$$S = ma + nb\,, \tag{1.1}$$

kde m a n sú nejaké celé čísla. A naopak, každý obnos, ktorý sa dá takto vyjadriť, dá sa aj zaplatiť. Na uspokojivé riešenie úlohy nám teda dobre poslúži známy fakt z teórie čísel, že v tvare (1.1) sa dajú zapísať práve násobky najväčšieho spoločného deliteľa čísel a a b (označujeme ho (a, b), v ďalšom texte budeme používať skrátený termín NSD). Hodnotu (a, b) pritom poľahky nájdeme *Euklidovým algoritmom*.

□

Uvedenú úlohu možno samozrejme zovšeobecniť na ľubovoľný konečný počet hodnôt mincí. Zovšeobecňovať však môžeme aj iným smerom. Hodnoty a a b (a k nim prislúchajúce m a n) v príklade 1.1 nemusia byť iba celými číslami, môžu to byť prvky hocakého okruhu. Zaoberajme sa chvíľu prípadom, keď týmto okruhom je okruh polynómov jednej premennej nad poľom $\mathbb{F}$ (označujeme ho $\mathbb{F}[x]$).

Príklad 1.2. Máme teda polynómy $p(x)$ a $q(x)$. Zaplatiť vieme každý polynóm $s(x)$, ktorý sa dá napísať v tvare

$$s(x) = f(x)p(x) + g(x)q(x)\,,$$

kde $f(x), g(x) \in \mathbb{F}[x]$. Slovko *zaplatiť* v tomto zmysle chápeme tak, že vezmeme f-krát polynóm p a pripočítame k nemu g-krát polynóm q – rovnako ako pri minciach. Avšak f a g sú polynómy.

Odpoveď, ktoré všetky obnosy vieme zaplatiť polynómami p a q, dostaneme rovnako ľahko ako v príklade 1.1. Opäť to budú všetky (polynomické) násobky polynómu (p, q), ktorý nájdeme Euklidovým algoritmom. Pri väčšom (konečnom) počte polynómov, ktorými môžeme platiť, je situácia podobná, stačí zobrať NSD všetkých zadaných polynómov, ktorý dostaneme rekurentným použitím rovnosti

$$(q_1, \ldots, q_n) = ((q_1, \ldots, q_{n-1}), q_n)\,.$$

Otázke, čo v prípade nekonečného počtu polynómov, ktorými môžeme platiť, sa budeme venovať o chvíľu.

□

Prirodzeným spôsobom vzniká otázka, ako to bude pri polynómoch viacerých premenných. Nápad zobrať aj tu NSD zlyhá hneď na začiatku, ako ukazuje nasledujúci príklad. Okrem toho, nájsť NSD dvoch polynómov viacerých premenných nie je vo všeobecnosti také ľahké ako v prípade polynómov jednej premennej.

Príklad 1.3. Pre polynómy $p = x^2$, $q = xy$ z $\mathbb{Q}[x, y]$ (takto označujeme okruh polynómov dvoch premenných nad poľom racionálnych čísel) máme $(p, q) = x$, avšak polynóm x nimi zaplatiť nevieme. Skutočne, v každom polynóme tvaru $fp + gq$ (tieto vieme zaplatiť) bude každý člen (po roznásobení) deliteľný x^2 alebo xy, takže polynóm x sa takto nemôže dať vyjadriť.

□

Aby sme mohli vyriešiť nastolenú otázku, zaveďme si presnejšie pojem *dá sa zaplatiť*. Urobme tak rovno pre ľubovoľný (aj nekonečný) počet polynómov, aj keď sa vzápätí nepríjemnej podmienky nekonečnosti zbavíme. Vopred sa ešte dohodnime, že okruh $\mathbb{F}[x_1, \ldots, x_n]$ (je to okruh polynómov n premenných nad poľom $\mathbb{F}$) budeme označovať $\mathbb{F}[\mathbf{x}]$.

Definícia 1.1. Majme okruh polynómov $\mathbb{F}[\mathbf{x}]$ a množinu Q, ktorá je jeho podmnožinou. Potom množinu polynómov

$$\langle Q \rangle = \left\{ \sum_{i=1}^{k} f_i q_i \ : \ f_i \in \mathbb{F}[\mathbf{x}],\ q_i \in Q,\ k = 0, 1, 2, \dots \right\} \tag{1.2}$$

nazývame *ideál* generovaný množinou Q a množinu Q nazývame *báza* ideálu $\langle Q \rangle$.

□

Pojem ideálu sa zvykne definovať všeobecnejšie pre ľubovoľný okruh ako jeho podokruh, ktorého každý prvok po vynásobení ľubovoľným prvkom z celého okruhu ostane v ňom. Táto charakteristika je ekvivalentná s našou, my si však v celom texte vystačíme s definíciou 1.1.

Náš problém preto môžeme preformulovať takto. Daná je množina $Q \subseteq \mathbb{F}[\mathbf{x}]$. Ako vyzerá množina $\langle Q \rangle$? Alebo presnejšie, ako pre daný polynóm $p \in \mathbb{F}[\mathbf{x}]$ určíme, či $p \in \langle Q \rangle$? Skúšať dosadzovať v (1.2) za f_i a q_i rôzne polynómy a zisťovať, či výsledok je p, nie je najlepšie riešenie vzhľadom na nekonečnosť $\mathbb{F}[\mathbf{x}]$ a možnú nekonečnosť Q.

O báze Q ale môžeme predpokladať, že je konečná. Okruh $\mathbb{F}[\mathbf{x}]$ je totiž *noetherovský obor integrity*. To znamená, že každý ideál v ňom má konečnú bázu. Vyplýva to z nasledujúcej vety.

Veta 1.1. (*Hilbertova o báze*.) Ak $\mathbb{D}$ je noetherovský obor integrity, je ním aj $\mathbb{D}[x]$.

□

Akékoľvek pole má len dva ideály – celé pole a množinu $\{0\}$. Oba majú konečnú bázu (dokonca jednoprvkovú). A každé pole je aj oborom integrity. Čiže každé pole $\mathbb{F}$ spĺňa predpoklad vety 1.1. Jej induktívnym použitím dostaneme, že aj $\mathbb{F}[\mathbf{x}]$ je noetherovský. Viac o noetherovských oboroch integrity a aj dôkaz vety 1.1 možno nájsť v [1]. My vetu ponecháme bez dôkazu, nakoľko aplikácie, ktorým sa budeme venovať, vystupujú automaticky s konečnými bázami.

Finálne zadanie problému patrenia do polynomického ideálu (skúšal ho riešiť už v roku 1926 Hermann [2]) teda znie nasledovne. Máme polynómy $q_1, \dots, q_m \in \mathbb{F}[\mathbf{x}]$. Ako pre daný $p \in \mathbb{F}[\mathbf{x}]$ určíme, či $p \in \langle \{q_1, \dots, q_m\} \rangle$? Množinové zátvorky budeme v tomto prípade na sprehľadnenie zápisu ďalej vynechávať. V spojení s definíciou 1.1 platí

$$\langle q_1, \dots, q_m \rangle = \left\{ \sum_{i=1}^{m} f_i q_i \ : \ f_i \in \mathbb{F}[\mathbf{x}] \right\}. \tag{1.3}$$

Ak niektorý z polynómov q_i vo vyjadrení (1.3) nechceme použiť, jednoducho ho použijeme a príslušné f_i dáme nulové.

Spomeňme si na jednu zaujímavú vlastnosť ideálov. Okruh sa dá podľa nich faktorizovať. Presnejšie povedané, relácia $\sim$ na $\mathbb{F}[\mathbf{x}]$ definovaná

$$p_1 \sim p_2 \qquad \Longleftrightarrow \qquad p_1 - p_2 \in \langle Q \rangle$$

je reláciou ekvivalencie. Okruh $\mathbb{F}[\mathbf{x}]$ sa podľa nej dá rozložiť na triedy ekvivalencie, pričom jednou triedou je práve $\langle Q \rangle$. Keby sme pre každý polynóm p vedeli nájsť reprezentanta triedy, do ktorej patrí, problém patrenia do ideálu by bol vyriešený. Stačilo by zistiť, či $p \sim 0$ (t. j. či triedy polynómov p a 0 majú toho istého reprezentanta). Hľadáme teda *kanonickú funkciu* $\varphi : \mathbb{F}[\mathbf{x}] \longrightarrow \mathbb{F}[\mathbf{x}]$ s vlastnosťami

(*i*) $\forall p \in \mathbb{F}[\mathbf{x}] \qquad \varphi(p) \sim p\,,$

(*ii*) $\forall p_1, p_2 \in \mathbb{F}[\mathbf{x}] \qquad p_1 \sim p_2 \quad \Longrightarrow \quad \varphi(p_1) = \varphi(p_2)\,.$

Namiesto druhej podmienky by nám stačila aj vlastnosť

(*ii*)' $\forall p \in \mathbb{F}[\mathbf{x}] \qquad p \sim 0 \quad \Longrightarrow \quad \varphi(p) = \varphi(0)$

(vtedy hovoríme o *normálnej funkcii*), ale neskôr sa ukáže, že silnejší predpoklad nebude na škodu. Pritom nájsť normálnu funkciu nie je v tomto prípade o nič jednoduchšie ako nájsť kanonickú funkciu.

Skôr, ako sa pustíme do hľadania, spomeňme, že tento problém úplne vyriešil Buchberger [3]. Jeho prístup spočíva v transformácii pôvodnej bázy ideálu na novú (v istom zmysle lepšiu), z ktorej sa kanonická funkcia vytvorí prirodzenou cestou. Takúto novú bázu nazval (podľa svojho školiteľa) *Gröbnerova báza*. O jej existencii a vytvorení pojednáva nasledujúca kapitola.

Kapitola 2

Gröbnerove bázy

2.1 Usporiadanie členov

V úvodnej kapitole sme zistili, že pre polynómy viacerých premenných nefunguje postup, ktorý sa používa pre polynómy jednej premennej (pozri príklad 1.3). Nezavrhneme ho hneď, radšej sa detailnejšie pozrieme ako funguje.

Príklad 2.1. Keď máme nejaký ideál $\langle q \rangle \subseteq \mathbb{F}[x]$ (je generovaný jedným polynómom, pretože ak by mal viac ako jeden generátor, stačí ich nahradiť ich NSD, pozri príklad 1.2) a chceme zistiť, či polynóm p do neho patrí, postupne odčitujeme od p čo najväčšie násobky q (v praxi hovoríme, že polynóm p delíme polynómom q). Ak dostaneme nulový polynóm, tak $p \in \langle q \rangle$ (spätne vyjadríme p ako súčet násobkov q). Ak dostaneme nenulový polynóm p', ktorého *stupeň* je nižší ako stupeň q, tak $p \notin \langle q \rangle$. Prirodzenou cestou tak vlastne máme definovanú kanonickú funkciu $\varphi(p) = p'$ na $\mathbb{F}[x]$.

□

Pri polynómoch viacerých premenných nemáme apriori dané niečo ako stupeň polynómu. Ak chceme navrhnúť podobný postup ako pri polynómoch jednej premennej, musíme najprv preklenúť túto prekážku. Na to bude dobré zaviesť si nasledujúci termín.

Definícia 2.1. Množinou *termov* v $\mathbf{x}$ je

$$\mathbb{T}_{\mathbf{x}} = \left\{ x_1^{i_1} \cdots x_n^{i_n} \ : \ i_1, \ldots, i_n \in \mathbb{N} \right\} ,$$

kde $\mathbb{N}$ je množina nezáporných celých čísel.

□

Všimnime si, že termy tvoria bázu pre $\mathbb{F}[\mathbf{x}]$, keď ho berieme ako vektorový priestor. Každý polynóm možno jednoznačne vyjadriť ako súčet konečného počtu termov prenásobených nejakými koeficientami z $\mathbb{F}$. Dohodnime sa, že jeden nenulový sčítanec (t. j. term prenásobený nenulovým koeficientom) budeme nazývať *člen*, prípadne *jednočlen*.

Na $\mathbb{T}_{\mathbf{x}}$ máme zatiaľ iba reláciu delenia zdedenú z okruhu $\mathbb{F}[\mathbf{x}]$. Inak povedané,

$$x_1^{i_1} \cdots x_n^{i_n} \mid x_1^{j_1} \cdots x_n^{j_n} \qquad \Longleftrightarrow \qquad i_k \leq j_k,\ k = 1, \ldots, n\,.$$

Stupeň z polynómov jednej premennej nahradíme vhodným usporiadaním množiny $\mathbb{T}_{\mathbf{x}}$. Nemôže to byť ľubovoľné usporiadanie. Musíme ho zvoliť tak, aby fungovalo zovšeobecnenie postupu z príkladu 2.1. Toto zovšeobecnenie presnejšie popíšeme v ďalšej podkapitole. Jasné je, že nejakým spôsobom budeme odpočítavať násobky generátorov ideálu od testovaného polynómu tak, aby sa termy v ňom (v zmysle nového usporiadania) zmenšovali. Preto bude žiadúce, aby naše usporiadanie spĺňalo nasledujúcu vlastnosť.

Definícia 2.2. *Prípustné úplné usporiadanie* $<_T$ množiny $\mathbb{T}_{\mathbf{x}}$ je také, ktoré vyhovuje podmienkam

(*i*) $1 \leq_T t\,,$

(*ii*) $s < t \quad \Longrightarrow \quad s \cdot u < t \cdot u$

pre všetky $s, t, u \in \mathbb{T}_{\mathbf{x}}$, kde $1 = x_1^0 \cdots x_n^0$.

□

Dôsledkom tejto definície je

$$\forall s, t \in \mathbb{T}_{\mathbf{x}} \qquad s \mid t \quad \Longrightarrow \quad s \leq_T t\,, \tag{2.1}$$

pretože ak $s \mid t$, tak $t = us$ pre nejaké $u \in \mathbb{T}_{\mathbf{x}}$, v definícii 2.2 podľa (*i*) $1 \leq_T u$ a tak podľa (*ii*) $s = 1 \cdot s \leq_T u \cdot s = t$.

Prípustných usporiadaní je viacero. Venovať sa budeme dvom, ktoré sú najpraktickejšie a bežne sa používajú v literatúre. Všetky tvrdenia v tejto kapitole ale platia pre ľubovoľné pevne dané prípustné usporiadanie a takto ich budeme aj formulovať (bez ďalšieho upozornenia).

Prvé usporiadanie je motivované abecedou. V každom terme nahradíme časť $x_k^{i_k}$ reťazcom i_k po sebe idúcich k-tych znakov abecedy. Na koniec pridáme posledný znak abecedy (tak zabezpečíme, aby napríklad platilo $1 < x_k^1 <_T x_k^2 <_T \cdots$). Výsledné slová nakoniec zoradíme podľa abecedy (t. j. slovo, ktoré je v abecede skôr, reprezentuje term, ktorý je v zmysle usporiadania väčší). Aplikovaním popísaného pravidla napríklad dostaneme $1 <_T x_1^2 x_3^2 <_T x_1^2 x_2$, pretože

`aabz` je v abecede skôr ako `aaccz` a to je skôr ako `z`. Stručnejšia ekvivalentná charakterizácia je nasledovná.

Definícia 2.3. *Lexikografické* usporiadanie termov definujeme

$$x_1^{i_1}\cdots x_n^{i_n} <_L x_1^{j_1}\cdots x_n^{j_n} \qquad \Longleftrightarrow \qquad \exists \ell \quad \text{také, že} \quad i_\ell < j_\ell \quad \text{a} \quad i_k = j_k,\ 1 \le k < \ell\,.$$

□

Zavedením lexikografického usporiadania sme od seba úplne odlíšili jednotlivé premenné. Iné usporiadanie získame, ak najprv na množine termov zavedieme funkciu *stupeň* ako

$$\deg(x_1^{i_1}\cdots x_n^{i_n}) = i_1 + \cdots + i_n\,. \tag{2.2}$$

Termy potom usporiadame podľa ich stupňov, pričom termy s rovnakým stupňom zoradíme *inverzným* lexikografickým usporiadaním (mohli by sme použiť aj lexikografické). Máme teda druhý predpis.

Definícia 2.4. (*Totálne*) *stupňové* usporiadanie termov definujeme

$$\begin{aligned} s = x_1^{i_1}\cdots x_n^{i_n} <_D x_1^{j_1}\cdots x_n^{j_n} = t \qquad &\Longleftrightarrow \\ \deg(s) < \deg(t) \qquad &\text{alebo} \\ \deg(s) = \deg(t) \quad \text{a} \quad \exists \ell \quad &\text{také, že} \quad i_\ell > j_\ell \quad \text{a} \quad i_k = j_k,\ \ell < k \le n\,. \end{aligned}$$

□

Toto usporiadanie trochu viac pripomína stupeň pri polynómoch jednej premennej. Pri aplikáciách v ďalších kapitolách uvidíme, aké sú výhody prvej či druhej definície.

Uvedomme si teraz dve významné vlastnosti týkajúce sa $\mathbb{T}_{\mathbf{x}}$ a usporiadania $<_T$, ktoré neskôr zohrajú dôležitú úlohu.

Veta 2.1. Neexistuje nekonečná postupnosť termov $t_1, t_2, \ldots$ z $\mathbb{T}_{\mathbf{x}}$ taká, že

$$\forall k = 1, 2, \ldots \quad \forall i = 1, \ldots, k-1 \qquad t_i \nmid t_k\,. \tag{2.3}$$

Inými slovami, nemožno vytvoriť nekonečnú postupnosť termov takú, že žiadny term nie je násobkom ani jedného z predchádzajúcich.

Ukážeme si dva dôkazy tejto vety. Prvý, kratší, využíva známu netriviálnu vlastnosť noetherovských oborov integrity. Druhý je komplikovanejší, ale elementárny a neodvoláva sa na zbytočne silné výsledky z teórie okruhov.

Dôkaz 1: Predpokladajme sporom, že taká postupnosť existuje. Označme $T_k = \{t_1, \ldots, t_k\}$, pričom chápeme t_i ako polynómy (t. j. členy s jednotkovými koeficientami), čiže $T_k \subset \mathbb{F}[\mathbf{x}]$. Žiaden polynóm sa v postupnosti neopakuje (bol by násobkom sám seba), máme preto inklúzie $T_1 \subsetneq T_2 \subsetneq \cdots$. Akýkoľvek polynóm z ideálu $\langle T_k \rangle$ je podľa (1.3) tvaru

$$f_1 t_1 + \cdots + f_k t_k \,. \tag{2.4}$$

Keďže t_i sú jednočleny, každý člen tohto vyjadrenia je násobkom niektorého z $t_1, \ldots, t_k$. Podľa predpokladu vety t_{k+1} nie je násobkom žiadneho prvku z T_k a teda sa nedá zapísať v tvare (2.4) a $t_{k+1} \notin \langle T_k \rangle$. Pritom $t_{k+1} \in \langle T_{k+1} \rangle$, dostávame teda vlastné inklúzie

$$\langle T_1 \rangle \subsetneq \langle T_2 \rangle \subsetneq \cdots \,.$$

Keďže $\mathbb{F}[\mathbf{x}]$ je noetherovský, takýto reťazec ideálov nemôže byť podľa *Hilbertovej podmienky* nekonečný (pozri napríklad [1]). Dospeli sme k sporu.

Dôkaz 2: Tvrdenie dokážeme indukciou podľa počtu premenných v $\mathbb{F}[\mathbf{x}]$. V prípade jednopremenného okruhu $\mathbb{F}[x_1]$ je situácia jasná. Ak $t_1 = x_1^m$, potom postupnosť $t_1, t_2, \ldots$ môže mať najviac $m+1$ prvkov, lebo každý nasledujúci term musí mať x_1 s exponentom menším ako predchádzajúci. Prepokladajme, že tvrdenie platí pre okruh $\mathbb{F}[x_1, \ldots, x_{n-1}]$. Ukážeme, že potom platí aj pre $\mathbb{F}[x_1, \ldots, x_n]$.

Sporom nech to neplatí a máme nekonečnú postupnosť termov

$$t_1, t_2, \ldots, \qquad t_k = x_1^{i_{1,k}} \cdots x_n^{i_{n,k}} \,,$$

pričom t_k nie je násobkom žiadneho termu pred ním. Pozrime sa v termoch na exponenty premennej x_n, t. j. sledujme postupnosť $i_{n,1}, i_{n,2}, \ldots$.

Ak by sa z nej dala vybrať neklesajúca podpostupnosť $i_{n,k_1} \leq i_{n,k_2} \leq \cdots$, príslušná vybraná podpostupnosť termov $t_{k_1}, t_{k_2}, \ldots$ by musela spĺňať vlastnosť (2.3) aj po odstránení premenných x_n (lebo pred odstránením ju spĺňa a premenná x_n – keďže jej exponenty neklesajú – na ňu nemá vplyv). To je v spore s indukčným predpokladom.

Teda z postupnosti $i_{n,1}, i_{n,2}, \ldots$ sa nedá vybrať neklesajúca podpostupnosť. Taká postupnosť nezáporných celých čísel neexistuje, lebo každá postupnosť je buď neohraničená – vtedy sa z nej dá vybrať dokonca rýdzorastúca postupnosť – alebo ohraničená – vtedy nadobúda len konečne

veľa hodnôt a vieme z nej vybrať stacionárnu (tým pádom neklesajúcu) postupnosť. Tým je indukčný krok dokončený.

□

Veta 2.2. Neexistuje nekonečná postupnosť termov $t_1, t_2, \ldots$ z $\mathbb{T}_{\mathbf{x}}$ spĺňajúca $t_1 >_T t_2 >_T \cdots$.

Dôkaz: Ak by každý ďalší term bol menší od predchádzajúceho (a teda aj od všetkých pred ním), podľa (2.1) by ani jeden z nich nebol jeho deliteľom. Postupnosť $t_1, t_2, \ldots$ by teda spĺňala predpoklady kladené vo vete 2.1, čo je v spore s tvrdením tejto vety.

□

Zrejme každý nenulový polynóm v $\mathbb{F}[\mathbf{x}]$ obsahuje nenulový člen, ktorého term je v zmysle usporiadania najväčší. Tento bude hrať významnú rolu pri ďalších úvahách, preto si preň zaveďme označenie.

Definícia 2.4. *Vedúci člen* polynómu $p \in \mathbb{F}[\mathbf{x}]$ vzhľadom k $<_T$ je člen vystupujúci v p, ktorého term je maximálny spomedzi všetkých termov prislúchajúcich členom v p. Označíme ho $\mathrm{M}_T(p)$, alebo iba $\mathrm{M}(p)$, ak je zrejmé, ktoré usporiadanie berieme. Označme ešte $\mathrm{ht}(p)$ *vedúci term* a $\mathrm{hc}(p)$ príslušný *vedúci koeficient*. Spolu máme

$$\mathrm{M}(p) = \mathrm{hc}(p)\mathrm{ht}(p)\,.$$

Pre úplnosť položme $\mathrm{hc}(0) = 0$ a $\mathrm{ht}(0) = 1$, majme však na vedomí, že v skutočnosti nulový polynóm nemá žiaden (ani vedúci) člen.

□

Podobne ako v príklade 2.1, budeme chcieť aj pri polynómoch viacerých premenných nahrádzať postupne testovaný polynóm p novými polynómami p', ktoré budú v tej istej triede ($p \sim p'$) a ktoré budú v zmysle $<_T$ menšie. Bude preto užitočné zaviesť reláciu (neúplného) usporiadania aj na množine polynómov.

Definícia 2.5. Hovoríme, že polynóm p je *jednoduchší* ako polynóm q vzhľadom na $<_T$ a píšeme $p \prec_T q$ (v praxi iba $p \prec q$), ak platí

$$\{\quad \mathrm{ht}(p) = \mathrm{ht}(q) = 1 \quad \text{a} \quad p = 0 \neq q \quad \} \qquad \text{alebo}$$
$$\mathrm{ht}(p) <_T \mathrm{ht}(q) \qquad \text{alebo} \qquad \{\quad \mathrm{ht}(p) = \mathrm{ht}(q) \quad \text{a} \quad p - \mathrm{M}(p) \prec q - \mathrm{M}(q) \quad \}\,.$$

Ak $p \not\prec q$ a $p \not\succ q$, budeme písať $p \asymp q$.

□

Relácia $\prec$ je vybudovaná rekurentne. V princípe, keď podľa nej porovnávame dva polynómy, pozrieme sa na termy ich vedúcich členov. Ak sú rovnaké, pozrieme sa na ich ďalšie členy v poradí a tak ďalej. V momente, keď narazíme na členy s rôznymi termami, určíme, ktorý polynóm je jednoduchší. Pri ďalšom výklade nám pomôže prirodzene sa ponúkajúca vlastnosť relácie $\prec$, ktorú popíšeme vo vete.

Veta 2.3. Postupnosť polynómov $p_0 \succ p_1 \succ \cdots$ nemôže byť nekonečná.

Dôkaz: Postupujme sporom. Nech je daná postupnosť nekonečná. Z definície 2.5 máme

$$\mathrm{ht}(p_0) \geq_T \mathrm{ht}(p_1) \geq_T \cdots .$$

Ak by sme v tomto zápise mohli $\geq_T$ nekonečne veľa krát nahradiť znakom $>_T$, mali by sme nekonečnú klesajúcu postupnosť termov, čo protirečí vete 2.2. Takže postupnosť vedúcich termov je od určitého polynómu p_{m_1} konštantná. Isto $t_1 = \mathrm{ht}(p_{m_1}) \neq 1$, inak by za polynómom p_{m_1} nemohlo byť nekonečne veľa jednoduchších polynómov. Vygenerujme nové polynómy $p_{1,i}$ odpočítaním vedúcich členov, t. j.

$$p_{1,i} = p_i - \mathrm{M}(p_i) \qquad i = m_1, m_1 + 1, \ldots$$

Podľa definície 2.5 platí

$$p_{1,m_1} \succ p_{1,m_1+1} \succ \cdots .$$

Z tých istých dôvodov ako v predchádzajúcich riadkoch aj táto postupnosť má vedúce termy od určitého polynómu p_{1,m_2} konštantné a $t_2 = \mathrm{ht}(p_{1,m_2}) \neq 1$, naviac

$$t_1 = \mathrm{ht}(p_{m_1}) >_T \mathrm{ht}(p_{m_1} - \mathrm{M}(p_{m_1})) = \mathrm{ht}(p_{1,m_1}) \geq_T \mathrm{ht}(p_{1,m_2}) = t_2 .$$

Opäť vygenerujeme nové polynómy odpočítaním vedúcich členov, atď.

Induktívne vyrobíme nekonečnú postupnosť termov $t_1 >_T t_2 >_T \cdots$, taká však podľa vety 2.2 neexistuje.

□

Máme tak pripravené všetko, aby sme mohli skúsiť vyrobiť kanonickú funkciu pre daný ideál založenú na zjednodušovaní polynómu.

2.2 Redukcia a jej základné vlastnosti

Ak chceme zistiť, či polynóm p patrí do ideálu s bázou $Q = \{q_1, \ldots, q_m\}$, môžeme postupovať tak, že postupne zjednodušujeme p, pričom stále ostávame v tej istej triede rozkladu $\mathbb{F}[\mathbf{x}]/\langle Q\rangle$. O jednoduchšom polynóme sa bude dať hádam ľahšie rozhodnúť, či do $\langle Q\rangle$ patrí. Princíp zjednodušovania presne kopíruje príklad 2.1. Detailne si ho popíšme a preskúmajme jeho vlastnosti.

Definícia 2.6. Pre nenulové $p, q \in \mathbb{F}[\mathbf{x}]$ hovoríme, že p *sa redukuje modulo* q (vzhľadom k danému $<_T$), ak existuje jednočlen v p, ktorý je deliteľný $\mathrm{ht}(q)$. Ak $p = \alpha t + r$, kde $\alpha \in \mathbb{F} - \{0\}$, $t \in \mathbb{T}_{\mathbf{x}}$, $r \in \mathbb{F}[\mathbf{x}]$ a $t/\mathrm{ht}(q) = u \in \mathbb{T}_{\mathbf{x}}$, potom píšeme

$$p \mapsto_q p - \frac{\alpha t}{\mathrm{M}(q)} \cdot q = p - \frac{\alpha}{\mathrm{hc}(q)} u \cdot q = p'$$

a hovoríme, že p *sa redukuje na* p' (*modulo* q). Ak $p \mapsto_q p'$ pre nejaké $q \in Q = \{q_1, \ldots, q_m\}$, hovoríme, že p *sa redukuje modulo* Q a píšeme $p \mapsto_Q p'$, inak hovoríme, že p je *ireducibilný* (alebo *redukovaný*) *modulo* Q. Dohodnime sa, že polynóm 0 je vždy ireducibilný modulo Q.

□

Definícia 2.6 formálne popisuje presne to, o čom sme hovorili na predchádzajúcich stranách. Zápis $p \mapsto_q p'$ hovorí, že po odpočítaní vhodného násobku q od p dostaneme p', pričom $p \sim p'$ a $p \succ p'$ (z p ubudol člen αt a pribudli iba členy s menšími termami). Zrejmá je aj nasledujúca vlastnosť redukcie.

Veta 2.4. Pre danú množinu Q a usporiadanie $<_T$ neexistuje nekonečná postupnosť redukcií

$$p_0 \mapsto_Q p_1 \mapsto_Q \cdots .$$

Dôkaz: Z definície 2.6 je jasné (ako sme už poznamenali), že ak $p \mapsto_q p'$, tak $p \succ p'$. Ak by existovala zobrazená postupnosť, mali by sme $p_0 \succ p_1 \succ \cdots$, čo je v spore s vetou 2.3.

□

Význam redukcie $\mapsto_Q$ je v tom, že ju môžeme na jeden polynóm použiť opakovane, kým nedostaneme polynóm ireducibilný modulo Q. Bude výhodné zaviesť nasledovnú notáciu.

Definícia 2.7. *Reflexívny tranzitívny uzáver* relácie $\mapsto_Q$ označujeme $\mapsto_Q^+$. To znamená, že $p \mapsto_Q^+ p'$ práve vtedy, keď existuje postupnosť polynómov (môže byť aj triviálna) taká, že

$$p = p_0 \mapsto_Q p_1 \mapsto_Q \cdots \mapsto_Q p_n = p' .$$

Ak $p \mapsto_Q^+ p'$ a p' je ireducibilný modulo Q, budeme písať $p \mapsto_Q^* p'$.

□

Príklad 2.2. Uvažujme $p, q_1, q_2 \in \mathbb{Q}[x, y, z]$, $Q = \{q_1, q_2\}$ a usporiadanie $<_L$, pričom

$$q_1 = xz - 1\,, \qquad q_2 = y^2 + z^2\,, \qquad p = -xz^3 - y^2\,.$$

Potom máme redukcie

$$p \mapsto_{q_1} p' = p - (-z^2) \cdot q_1 = -y^2 - z^2 \mapsto_{q_2} p' - (-1) \cdot q_2 = 0\,,$$

teda $p \mapsto_Q^+ 0$ a keďže 0 je ireducibilný modulo Q, tak aj $p \mapsto_Q^* 0$.

□

Na základe vety 2.4 vieme skonštruovať konečný algoritmus (*úplnú redukciu*), ktorý k danému p nájde p' také, že $p \mapsto_Q^* p'$. Jednoducho redukujeme, kým nedostaneme polynóm ireducibilný modulo Q. Jednou z možných implementácií je algoritmus 1. Napadne nás, že práve tento algoritmus by mohol byťkanonickou funkciou pre $\langle Q \rangle$, inými slovami, ak $p \in \langle Q \rangle$, nutne $p \mapsto_Q^* 0$. Nasledujúci príklad ukazuje, že to tak nie je.

Príklad 2.3. Nech $Q = \{q_1, q_2\} \subset \mathbb{Q}[x, y]$ a $p \in \mathbb{Q}[x, y]$ kde

$$q_1 = x^2 - y, \qquad q_2 = x^2 + y, \qquad p = x^2 y\,.$$

Uvažujme stupňové usporiadanie termov $>_D$. Potom máme $p \mapsto_Q p - y \cdot q_1 = y^2$. Polynóm y^2 je ireducibilný modulo Q. Pritom ale

$$p = \frac{1}{2} y \cdot q_1 + \frac{1}{2} y \cdot q_2 \in \langle Q \rangle\ .$$

Naviac, úplnou redukciou p modulo Q, keby sme redukovali najprv pomocou q_2, by sme dostali $-y^2$. Teda výsledok úplnej redukcie nie je jednoznačný.

□

Samotný proces redukcie má dobrú myšlienku, no na kanonickú funkciu nestačí. Pozrime sa na zopár vlastností redukcie, ktoré nám pomôžu prekonať súčasné ťažkosti.

Veta 2.5. Majme $p_1, p_2, p' \in \mathbb{F}[\mathbf{x}]$ a $Q \subset \mathbb{F}[\mathbf{x}]$. Ak $p_1 - p_2 \mapsto_Q p'$, existujú p_1', p_2' také, že

$$p_1 \mapsto_Q^+ p_1', \qquad p_2 \mapsto_Q^+ p_2', \qquad p' = p_1' - p_2'\,.$$

Dôkaz: Nech $q \in Q$, $0 \neq \alpha \in \mathbb{F}$ a $v \in \mathbb{T}_{\mathbf{x}}$ sú také, že

$$p' = (p_1 - p_2) - \alpha v \cdot \frac{q}{\mathrm{M}(q)}\,.$$

(Teda v je term eliminovaný v redukcii $p_1 - p_2 \mapsto_Q p'$.) Predpokladajme, že v má v p_1 koeficient β_1 a v p_2 koeficient β_2. Keďže v sa nachádza v $p_1 - p_2$ s koeficientom α, máme $\alpha = \beta_1 - \beta_2$. Položme $u = v/\mathrm{ht}(q)$. Polynómy

$$p_1' = p_1 - \frac{\beta_1}{\mathrm{hc}(q)} u \cdot q\,, \qquad p_2' = p_2 - \frac{\beta_2}{\mathrm{hc}(q)} u \cdot q$$

zrejme spĺňajú požiadavky tvrdenia.

□

Veta 2.6. Nech $p_1, p_2 \in \mathbb{F}[\mathbf{x}]$ spĺňajú $p_1 - p_2 \mapsto_Q^+ 0$ pre $Q \subset \mathbb{F}[\mathbf{x}]$. Potom existuje $p' \in \mathbb{F}[\mathbf{x}]$ taký, že $p_1 \mapsto_Q^+ p'$ a $p_2 \mapsto_Q^+ p'$, t. j. p_1, p_2 majú *spoločného následníka*, keď ich redukujeme modulo Q.

Dôkaz: Postupujme indukciou podľa počtu krokov potrebných na redukovanie $p_1 - p_2$ na 0. Ak počet krokov je 0, t. j. $p_1 = p_2$, tvrdenie platí. Predpokladajme, že tvrdenie platí pre $n - 1$ krokov redukcie a nech

$$p_1 - p_2 \mapsto_Q h_1 \mapsto_Q \cdots \mapsto_Q h_n = 0\,.$$

Podľa vety 2.5 existujú p_1', p_2' také, že $p_1 \mapsto_Q^+ p_1'$, $p_2 \mapsto_Q^+ p_2'$ a $p_1' - p_2' = h_1$. Podľa indukčného predpokladu majú p_1' a p_2' (a teda aj p_1 a p_2) spoločného následníka.

□

Veta 2.7. Ak p, p' sú polynómy také, že $p \mapsto_Q p'$, potom pre ľubovoľný polynóm r existuje s taký, že

$$p + r \mapsto_Q^+ s, \qquad p' + r \mapsto_Q^+ s\,.$$

Dôkaz: Nech $\alpha \in \mathbb{F}$, $u \in \mathbb{T}_{\mathbf{x}}$ a $q \in Q$ sú také, že $p' = p - \alpha u \cdot q/\mathrm{hc}(q)$ a nech $t = u \cdot \mathrm{ht}(q)$ je term eliminovaný v tejto redukcii. Zoberme ľubovoľný r. Predpokladajme, že term t má v r (a teda aj v $p' + r$) koeficient β (môže byť aj nulový). Potom t má v $p + r$ koeficient $\alpha + \beta$. Pri označení $\tilde{q} = q/\mathrm{hc}(q)$ tak máme (možno triviálne) redukcie

$$p + r \mapsto_q^+ (p + r) - (\alpha + \beta) u \cdot \tilde{q} = s_1\,, \qquad p' + r \mapsto_q^+ (p' + r) - \beta u \cdot \tilde{q} = s_2$$

a $s_1 - s_2 = (\alpha - (\alpha + \beta) + \beta) u \cdot \tilde{q} = 0$. Preto polynóm $s = s_1 = s_2$ spĺňa požiadavky tvrdenia.

□

2.3 Gröbnerove bázy a Buchbergerov algoritmus

Pokiaľ pre nejaký polynóm p úplnou redukciou dostaneme $p \mapsto_Q^* 0$, vieme, že $p \in \langle Q \rangle$. Príklad 2.3 ukazuje, že opačná implikácia neplatí. Len pomocou redukcie problém patrenia do ideálu nevyriešime. Samotný algoritmus redukcie možno ťažko vylepšiť tak, aby fungoval stopercentne. Ukážeme, že chyba nie je v ňom, ale skôr v štruktúre bázy Q. Tá sa bude dať pretransformovať na novú bázu, ktorá generuje rovnaký ideál a spĺňa podmienky nasledujúcej definície.

Definícia 2.8. Báza $G \subset \mathbb{F}[\mathbf{x}]$ sa nazýva *Gröbnerova* (vzhľadom na pevné usporiadanie termov $<_T$), ak

$$p \in \langle G \rangle \qquad \Longleftrightarrow \qquad p \mapsto_G^* 0\,.$$

□

Z definície zrejme vyplýva, že G je Gröbnerova báza práve vtedy, keď jediný polynóm v $\langle G \rangle$ ireducibilný modulo G je $p = 0$. Úplná redukcia podľa takejto bázy je preto normálnou funkciou. Naša otázka je, či (konečná) Gröbnerova báza existuje pre každý ideál a ako sa dá pre daný ideál $\langle q_1, \ldots, q_n \rangle$ skonštruovať.

Buchbergerova metóda spočíva v doplnení pôvodnej bázy Q konečným počtom nových polynómov z ideálu. Skutočne, pridaním nového polynómu $q \in \langle Q \rangle$ medzi generátory sa generovaný ideál nezmení ($\langle Q \rangle = \langle Q \cup \{q\} \rangle$), zato redukcia $\mapsto_{Q \cup \{q\}}$ bude môcť redukovať polynómy, ktoré boli modulo Q ireducibilné.

Príklad 2.4. Keď v príklade 2.3 pridáme do Q polynóm

$$q_3 = y = -\frac{1}{2} \cdot q_1 + \frac{1}{2} \cdot q_2 \in \langle Q \rangle\ ,$$

budeme môcť polynóm p redukovať

$$p \mapsto_{q_1} y^2 \mapsto_{q_3} 0\,,$$

hoci pôvodne sme mali $p \mapsto_Q^* y^2$.

□

Treba vymyslieť, aké polynómy musíme do bázy pridať, aby sa stala Gröbnerovou. Dobre sa redukuje polynómami, ktorých vedúce termy sú čo najmenšie. Zbytočné je pridať do Q polynóm $\tilde{q}$, ktorého vedúci term je násobkom vedúceho termu niektorého polynómu q z Q (čo sa nedalo redukovať pomocou q, nebude sa dať ani pomocou $\tilde{q}$). Naproti tomu, polynómy z $\langle Q \rangle$ (tie

môžeme pridávať) sú tvaru (1.3) a v takomto tvare nám väčšinou vyjde vedúci term ako násobok vedúceho termu niektorého z q_i. Zabrániť tomu môžeme iba vhodnou voľbou polynómov f_i. Konkrétne ich treba zvoliť tak, aby sa vedúce členy výrazov $f_i q_i$ a $f_j q_j$ navzájom eliminovali. Taká eliminácia pre dva polynómy z Q zasluhuje osobitné označenie.

Definícia 2.9. *S-polynóm* polynómov $q_1, q_2 \in \mathbb{F}[\mathbf{x}]$ je

$$\mathrm{S}(q_1, q_2) = \mathrm{nsn}(\mathrm{M}(q_1), \mathrm{M}(q_2)) \left(\frac{q_1}{\mathrm{M}(q_1)} - \frac{q_2}{\mathrm{M}(q_2)} \right) ,$$

kde $\mathrm{nsn}(f, g)$ označuje najmenší spoločný násobok polynómov f a g.

□

Príklad 2.5. V situácii z príkladu 2.2 máme

$$\mathrm{S}(q_1, q_2) = y^2 \cdot (xz - 1) - xz \cdot (y^2 + z^2) = -xz^3 - y^2 = p \, .$$

□

S-polynóm získame tak, že vynásobíme q_1 a q_2 každý vhodným (najmenším možným) jednočlenom, aby sa vedúce členy oboch rovnali a výsledky od seba odpočítame. (Takže $\mathrm{S}(q_1, q_2) \in \langle q_1, q_2 \rangle$ a môžeme ho pridať do bázy obsahujúcej q_1 a q_2.) Užitočné je všimnúť si, že S-polynóm je rozdiel medzi redukovaním $\mathrm{nsn}(\mathrm{M}(q_1), \mathrm{M}(q_2))$ modulo q_2 a redukovaním modulo q_1. Bude to mať rozhodujúci význam v nasledujúcej fundamentálnej Buchbergerovej vete (publikovanej v [4]), ktorá priamo vedie k algoritmu na nájdenie Gröbnerovej bázy.

Veta 2.8. (*Alternatívna charakterizácia Gröbnerovej bázy.*) Nasledujúce tri podmienky sú ekvivalentné.

(*i*) G je Gröbnerova báza,

(*ii*) $\forall q_1, q_2 \in G \quad \mathrm{S}(q_1, q_2) \mapsto_G^+ 0 \, ,$

(*iii*) Ak $p \mapsto_G^* p_1'$ a $p \mapsto_G^* p_2'$, potom $p_1' = p_2'$.

Motivácia k vete je zrejmá. Podmienka (*ii*) nám dovoľuje otestovať, či daná báza je Gröbnerova a ponúka algoritmus na nájdenie takej bázy. Podľa nej netreba pridávať k báze všetky S-polynómy (tak by sme nikdy neskončili, nakoľko pridaním polynómu k báze vznikne možnosť generovať nové S-polynómy). Podmienka (*iii*) zasa pomôže nahliadnuť, že úplná redukcia $\mapsto_G^*$ je kanonickou funkciou.

Dôkaz: Postupujme v troch krokoch.
(*i*)⇒(*ii*): Prvá implikácia je triviálna, pretože pre $q_1, q_2 \in G$ máme $\mathrm{S}(q_1, q_2) \in \langle G \rangle$ a teda za predpokladu gröbnerovskosti G

$$\mathrm{S}(q_1, q_2) \mapsto_G^+ 0\,.$$

(*ii*)⇒(*iii*): Implikáciu dokážeme indukciou podľa vedúceho termu polynómu p. Najprv uvažujme prípad $\mathrm{ht}(p) = 1$. Zrejme tvrdenie platí, pretože buď je p ireducibilný modulo G (t. j. $p = p'_1 = p'_2$), alebo sa jedným krokom zredukuje na 0 (t. j. $0 = p'_1 = p'_2$). Predpokladajme, že (*iii*) platí pre všetky p také, že $\mathrm{ht}(p) <_T t$ pre nejaké pevné $t \in \mathbb{T}_{\mathbf{x}}$ (hlavný indukčný predpoklad). Uvažujme p taký, že $\mathrm{ht}(p) = t$. Ak t je ireducibilný modulo G, tvrdenie iste platí. Dôvodom je, že redukcie polynómu p môžu zahŕňať iba termy menšie v zmysle $<_T$, čiže ak

$$p = \mathrm{M}(p) + (p - \mathrm{M}(p)) \mapsto_G^* \mathrm{M}(p) + p_1 = p'_1$$

a tiež

$$p \mapsto_G^* \mathrm{M}(p) + p_2 = p'_2\,,$$

indukčný predpoklad (použitý na $p - \mathrm{M}(p)$) implikuje $p_1 = p_2$ a teda $p'_1 = p'_2$. Predpokladajme preto, že t je redukovateľný a označme množinu polynómov z G, ktoré ho dokážu redukovať,

$$R_{p,G} = \{g_1, \ldots, g_m\}\,.$$

Zoberme polynómy $r, \tilde{p}_1, p'_1$ také, že

$$\mathrm{M}(p) \mapsto_{g_1} r\,, \qquad p - \mathrm{M}(p) \mapsto_G^* \tilde{p}_1\,, \qquad r + \tilde{p}_1 \mapsto_G^* p'_1 \tag{2.5}$$

a teda aj

$$p \mapsto_G^+ \mathrm{M}(p) + \tilde{p}_1 \mapsto_G r + \tilde{p}_1 \mapsto_G^* p'_1\,.$$

Predpokladajme teraz, že existuje tiež polynóm p'_2 taký, že $p \mapsto_G^* p'_2$. Rozoberme dve možnosti.

(*a*) Najprv predpokladajme, že nová redukcia je tvaru

$$\mathrm{M}(p) \mapsto_{g_1} r\,, \qquad p - \mathrm{M}(p) \mapsto_G^+ \tilde{p}_2\,, \qquad r + \tilde{p}_2 \mapsto_G^* p'_2\,, \tag{2.6}$$

pričom prostredné redukcie (ak nejaké sú) sa vykonajú najskôr. Tvrdíme, že za týchto podmienok majú $r + \tilde{p}_1$ a $r + \tilde{p}_2$ spoločného následníka. Dokážeme to indukciou podľa počtu krokov v redukcii $\tilde{p}_2 \mapsto_G^+ \tilde{p}_1$ (ktorá vždy existuje vďaka hlavnému indukčnému predpokladu). Ak počet krokov je 0, je to triviálne. Predpokladajme teraz, že $r + f$ a $r + \tilde{p}_2$ majú spoločného následníka vždy, keď

$\tilde{p}_2 \mapsto_G^+ f$ v ℓ krokoch. Nech $\tilde{f}$ je taký, že $\tilde{p}_2 \mapsto_G^+ \tilde{f}$ v ℓ krokoch a $\tilde{f} \mapsto_G \tilde{p}_1$. Podľa vety 2.7 existuje s taký, že

$$r + \tilde{f} \mapsto_G^+ s\,, \qquad r + \tilde{p}_1 \mapsto_G^+ s\,.$$

Keďže podľa indukčného predpokladu (neskoršieho) existuje h taký, že

$$r + \tilde{p}_2 \mapsto_G^+ h\,, \qquad r + \tilde{f} \mapsto_G^+ h\,,$$

máme pre nejaké $\tilde{s}, \tilde{h}$

$$r + \tilde{f} \mapsto_G^* \tilde{s}\,, \quad r + \tilde{p}_1 \mapsto_G^* \tilde{s}\,, \qquad r + \tilde{p}_2 \mapsto_G^* \tilde{h}\,, \quad r + \tilde{f} \mapsto_G^* \tilde{h}\,.$$

Keďže vedúce termy všetkých týchto polynómov sú menšie ako t, podľa hlavného indukčného predpokladu $\tilde{s} = \tilde{h}$, t. j. $r + \tilde{p}_1$ a $r + \tilde{p}_2$ majú spoločného následníka. Spolu s (2.5), (2.6) a hlavným indukčným predpokladom máme $p_1' = p_2'$.

(*b*) Predpokladajme teraz, že máme $\tilde{r}, \tilde{p}_2$ také, že

$$\mathrm{M}(p) \mapsto_{g_j} \tilde{r}\,, \qquad p - \mathrm{M}(p) \mapsto_G^+ \tilde{p}_2\,, \qquad \tilde{r} + \tilde{p}_2 \mapsto_G^* p_2'\,, \tag{2.7}$$

kde $2 \leq j \leq m$ a teda

$$p \mapsto_G^+ \mathrm{M}(p) + \tilde{p}_2 \mapsto_G \tilde{r} + \tilde{p}_2 \mapsto_G^* p_2'\,.$$

Uvažujme tiež redukcie

$$\mathrm{M}(p) \mapsto_{g_1} r\,, \qquad p - \mathrm{M}(p) \mapsto_G^+ \tilde{p}_2\,, \qquad r + \tilde{p}_2 \mapsto_G^* p_3'\,, \tag{2.8}$$

t. j.

$$p \mapsto_G^+ \mathrm{M}(p) + \tilde{p}_2 \mapsto_G r + \tilde{p}_2 \mapsto_G^* p_3' = p_1' \tag{2.9}$$

(vďaka výsledku z časti (*a*)). Úpravou dostávame

$$\begin{aligned}(\tilde{r} + \tilde{p}_2) - (r + \tilde{p}_2) = \tilde{r} - r = \left(\mathrm{M}(p) - \mathrm{M}(p) \cdot \tfrac{g_j}{\mathrm{M}(g_j)}\right) - \left(\mathrm{M}(p) - \mathrm{M}(p) \cdot \tfrac{g_1}{\mathrm{M}(g_1)}\right) = \\ = \mathrm{M}(p) \left(\tfrac{g_1}{\mathrm{M}(g_1)} - \tfrac{g_j}{\mathrm{M}(g_j)}\right)\,.\end{aligned}$$

Keďže $g_1, g_j \in R_{p,G}$, posledný výraz je súčin $\mathrm{S}(g_1, g_j)$ a jednočlenu. Podľa podmienky (*ii*) a vety 2.6 existuje f také, že

$$\tilde{r} + \tilde{p}_2 \mapsto_G^+ f\,, \qquad r + \tilde{p}_2 \mapsto_G^+ f\,.$$

Konečne, podľa (2.7), (2.8), (2.9) a hlavného indukčného predpokladu, $p_1' = p_2'$.

(*iii*)⇒(*i*): Majme ľubovoľný $p \in \langle G \rangle$. Ukážeme, že za predpokladu (*iii*) platí $p \mapsto_G^+ 0$. Podľa (1.2) existujú $k \in \mathbb{N}$, $0 \neq h_i \in \mathbb{F}[\mathbf{x}]$ a $g_i \in G$ ($i = 1, 2, \ldots k$), že $p = h_1 g_1 + \cdots + h_k g_k$.

Postupujme indukciou podľa k. Ak $k = 1$, tak $p = h_1 g_1$. Keďže $\mathrm{M}(p) = \mathrm{M}(h_1)\mathrm{M}(g_1)$, p (ak je nenulový) sa dá redukovať modulo g_1. Výsledok redukcie je opäť násobkom g_1, preto ho (ak je nenulový) možno opäť redukovať modulo g_1 atď. Postupnosť redukcií je vždy konečná (veta 2.4), preto nutne $p \mapsto_G^+ 0$.

Predpokladajme, že tvrdenie platí pre k a

$$p = \underbrace{h_1 g_1 + \cdots + h_k g_k}_{p_1} + \underbrace{h_{k+1} g_{k+1}}_{p_2} = p_1 + p_2 \,.$$

Z indukčného predpokladu (nakoľko $p - p_2 = p_1$)

$$p_2 \mapsto_G^+ 0 \qquad \text{a} \qquad p - p_2 \mapsto_G^+ 0 \,. \tag{2.10}$$

Podľa vety 2.6 majú p a p_2 spoločného následníka p', t. j.

$$p \mapsto_G^+ p' \mapsto_G^* p'', \qquad p_2 \mapsto_G^+ p' \mapsto_G^* p'' \,. \tag{2.11}$$

Z (2.10) a (2.11) vieme p_2 zredukovať úplnou redukciou na 0 aj na p'', takže podľa (*iii*) $p'' = 0$ a z (2.11) $p \mapsto_G^* 0$. Tvrdenie preto platí aj pre $k + 1$.

□

Podľa vety 2.8 je výsledok úplnej redukcie podľa Gröbnerovej bázy jednoznačný (bez ohľadu na kroky redukcie). Budeme preto písať $p' = \mathrm{Red}(p, G)$ namiesto $p \mapsto_G^* p'$. Funkcia $\mathrm{Red}(\,\cdot\,, G) : \mathbb{F}[\mathbf{x}] \longrightarrow \mathbb{F}[\mathbf{x}]$ je kanonickou funkciou pre $\mathbb{F}[\mathbf{x}]/\langle G \rangle$, o čom hovorí nasledujúca veta.

Veta 2.9. Ak G je Gröbnerova báza, tak

$$\mathrm{Red}(p_1, G) = \mathrm{Red}(p_2, G) \qquad \Longleftrightarrow \qquad p_1 - p_2 \in \langle G \rangle \,.$$

Dôkaz: Dokážme najprv prvú implikáciu. Nech $p' = \mathrm{Red}(p_1, G) = \mathrm{Red}(p_2, G)$. Potom $p_1 - p' \in \langle G \rangle$ a $p_2 - p' \in \langle G \rangle$. Preto

$$(p_1 - p') - (p_2 - p') = p_1 - p_2 \in \langle G \rangle \,.$$

Na dôkaz druhej implikácie stačí použiť vetu 2.6 (na $p_1 - p_2 \in \langle G \rangle$) a potom časť (*iii*) z vety 2.8.

□

Kanonickosť je veľmi významná vlastnosť, ktorá nám umožňuje robiť výpočty vo faktorovom okruhu $\mathbb{F}[\mathbf{x}]/\langle G\rangle$. Viac sa tomu budeme venovať v kapitole 4. Uveďme teraz, ako nám veta 2.8 umožňuje zostrojiť algoritmus na výpočet Gröbnerovej bázy.

Veta nám dala návod, ako otestovať, či daná báza $Q \subset \mathbb{F}[\mathbf{x}]$ je Gröbnerova. Stačí testovať, či

$$\mathrm{S}(q_1, q_2) \mapsto_Q^+ 0 \qquad \forall q_1, q_2 \in Q,\ q_1 \neq q_2\,. \tag{2.12}$$

Povedzme, že nájdeme dvojicu (q_1, q_2) takú, že

$$\mathrm{S}(q_1, q_2) \mapsto_Q^* r_1 \neq 0\,. \tag{2.13}$$

Zistili sme, že Q nie je Gröbnerova a musíme k nej pridať nejaký polynóm z $\langle Q\rangle$. Už sme naznačili, že dobrý kandidát na pridanie je $\mathrm{S}(q_1, q_2)$ (v ktorom sú navzájom eliminované $\mathrm{ht}(q_1)$ a $\mathrm{ht}(q_2)$). Ešte lepší kandidát je r_1 z (2.13), pretože $r_1 \in \langle Q\rangle$ (nakoľko $r_1 \sim \mathrm{S}(q_1, q_2) \in \langle Q\rangle$) a $r_1 \preceq \mathrm{S}(q_1, q_2)$. Spolu máme

$$\langle Q\rangle = \langle Q \cup \{r_1\}\rangle \qquad \text{a} \qquad \mathrm{S}(q_1, q_2) \mapsto_{Q\cup\{r_1\}}^* 0\,.$$

Po pridaní r_1 do Q tak zabezpečíme vynulovanie (redukciou) jedného S-polynómu. Testujeme ďalej na (2.12) rozšírenú množinu (pridaním r_1 vznikli nové S-polynómy a niektoré staré môžu byť ešte neotestované). Ak nájdeme S-polynóm, ktorý zredukujeme (modulo $Q\cup\{r_1\}$) na ireducibilný polynóm $r_2 \neq 0$, pridáme ho k báze atď.

Ostáva jediná otázka, či popísaný algoritmus vždy skončí. Na ňu sme sa pripravili v úvode kapitoly. Stačí sa pozrieť na postupnosť

$$\mathrm{ht}(r_1),\ \mathrm{ht}(r_2),\ \ldots\,. \tag{2.14}$$

Pre každé k je r_k ireducibilný modulo $Q \cup \{r_1, \ldots, r_{k-1}\}$, preto $\mathrm{ht}(r_k)$ nie je násobkom žiadneho z $\mathrm{ht}(r_1), \ldots, \mathrm{ht}(r_{k-1})$ (inak by sa dal redukovať). Postupnosť (2.14) preto podľa vety 2.1 nemôže byť nekonečná.

Príklad 2.6. Uvažujme $q_0, q_2 \in \mathbb{Q}[x, y, z]$, $Q = \{q_0, q_1\}$ a usporiadanie $<_L$, pričom

$$q_0 = xy^2 + z\,, \qquad q_1 = xz - 1\,.$$

Zostrojme pre $\langle Q\rangle$ Gröbnerovu bázu. Máme

$$\mathrm{S}(q_0, q_1) = z \cdot q_0 - y^2 \cdot q_1 = y^2 + z^2 = q_2 \mapsto_Q^* q_2\,.$$

S-polynóm sa nezredukoval na 0, testujeme teda ďalej.

$$\mathrm{S}(q_0, q_2) = 1 \cdot q_0 - x \cdot q_2 = -xz^2 + z \mapsto_{q_1} 0\,.$$

Podľa príkladov 2.5 a 2.2 aj $\mathrm{S}(q_1, q_2) \mapsto^+_{\{q_1,q_2\}} 0$. Teda množina $\{q_0, q_1, q_2\}$ je Gröbnerova báza ideálu $\langle Q \rangle$.

□

2.4 Jednoznačnosť redukovanej Gröbnerovej bázy

Ukázali sme si existenciu Gröbnerovej bázy a algoritmus na jej nájdenie (pozri aj algoritmus 2). Pripravili sme tak zázemie pre mnohé aplikácie. Prv, než sa im začneme venovať, pozrime sa na dôležité výsledky, ktoré prácu s Gröbnerovými bázami zefektívnia.

Je jasné, že Gröbnerova báza pre daný ideál nie je jednoznačne určená. Nezávisí iba od $<_T$. Napríklad ak G je Gröbnerova báza pre $\langle G \rangle$, je ňou aj $G \cup \{r\}$ pre každý polynóm $r \in \langle G \rangle$. Mohlo by nás zaujímať, či z danej Gröbnerovej bázy nemožno niektoré polynómy vynechať (prípadne nahradiť jednoduchšími) tak, aby ostala Gröbnerovou. Nasledujúce vety a definície ukazujú, že to možné je.

Veta 2.10. Ak G je Gröbnerova báza, $g_1, g_2 \in G$, $g_1 \neq g_2$ a $\mathrm{ht}(g_2) \mid \mathrm{ht}(g_1)$, potom aj $H = G - \{g_1\}$ je Gröbnerova báza toho istého ideálu.

Dôkaz: Zrejme $H \subseteq \langle G \rangle$. Stačí (podľa definície 2.8) ukázať, že pre každý $p \in \langle G \rangle$ platí $p \mapsto^+_H 0$ (z toho okrem gröbnerovskosti H máme aj $p \in \langle H \rangle$ a teda $\langle H \rangle = \langle G \rangle$). Keby sme mali $p \mapsto^*_H p' \neq 0$, keďže $p' \mapsto^+_G 0$, existuje polynóm $g \in G$, ktorým sa redukuje p'. Ak $g \in H$, máme spor s ireducibilnosťou p' modulo H. Preto $g = g_1$. Ale potom sa dá p' redukovať aj polynómom $g_2 \in H$.

□

Z Gröbnerovej bázy teda môžeme postupne vynechať každý polynóm, ktorého vedúci term je násobkom vedúceho termu iného polynómu z bázy. Po vynechaní všetých možných polynómov dostaneme bázu, ktorá bude mať k jednoznačnosti bližšie. V akom zmysle, to ukazuje nasledujúca definícia a veta.

Definícia 2.10. Gröbnerova báza sa nazýva *minimálna*, ak $\mathrm{ht}(g_1) \nmid \mathrm{ht}(g_2)$ pre každé dva rôzne $g_1, g_2 \in G$ a $\mathrm{hc}(g) = 1$ pre každý $g \in G$.

□

Z predchádzajúceho je jasné, ako minimálnu bázu vyrobiť z ľubovoľnej Gröbnerovej bázy. (Polynómy v báze si zrejme môžeme dovoliť normovať.) Len pre doplnenie, na základe vety 2.1 je každá minimálna báza konečná (Buchbergerov algoritmus nám samozrejme vygeneruje konečnú bázu, vo všeobecnosti však môže byť Gröbnerova báza nekonečná – napríklad každý ideál je svojou Gröbnerovou bázou).

Veta 2.11. Ak $G = \{g_1, \ldots, g_m\}$ a $F = \{f_1, \ldots, f_\ell\}$ sú dve minimálne Gröbnerove bázy pre ideál $\langle Q \rangle$, potom $m = \ell$ a po prečíslovaní (ak je potrebné) $\mathrm{ht}(f_i) = \mathrm{ht}(g_i)$ pre všetky $i = 1, \ldots, m$.

Dôkaz: Keďže f_1 je v $\langle Q \rangle$ a keďže G je Gröbnerova báza pre $\langle Q \rangle$, existuje i také, že $\mathrm{ht}(g_i)$ delí $\mathrm{ht}(f_1)$. Po prečíslovaní, ak je potrebné, môžeme predpokladať, že $i = 1$. Aj g_1 je v $\langle Q \rangle$ a keďže F je Gröbnerova báza pre $\langle Q \rangle$, existuje j také, že $\mathrm{ht}(f_j)$ delí $\mathrm{ht}(g_1)$. Spolu máme $\mathrm{ht}(f_j) \mid \mathrm{ht}(f_1)$ a z minimálnosti F nutne $j = 1$ a $\mathrm{ht}(f_1) = \mathrm{ht}(g_1)$.

Podobne f_2 je v $\langle Q \rangle$ a teda existuje i také, že $\mathrm{ht}(g_i)$ delí $\mathrm{ht}(f_2)$ (keďže G je Gröbnerova báza). Minimálnosť F a fakt, že $\mathrm{ht}(f_1) = \mathrm{ht}(g_1)$ zabezpečia $i \neq 1$ a po prečíslovaní (ak je potrebné) máme $i = 2$. Rovnako ako v predošlom dostaneme $\mathrm{ht}(f_2) = \mathrm{ht}(g_2)$.

Tento proces pokračuje, kým neminieme všetky polynómy z F a G. Preto $m = \ell$ a po prečíslovaní (ak je potrebné) $\mathrm{ht}(f_i) = \mathrm{ht}(g_i)$ pre všetky $i = 1, \ldots, m$.

□

Ani minimálna Gröbnerova báza nie je jednoznačne určená, jednoznačne určená je množina vedúcich termov jej polynómov. Minimalizáciou sme zmenšili počet jej polynómov najviac, ako sa dalo (skutočne, veta 2.11 spolu s postupom mimimalizácie ukazuje, že menší počet prvkov mať žiadna Gröbnerova báza nemôže). Čo ešte môžeme s bázou urobiť je skúsiť zjednodušiť jej prvky. Zjednodušovať (redukovať) nejaký prvok $g \in G$ môžeme len modulo iné prvky z G (aby sme s ním ostali v ideále). Ostane ale báza po takejto redukcii Gröbnerovou? Odpoveď dáva ďalšia veta.

Veta 2.12. Nech G je minimálna Gröbnerova báza, $g_1 \in G$ a $g_1 \mapsto_{G-\{g_1\}} g_2$. Potom aj $H = (G - \{g_1\}) \cup \{g_2\}$ je minimálna Gröbnerova báza toho istého ideálu.

Dôkaz: Nakoľko G je minimálna, $\mathrm{ht}(g_1) = \mathrm{ht}(g_2)$. Zrejme $g_2 \in \langle G \rangle$, čiže $H \subset \langle G \rangle$. Ďalej stačí skopírovať postup z dôkazu vety 2.10.

□

Uvedená veta platí aj vo verzii bez slovka *minimálna*. Platí aj keď namiesto jedného kroku redukcie ich urobíme ľubovoľne veľa (stačí vetu použiť opakovane). To nám umožňuje transformovať minimálnu Gröbnerovu bázu $G = \{g_1, \ldots, g_m\}$ na novú bázu nasledovne.

$g_1 \mapsto^*_{H_1} h_1$, kde $H_1 = \{g_2, \ldots, g_m\}$,

$g_2 \mapsto^*_{H_2} h_2$, kde $H_2 = \{h_1, g_3, \ldots, g_m\}$,

$g_3 \mapsto^*_{H_3} h_3$, kde $H_3 = \{h_1, h_2, g_4, \ldots, g_m\}$,

$\vdots$

$g_m \mapsto^*_{H_m} h_m$, kde $H_m = \{h_1, h_2, \ldots, h_{m-1}\}$.

Podľa predchádzajúcej vety máme pre ideál $\langle G \rangle$ postupnosť minimálnych Gröbnerových báz

$$G\ ,\ \{h_1, g_2, \ldots, g_m\}\ ,\ \{h_1, h_2, g_3, \ldots, g_m\}\ ,\ \ldots\ ,\ \{h_1, \ldots, h_m\} = H\ . \tag{2.15}$$

Dostali sme novú bázu H. Pritom žiadny h_i sa už ďalej nedá redukovať modulo $H - \{h_i\}$, pretože vedúce termy polynómov množiny $H - \{h_i\}$ sú rovnaké ako vedúce termy polynómov z H_i (to vyplýva z vety 2.11 a z toho, že H a $H_i \cup \{h_i\}$ sú podľa (2.15) minimálne Gröbnerove bázy pre $\langle G \rangle$) a h_i je ireducibilný modulo H_i. Báza H sa teda nedá viacej zjednodušiť a spĺňa túto definíciu.

Definícia 2.11. Gröbnerova báza G sa nazýva *redukovaná*, ak pre každé $g \in G$ platí $\mathrm{hc}(g) = 1$ a g je ireducibilný modulo $G - \{g\}$.

□

Ukázali sme si, ako redukovanú bázu zostrojiť. Na záver ostáva overiť to, k čomu v tejto podkapitole smerujeme, totiž či pre daný ideál je redukovaná Gröbnerova báza jednoznačne určená. Potvrdzuje nám to Buchbergerova veta (publikovaná v [5]).

Veta 2.13. (*Buchbergerova*.) Vzhľadom na pevné usporiadanie termov $<_T$ má každý ideál v $\mathbb{F}[\mathbf{x}]$ práve jednu redukovanú Gröbnerovu bázu.

Dôkaz: Z predchádzajúceho vieme, že každý ideál má nejakú redukovanú Gröbnerovu bázu. Potrebujeme len dokázať jednoznačnosť. Nech $G = \{g_1, \ldots, g_m\}$ a $H = \{h_1, \ldots, h_m\}$ sú redukované Gröbnerove bázy toho istého ideálu $\langle Q \rangle$. Podľa vety 2.11, keďže každá redukovaná báza je minimálna, obe množiny G a H majú rovnaký počet prvkov a môžeme predpokladať, že pre každé i platí $\mathrm{ht}(g_i) = \mathrm{ht}(h_i)$.

Zoberme ľubovoľné i, $1 \leq i \leq m$. Ak $g_i \neq h_i$, potom $g_i - h_i \neq 0$ leží v $\langle Q \rangle$ a preto existuje j také, že $\mathrm{ht}(g_j)$ delí $\mathrm{ht}(g_i - h_i)$. Keďže $\mathrm{ht}(g_i - h_i) <_T \mathrm{ht}(g_i)$, nutne $j \neq i$. Pritom ale $\mathrm{ht}(g_j) = \mathrm{ht}(h_j)$ delí nejaký term g_i alebo h_i. To je v spore s predpokladom, že G a H sú redukované Gröbnerove bázy. Preto $g_i = h_i$ a následne $G = H$.

□

Príklad 2.7. Báza, ktorú sme vygenerovali v priklade 2.6, nie je minimálna, pretože $\mathrm{ht}(q_2) \mid \mathrm{ht}(q_0)$. Po odstránení q_0 dostaneme Gröbnerovu bázu $\{y^2 + z^2, xz - 1\}$, ktorá už je minimálna a je aj redukovaná. Podľa predošlej vety je pre svoj ideál jediná (vzhľadom na usporiadanie $<_L$).

□

2.5 Vylepšenia Buchbergerovho algoritmu

Na záver tejto kapitoly si ukážeme niekoľko zefektívnení a vylepšení algoritmu na výpočet Gröbnerovej bázy. V prvom rade, s redukovanou bázou sa pracuje lepšie ako s neredukovanou, takže na konci Buchbergerovho algoritmu môžeme vykonať proces redukcie z predošlej podkapitoly. Redukovanosť množiny je však vlastnosť, na ktorú sa nemusíme pýtať iba pri Gröbnerových bázach. Definíciu 2.11 môžeme rovnako dobre sformulovať pre ľubovoľnú bázu ideálu.

Na skonštruovanie redukovanej bázy k danej báze, ktorá nie je Gröbnerova, nestačí postup, ktorý sme aplikovali na Gröbnerovu bázu. Pri minimalizovaní by sme mohli odstránením nevhodného polynómu zmeniť ideál, ktorý daná množina generuje. Na druhej strane, nepotrebujeme, aby sa pri transformovaní zachovávala podmienka gröbnerovskosti. Modifikácia vety 2.12 (vynechaním spojenia *minimálna Gröbnerova*) pre ľubovoľnú bázu platí. Opakovaným použitím tejto modifikácie na danú bázu ju vieme vždy spraviť redukovanou (hoci výsledok takejto redukcie nebude jednoznačný). Detaily, ako takú redukciu spraviť čo najefektívnejšie možno nájsť v [3]. Univerzálny algoritmus, ktorý Gröbnerovu bázu pretransformuje na redukovanú Gröbnerovu bázu a každú bázu pretransformuje na redukovanú bázu je algoritmus 3.

Pred tým, ako použijeme na bázu Buchbergerov algoritmus, môžeme ju zredukovať. V mnohých prípadoch tak samotný výpočet Gröbnerovej bázy zrýchlime (zmenšíme počet začiatočných S-polynómov a tie budú jednoduchšie). Takisto je možné vykonávať redukciu po každom pridaní

nového polynómu. Takáto medziredukcia môže výpočet zrýchliť, môže ho však aj spomaliť (veľa medziredukcií môže zabrať viac času, ako samotný výpočet bez nich).

Zaujímavejšie je zrýchliť algoritmus na inom mieste. Najviac času zaberie testovanie, či daný S-polynóm sa redukuje na nulový polynóm. Pritom práve nulový výsledok redukcie sa objaví pomerne často (algoritmus vďaka tomu skončí) a celý proces redukcie na nulu nijako ďalej nevyužívame. Našťastie, veľa takýchto nulových redukcií možno predvídať bez výpočtov a preskočiť ich. Stačia k tomu nasledovné dve zistenia.

Veta 2.14. Ak $\mathrm{nsn}(\mathrm{ht}(f), \mathrm{ht}(g)) = \mathrm{ht}(f) \cdot \mathrm{ht}(g)$, potom $\mathrm{S}(f, g) \mapsto^{+}_{\{f,g\}} 0$.

□

Veta 2.15. G je Gröbnerova báza práve vtedy, keď pre každé $f, g \in G$ platí aspoň jedna z týchto podmienok.

(*i*) $\mathrm{S}(f, g) \mapsto^{+}_{G} 0$,

(*ii*) $\exists h \in G$, $f \neq h \neq g$, taký, že

$$\mathrm{ht}(h) \mid \mathrm{nsn}(\mathrm{ht}(f), \mathrm{ht}(g)), \quad \mathrm{S}(f, h) \mapsto^{+}_{G} 0\,, \quad \mathrm{S}(h, g) \mapsto^{+}_{G} 0\,.$$

□

Veta 2.14 umožňuje netestovať v Buchbergerovom algoritme S-polynómy takých f, g z bázy, pre ktoré $\mathrm{nsn}(\mathrm{ht}(f), \mathrm{ht}(g)) = \mathrm{ht}(f) \cdot \mathrm{ht}(g)$. Veta 2.15 zasa takých, ku ktorým existuje v báze polynóm h, ktorý sme už s oboma testovali (teda $\mathrm{S}(f, h)$ aj $\mathrm{S}(h, g)$ sa už oba redukujú na nulu) a ktorý spĺňa $\mathrm{ht}(h) \mid \mathrm{nsn}(\mathrm{ht}(f), \mathrm{ht}(g))$. Dôkazy uvedených kritérií možno nájsť v [6].

Hlbší pohľad do problematiky detekovania nenutných redukcií v algoritme možno nájsť v [7]. My si vystačíme s textom uvedeným v tejto kapitole, ktorý nás teoreticky zabezpečil pre ďalšie využitie.

Kapitola 3

Dôkazy viet elementárnej geometrie

3.1 Princíp dokazovania

V dvadsiatom storočí zaznamenala matematika veľké zmeny. Vyvinulo sa množstvo nových odvetví, vyriešili sa problémy, ktoré odolávali celé desaťročia a storočia a nastolili sa nové. Jednu z významných zmien priniesli počítače. Pomocou nich je možné obrovské množstvo automatických operácií vykonať v krátkom čase. Spomeňme napríklad *problém štyroch farieb* alebo *Keplerov problém* (zaoberá sa úlohou, ako čo najefektívnejšie pokryť priestor rovnakými guľami), ktoré sa tak podarilo vyriešiť. Výpočtová technika nám pomôže aj pri transformácii bázy ideálu na Gröbnerovu. Stačí vhodne implementovať Buchbergerov algoritmus. Množstvo výpočtov potrebných pri redukcii je ručne vykonávať nemožné.

Otázkou, ktorou sa budeme zaoberať a ktorú prevedieme do reči polynomických ideálov, je dokazovanie viet v geometrii. Zamyslime sa, ako sú často formulované geometrické dôkazové úlohy. Dané sú nejaké predpoklady hovoriace o tom, v akom vzťahu (kolmosť, rovnobežnosť, incidencia, vzdialenosť) sú k sebe postavené rôzne geometrické útvary (priamky, body, kružnice a iné). Na základe týchto predpokladov treba odvodiť tvrdenie, ktoré takisto hovorí o vzťahoch medzi útvarmi.

Pritom všetky tieto vzťahy sa dajú dobre algebraicky popísať pomocou analytickej geometrie. Každý bod v rovine vieme jednoznačne určiť jeho dvoma reálnymi súradnicami (množinu reálnych čísel označujme $\mathbb{R}$) a útvary zasa konečným počtom bodov. Jednotlivé súvislosti tak prepíšeme pomocou súradníc vystupujúcich bodov. Ukážme si stručne na príkladoch algebraický prepis základných vzťahov, aby sme videli, aké výrazy vzniknú.

Príklad 3.1. V rovine sú súradnicami dané body $A = (a_x, a_y)$, $B = (b_x, b_y)$ a $C = (c_x, c_y)$ ($B \neq C$). Chceme pomocou súradníc prepísať podmienku, že bod A leží na priamke BC. To platí práve vtedy, keď vektory $B - A = (b_x - a_x, b_y - a_y)$ a $C - A = (c_x - a_x, c_y - a_y)$ sú lineárne

závislé, teda keď determinant matice, ktorú tieto dva vektory tvoria, je nulový. To zapíšeme

$$(b_x - a_x)(c_y - a_y) - (b_y - a_y)(c_x - a_x) = 0\,. \tag{3.1}$$

Podmienka má teda tvar $q_1(a_x, a_y, b_x, b_y, c_x, c_y) = 0$, kde $q_1 \in \mathbb{Q}[x_1, \ldots, x_6]$.

□

Príklad 3.2. V rovine sú dané priamky AB a CD súradnicami bodov $A = (a_x, a_y)$, $B = (b_x, b_y)$, $C = (c_x, c_y)$ a $D = (d_x, d_y)$. Zaujíma nás, či sú na seba kolmé. Stačí otestovať, či skalárny súčin ich smerových vektorov je nulový, t. j. či

$$(b_x - a_x)(d_x - c_x) + (b_y - a_y)(d_y - c_y) = 0\,. \tag{3.2}$$

Podmienka má polynomický tvar $q_2(a_x, a_y, b_x, b_y, c_x, c_y, d_x, d_y) = 0$, $q_2 \in \mathbb{Q}[x_1, \ldots, x_8]$.

□

Príklad 3.3. Krajné body úsečiek AB a CD majú súradnice $A = (a_x, a_y)$, $B = (b_x, b_y)$, $C = (c_x, c_y)$ a $D = (d_x, d_y)$. Majú úsečky rovnakú dĺžku? Podľa Pytagorovej vety nás teda zaujíma platnosť rovnosti

$$\sqrt{(a_x - b_x)^2 + (a_y - b_y)^2} = \sqrt{(c_x - d_x)^2 + (c_y - d_y)^2}\,,$$

ktorá je ekvivalentná s rovnosťou

$$(a_x - b_x)^2 + (a_y - b_y)^2 - (c_x - d_x)^2 - (c_y - d_y)^2 = 0\,. \tag{3.3}$$

Opäť máme polynomický tvar $q_3(a_x, a_y, b_x, b_y, c_x, c_y, d_x, d_y) = 0$, $q_3 \in \mathbb{Q}[x_1, \ldots, x_8]$.

□

Podobným spôsobom sa dajú zapísať podmienky na rovnobežnosť priamok (cez lineárnu závislosť smerových vektorov), zhodnosť obsahov (cez vektorový súčin), zhodnosť uhlov, zhodnosť vzdialeností od útvarov a ďalšie. Samozrejme, nemusíme sa obmedziť iba na rovinu. Rovnako môžeme postupovať v priestore či vo viacrozmernej geometrii.

Majme teraz nejakú dôkazovú úlohu v geometrii a pozrime sa, ako ju môžeme preformulovať. Zvolíme si vhodnú súradnicovú sústavu a každému bodu zo zadania priradíme dve premenné – x-ovú a y-ovú súradnicu. V praxi je dobré zvoliť počiatok a smer osí tak, aby sme museli zaviesť čo najmenej premenných (napríklad ak leží bod na x-ovej osi, jeho prvá súradnica je automaticky nulová a stačí tak priradiť mu jednu premennú). Povedzme, že zavedené premenné budú $x_1, \ldots, x_n$. Predpoklady zadania prepíšeme pomocou polynómov p_i, ako ukazujú príklady

3.1, 3.2 a 3.3. Rovnako prepíšeme aj tvrdenie, ktoré chceme dokázať (povedzme podmienkou $t = 0$). Všetky tieto polynómy môžeme chápať ako prvky $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[\mathbf{x}]$ (konkrétne $\mathbb{F} = \mathbb{Q}$). Úloha nakoniec nadobudne tvar

$$p_1 = 0\,,\ \ldots\ ,\ p_m = 0 \qquad \stackrel{?}{\Longrightarrow} \qquad t = 0\,. \tag{3.4}$$

Inými slovami, chceme ukázať, že ak pre $x_1, \ldots, x_n \in \mathbb{R}$ platí $p_i(x_1, \ldots, x_n) = 0$ (pre každé $i = 1, \ldots, m$), potom aj $t(x_1, \ldots, x_n) = 0$. Ak sa nám implikáciu (3.4) podarí dokázať, znamená to, že kedykoľvek sú splnené predpoklady, platí aj tvrdenie. Vyriešime tým pôvodnú geometrickú úlohu. Ak implikáciu vyvrátime, t. j. nájdeme $x_1, \ldots, x_n \in \mathbb{R}$ také, že predpoklady sú splnené a tvrdenie nie, ešte to nemusí znamenať, že pôvodné geometrické tvrdenie neplatí. Hodnoty $x_1, \ldots, x_n$, ktoré implikáciu vyvracajú, totiž môžu reprezentovať takú geometrickú situáciu, ktorá pre zadanie nie je prípustná – tzv. *degenerovaný prípad* (napr. identickosť dvoch bodov, ktoré sú zo zadania apriori rôzne). Tomuto prípadu sa budeme venovať v nasledujúcej podkapitole.

Zamyslime sa nad tým, ako by sa dala implikácia (3.4) dokázať. Ak sa nám podarí vyjadriť polynóm t vhodným skombinovaním polynómov p_i, presnejšie, ak nájdeme $f_i \in \mathbb{F}[\mathbf{x}]$ také, že

$$t = f_1 p_1 + \cdots + f_m p_m\,, \tag{3.5}$$

potom zrejme (3.4) platí. Také f_i sa nám skutočne môže podariť nájsť, ako ukazuje nasledujúci príklad.

Príklad 3.4. Pokúsme sa načrtnutým postupom dokázať, že ťažnice v ľubovoľnom trojuholníku ABC sa pretínajú v jednom bode. Označme stredy strán BC, CA a AB postupne K, L a M. Priesečník priamok BL a CM označme T. Chceme ukázať, že T leží na AK.

Zaveďme súradnicovú sústavu a premenné c_x, c_y, t_x, t_y tak, ako ukazuje obrázok 3.1. Predpoklady tvrdenia sú $T \in BL$ a $T \in CM$. Pomocou (3.1) ich (po úprave) prepíšeme na

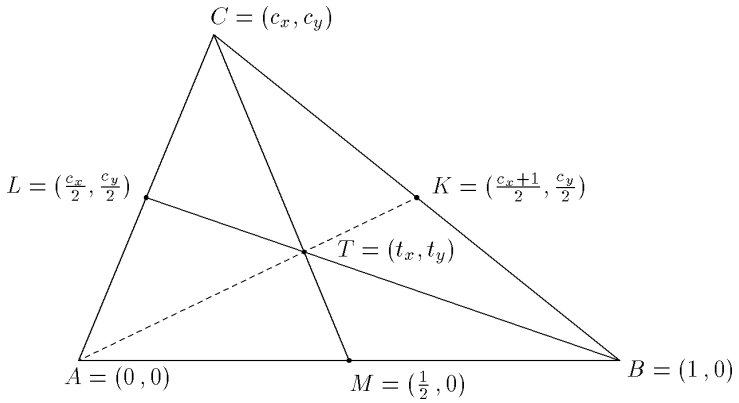
$$p_1 = \frac{c_y}{2} - t_y - \frac{t_x c_y}{2} + \frac{t_y c_x}{2} = 0 \qquad \text{a} \qquad p_2 = -t_y c_x - \frac{c_y}{2} + t_x c_y + \frac{t_y}{2} = 0\,.$$

Dokazované tvrdenie $T \in AK$ prepíšeme rovnakým spôsobom ako

$$t = -\frac{t_x c_y}{2} + \frac{t_y c_x}{2} + \frac{t_y}{2} = 0\,.$$

Keďže $t = -p_1 - p_2$, tvrdenie z predpokladov naozaj vyplýva – našli sme polynómy f_1 a f_2 také, že $t = f_1 p_1 + f_2 p_2$ (konkrétne $f_1 = f_2 = -1$).

□



Obr. 3.1: *Príklad 3.4*

Vo väčšine prípadov je situácia oveľa komplikovanejšia a polynómy f_i nemožno uhádnuť. Na pomoc tak prichádza teória polynomických ideálov, nakoľko vyjadrenie (3.5) je ekvivalentné s tým, že t patrí do ideálu $\langle p_1, \ldots, p_m \rangle$ (pozri (1.3)). Prvý spôsob na riešenie (3.4) sa nám priamo ponúka. Stačí skonštruovať pre bázu $\{p_1, \ldots, p_m\} = P$ Gröbnerovu bázu G (vzhľadom na ľubovoľne zvolené $<_T$) a redukovať ňou t. Ak $t \mapsto_G^+ 0$, tak (3.4) platí. Ale čo ak $t \mapsto_G^* t' \neq 0$? Môžeme v takom prípade povedať, že (3.4) neplatí? Určite nie. Neplatí to ani pri polynómoch jednej premennej. Na kontrapríklad stačí zobrať $m = 1$, $p_1 = x^2$ a $t = x$. Potom $t \notin \langle p_1 \rangle$, ale z nulovosti p_1 celkom iste vyplýva nulovosť t.

Ak teda zistíme, že $t \notin \langle P \rangle$, môžeme rovnakým spôsobom otestovať, či $t^2 \in \langle P \rangle$. Ak áno, potom (3.4) platí (ak $t^2 = 0$, nutne aj $t = 0$). A ak nie, môžeme skúšať šťastie s ďalšími mocninami t. Tento postup skutočne často funguje. V praxi dokonca (v prípade platnosti (3.4)) väčšinou už z prvého testu (či $t \in \langle P \rangle$) získame kladnú odpoveď. Takýmto spôsobom (spolu s pridaním doplňujúcich podmienok, o ktorých pojednáva ďalšia podkapitola) dokázali Kutzler a Stifter [8] množstvo základných viet elementárnej geometrie.

Teoretické zázemie pre Kutzlerov a Stifterov postup poskytuje slávna Hilbertova *Null-stellensatz*, ktorú použijeme aj neskôr a preto ju tu uvedieme (dôkaz možno nájsť v [6]).

Veta 3.1. (*Hilbertova o nulách.*) Nech $p_1, \ldots, p_m \in \mathbb{F}[\mathbf{x}]$ a $\mathbb{H}$ je algebraicky uzavreté rozšírenie poľa $\mathbb{F}$. Potom nasledujúce dve podmienky sú ekvivalentné.

(*i*) $\forall x \in \mathbb{H}^n \qquad p_1(x) = 0\,,\ \ldots\ ,\ p_m(x) = 0 \quad \Longrightarrow \quad t(x) = 0\,.$

(*ii*) $\exists r \in \mathbb{N}$ také, že $t^r \in \langle p_1, \ldots, p_m \rangle$.

□

Podľa tejto vety z platnosti implikácie (3.4) vyplýva, že niektorá mocnina t do $\langle P\rangle$ padne. Nutné ale je, aby implikácia platila pre algebraicky uzavreté rozšírenie poľa $\mathbb{F} = \mathbb{Q}$. Pole $\mathbb{R}$ pritom algebraicky uzavreté nie je, je ním až $\mathbb{C}$ (pole komplexných čísel). Uvedeným postupom tak možno dokázať len tvrdenia, ktoré platia vo všeobecnejšej komplexnej verzii. Tento nedostatok zatiaľ ponechajme bokom. Mnohé tvrdenia o reálnych číslach platia v skutočnosti aj o komplexných.

Zamyslime sa radšej nad situáciou, keď implikácia (3.4) v rozšírení na $\mathbb{C}$ neplatí. Vtedy nám predchádzajúci postup nedá odpoveď na otázku, či (3.4) platí. Nemôžeme testovať mocniny t nekonečne dlho. Môžeme len na základe neúspešných testov pre niekoľko prvých mocnín t odhadovať, že implikácia neplatí.

Chceli by sme taký algoritmus, ktorý implikáciu (3.4) dokáže nie iba overiť, ale (v prípade, že neplatí pre $\mathbb{C}$) aj vyvrátiť. Na to bude dobré preformulovať túto otázku trochu inak. Zrejme platnosť (3.4) (či už v $\mathbb{R}$ alebo v $\mathbb{C}$) je ekvivalentná s tým, že každé riešenie sústavy

$$p_1 = 0\,,\ \ldots\ ,\ p_m = 0 \tag{3.6}$$

(v príslušnom poli) je riešením rovnice $t = 0$. Pritom ak $t = 0$, tak rovnica $tz - 1 = 0$ nemá v neznámej z riešenie. Ale aj naopak, ak $t \neq 0$, rovnica $tz - 1 = 0$ riešenie celkom isto má (konkrétne $z = 1/t$). Uvedomiac si všetko spolu máme, že (3.4) platí práve vtedy, keď sústava

$$p_1 = 0\,,\ \ldots\ ,\ p_m = 0\,,\ tz - 1 = 0 \tag{3.7}$$

nemá riešenie v neznámych $\{x_1, \ldots, x_n, z\}$. (Skutočne, ak (3.4) platí a n-tica $(x_1, \ldots, x_n)$ spĺňa prvých m rovníc sústavy (3.7), spĺňa celú (3.6) a preto spĺňa aj $t = 0$. Preto $tz - 1 = 0$ nemá riešenie a nemôže ho mať ani (3.7). Naopak, ak (3.4) neplatí, existuje n-tica spĺňajúca (3.6) a $t \neq 0$, potom ale tá istá n-tica spolu so $z = 1/t$ je riešením (3.7)).

Otázku platnosti implikácie (3.4) sa nám teda podarilo transformovať na otázku neriešiteľnosti sústavy (3.7). O riešiteľnosti ľubovoľnej sústavy možno rozhodnúť vďaka nasledujúcemu jednoduchému dôsledku Hilbertovej Nullstellensatz.

Veta 3.2. Nech $q_1, \ldots, q_k \in \mathbb{F}[\mathbf{x}]$ a $\mathbb{H}$ je algebraicky uzavreté rozšírenie poľa $\mathbb{F}$. Potom sústava

$$q_1 = 0\,,\ \ldots\ ,\ q_k = 0 \tag{3.8}$$

nemá v $\mathbb{H}$ riešenie práve vtedy, keď $1 \in \langle q_1, \ldots, q_k\rangle$.

Dôkaz: Stačí vo vete 3.1 dosadiť $t = 1$, $m = k$ a $p_i = q_i$. Ak sústava (3.8) nemá riešenie, potom je v Hilbertovej vete podmienka (*i*) splnená (lebo predpoklad implikácie nie je splnený pre žiadne $x \in \mathbb{H}^n$) a teda je splnená aj podmienka (*ii*), čiže $1^r = 1 \in \langle q_1, \ldots, q_k\rangle$.

Naopak, ak $1 \in \langle q_1, \ldots, q_k \rangle$, je splnená (*ii*), preto platí aj (*i*) a sústava (3.8) nemôže mať riešenie (žiadne $x \in \mathbb{H}^n$ nespĺňa rovnicu $1 = 0$).

□

O neriešiteľnosti sústavy (3.7) vďaka vete 3.2 rozhodneme tak, že overíme, či $1 \in \langle P, tz - 1 \rangle$ (uvažujeme okruh $\mathbb{F}[\mathbf{x}, z]$), t. j. či Gröbnerova báza tohoto ideálu (po normovaní) obsahuje jednotku (ak ju neobsahuje, potom $1 \notin \langle P, tz - 1 \rangle$, lebo 1 sa dá redukovať iba sama sebou). Vlastne tak overíme, či $\langle P, tz - 1 \rangle = \mathbb{F}[\mathbf{x}]$. Poznamenajme, že ak Gröbnerova báza ideálu obsahuje 1, tak redukovaná Gröbnerova báza je rovná $\{1\}$. Takýmto spôsobom postupoval pri dokazovaní geometrických tvrdení Kapur [9].

Našli sme postup, ako určíme platnosť implikácie (3.4), opäť však overíme jej platnosť v $\mathbb{C}$, nie v $\mathbb{R}$. V prípade, že redukovaná Gröbnerova báza ideálu $\langle P, tz - 1 \rangle$ nebude $\{1\}$, vieme z vety 3.2, že (3.4) neplatí, teda existujú $x_1, \ldots, x_n \in \mathbb{C}$, že $p_i(x_1, \ldots, x_n) = 0$ ($i = 1, \ldots, m$) a $t(x_1, \ldots, x_n) \neq 0$. Ako uvidíme v nasledujúcej podkapitole, z Gröbnerovej bázy ideálu $\langle P, tz - 1 \rangle$ možno v tomto prípade dobre analyzovať štruktúru riešení (3.7) a dokonca niekedy komplexné riešenia a riešenia reprezentujúce degenerované prípady eliminovať a pôvodné geometrické tvrdenie dokázať. To je hlavná výhoda Kapurovej metódy oproti Kutzlerovej a Stifterovej metóde, ktorá je zasa rýchlejšia (Gröbnerovu bázu v nej tvoríme pre ideál s menším počtom generujúcich polynómov a menším počtom premenných – bez polynómu $tz - 1$ a bez premennej z).

Uveďme si teraz dva príklady. Jeden ako demonštráciu, že implikácia (3.4) môže platiť v $\mathbb{R}$ a neplatiť v $\mathbb{C}$, druhý ako aplikáciu Kapurovho postupu.

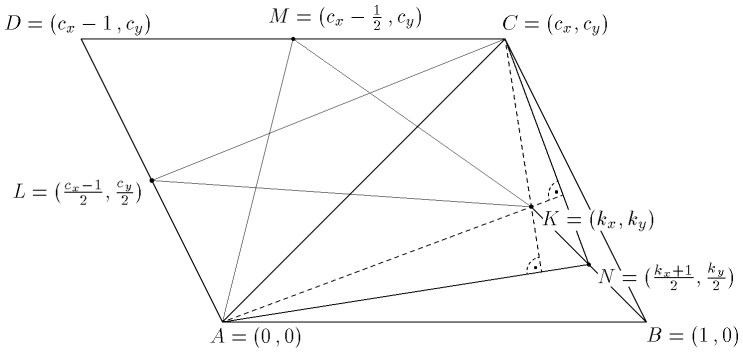
Príklad 3.5. Majme polynómy $p, t \in \mathbb{Q}[x, y]$, $p = x^2 + y^2$, $t = x$. Potom v reálnych číslach implikácia

$$p = 0 \qquad \Longrightarrow \qquad t = 0$$

platí (ak $x, y \in \mathbb{R}$ spĺňajú $x^2 + y^2 = 0$, nutne $x = y = 0$), ale v komplexných číslach neplatí (stačí zobrať $x = 1$ a $y = i$) a $1 \notin \langle x^2 + y^2, xz - 1 \rangle$. V skutočnosti pri lexikografickom usporiadaní takom, že $x <_L y <_L z$ je $\{y^2 + x^2, zx - 1\}$ priamo redukovaná Gröbnerova báza (stačí v príklade 2.7 vymeniť premenné x a z) a neobsahuje jednotku.

□

Príklad 3.6. (*Ruská MO 2001.*) Vnútri rovnobežníka $ABCD$ leží bod K, pričom $|CL| = |LK|$ a $|AM| = |MK|$, kde L a M sú postupne stredy strán AD a CD. Označme N stred úsečky BK. Dokážte, že K je priesečníkom výšok trojuholníka ANC.



Obr. 3.2: *Príklad 3.6*

Zaveďme súradnice a premenné ako na obrázku 3.2. Predpoklady sú $|CL| = |LK|$ a $|AM| = |MK|$, dokazované tvrdenia sú $AK \perp CN$ a $CK \perp AN$. Pomocou (3.3) prepíšeme predpoklady na

$$p_1 = \left(\tfrac{c_x}{2} + \tfrac{1}{2}\right)^2 + \tfrac{c_y^2}{4} - \left(\tfrac{c_x}{2} - \tfrac{1}{2} - k_x\right)^2 - \left(\tfrac{c_y}{2} - k_y\right)^2 = 0\,,$$
$$p_2 = \left(\tfrac{1}{2} - c_x\right)^2 + c_y^2 - \left(c_x - \tfrac{1}{2} - k_x\right)^2 - (c_y - k_y)^2 = 0$$

a tvrdenia cez (3.2) na

$$t_1 = k_x\left(\tfrac{k_x}{2} + \tfrac{1}{2} - c_x\right) + k_y\left(\tfrac{k_y}{2} - c_y\right) = 0\,,$$
$$t_2 = (k_x - c_x)\left(\tfrac{k_x}{2} + \tfrac{1}{2}\right) + (k_y - c_y)\tfrac{k_y}{2} = 0\,.$$

Gröbnerova báza ideálu $\langle p_1, p_2, t_1 z - 1\rangle$ v okruhu $\mathbb{Q}[c_x, c_y, k_x, k_y, z]$ je $\{1\}$, preto $AK \perp CN$. Rovnako aj ideál $\langle p_1, p_2, t_2 z - 1\rangle$ má Gröbnerovu bázu $\{1\}$ a teda $CK \perp AN$. K je potom nutne priesečník výšok trojuholníka ANC.

□

3.2 Doplňujúce podmienky

V predchádzajúcom texte sme úplne vyriešili otázku platnosti implikácie (3.4) nad $\mathbb{C}$. Ako sme poznamenali, môže sa stať, že (3.4) neplatí ani nad $\mathbb{R}$ a napriek tomu pôvodné geometrické tvrdenie platí. Príčinou je, že neplatnosť implikácie nastane len pre nejaký degenerovaný alebo špeciálny prípad, ktorý zadanie nepripúšťa. Presnejšie preformulovanie geometrického tvrdenia ako implikácia (3.4) poskytuje implikácia

$$p_1 = 0\,,\ \ldots\,,\ p_m = 0\,,\ s_1 \neq 0\,,\ \ldots\,,\ s_\ell \neq 0 \qquad \stackrel{?}{\Longrightarrow} \qquad t = 0\,, \tag{3.9}$$

kde $s_1, \ldots, s_\ell$ sú polynómy reprezentujúce degenerované alebo špeciálne prípady (prípadne aj komplexné riešenia sústavy (3.7)). Nazývajme ich *doplňujúce podmienky*. Doplňujúce podmienky môžeme vytvoriť priamo zo zadania. Povedzme v príklade 3.4 sme mohli pridať podmienku $c_y \neq 0$ (bod C nemôže ležať na priamke AB).

Podobne ako pre implikáciu (3.4), pokúsme sa pre (3.9) zostrojiť algoritmus, ktorý rozhodne o jej platnosti. Zrejme (3.9) je ekvivalentná s implikáciou

$$p_1 = 0\,,\ \ldots\ ,\ p_m = 0 \qquad \stackrel{?}{\Longrightarrow} \qquad s_1 = 0\ \vee\ \cdots\ \vee\ s_\ell = 0\ \vee\ t = 0\,. \tag{3.10}$$

Tento tvar sa už viac podobá na tvar (3.4), otázku platnosti ktorého sme v predchádzajúcej podkapitole transformovali na otázku neriešiteľnosti sústavy (3.7). Rovnako si pomôžeme aj teraz. Platnosť (3.10) je totiž ekvivalentná s tým, že sústava

$$p_1 = 0\,,\ \ldots\ ,\ p_m = 0\,,\ s_1 z_1 - 1 = 0\,,\ \ldots\ ,\ s_\ell z_\ell - 1 = 0\,, tz - 1 = 0 \tag{3.11}$$

nemá riešenie v neznámych $\{x_1, \ldots, x_n, z_1, \ldots, z_\ell, z\}$.

Zdôvodnenie tejto ekvivalencie je rovnaké ako v situácii bez doplňujúcich podmienok. Ak platí implikácia (3.10) a n-tica $(x_1, \ldots, x_n)$ spĺňa prvých m rovníc sústavy (3.11), musí spĺňať aspoň jednu z rovností na pravej strane (3.10), povedzme $s_i = 0$ (resp. $t = 0$). Potom nenájdeme z_i (resp. z) také, že $s_i z_i - 1 = 0$ (resp. $tz - 1 = 0$). Teda sústava (3.11) nemá riešenie.

Naopak, ak (3.10) neplatí, existuje n-tica spĺňajúca prvých m rovníc sústavy (3.11) a nespĺňajúca žiadnu z rovností na pravej strane (3.10). Potom ale tá istá n-tica spolu so $z_i = 1/s_i$ ($i = 1, \ldots, \ell$) a $z = 1/t$ je riešením (3.11).

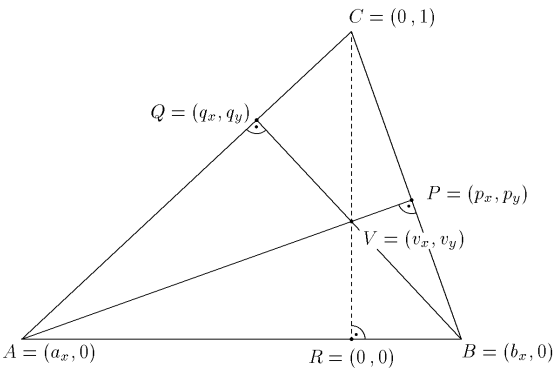
Na overenie platnosti (3.9) teda stačí overiť neriešiteľnosť sústavy (3.11). To urobíme (použijeme vetu 3.2) tak, že zistíme, či redukovaná Gröbnerova báza ideálu

$$\langle p_1\,,\ \ldots\ ,\ p_m\,,\ s_1 z_1 - 1\,,\ \ldots\ ,\ s_\ell z_\ell - 1\,,\ tz - 1\rangle$$

je rovná $\{1\}$. I keď platnosť (3.9) overíme iba nad $\mathbb{C}$, nie nad $\mathbb{R}$, tento prístup bude oveľa úspešnejší ako prístup bez doplňujúcich podmienok. Ilustrujme si to na nasledujúcom príklade.

Príklad 3.7. Snažme sa dokázať, že v každom trojuholníku ABC sa výšky pretínajú v jednom bode. Označme body a zaveďme súradnice a premenné tak, ako na obrázku 3.3. Predpoklady tvrdenia sú $P \in BC$, $AP \perp BC$, $Q \in AC$, $BQ \perp AC$, $V \in AP$ a $V \in BQ$. Dokazované tvrdenie je $V \in CR$. Pomocou (3.1) a (3.2) prepíšeme predpoklady na

$$\begin{aligned}
&p_1 = (b_x - p_x)(1 - p_y) - p_y p_x = 0\,, && p_2 = -(p_x - a_x)b_x + p_y = 0\,,\\
&p_3 = (a_x - q_x)(1 - q_y) - q_y q_x = 0\,, && p_4 = -(q_x - b_x)a_x + q_y = 0\,,\\
&p_5 = (a_x - v_x)(p_y - v_y) + v_y(p_x - v_x) = 0\,, && p_6 = (b_x - v_x)(q_y - v_y) + v_y(q_x - v_x) = 0
\end{aligned}$$



Obr. 3.3: *Príklad 3.7*

a tvrdenie na $t = v_x = 0$. Gröbnerovu bázu pre $\langle p_1, p_2, p_3, p_4, p_5, p_6, tz - 1\rangle$ so stupňovým usporiadaním termov takým, že $z >_D v_x >_D v_y >_D p_x >_D p_y >_D q_x >_D q_y >_D a_x >_D b_x$ tvoria polynómy (zoradené podľa $\prec_D$)

$$
\begin{array}{l}
a_x^2 - 2a_xb_x + b_x^2\,, \quad q_ya_x + q_x - a_x\,, \quad q_xa_x - a_xb_x - q_y\,, \quad q_x^2 - q_xb_x + q_y^2 - q_y\,, \quad p_yb_x + p_x - b_x\,,\\
p_ya_x - q_yb_x + p_x - q_x + a_x - b_x\,, \qquad -p_xq_y + p_yq_x + p_x - q_x + a_x - b_x\,, \qquad p_xb_x - a_xb_x - p_y\,,\\
p_xa_x - q_xb_x - 2a_xb_x + 2b_x^2 - p_y + q_y\,, \qquad p_xq_x + p_yq_y - q_xb_x - a_xb_x + b_x^2 - p_y\,,\\
p_x^2 + p_y^2 - q_xb_x - 2a_xb_x + 2b_x^2 - 2p_y + q_y\,, \qquad -v_xq_y + v_yq_x - v_yb_x + q_yb_x\,,\\
\quad \vdots
\end{array}
$$

preto implikácia (3.4) pre tento prípad neplatí (báza neobsahuje 1). Keď pridáme podmienku $s_1 = a_x - b_x \neq 0$ (body A a B sú rôzne), vyjde nám pre $\langle p_1, p_2, p_3, p_4, p_5, p_6, s_1z_1 - 1, tz - 1\rangle$ Gröbnerova báza $\{1\}$. Tvrdenie teda dokážeme až po pridaní doplňujúcej podmienky.

□

Pri zložitejšom zadaní sa ponúka doplňujúcich podmienok, ktoré možno pridať k predpokladom, viacej. Keď ich pridáme príliš veľa, môže sa stať, že ani na výkonnejších počítačoch Gröbnerovu bázu v rozumnom čase nevygenerujeme (každá doplňujúca podmienka pridá do generujúcej bázy jeden polynóm a jednu novú premennú z_i). Dopredu pritom nie je jasné, ktoré doplňujúce podmienky zabezpečia platnosť implikácie (3.9).

Dobré by bolo nájsť nejaký spôsob, ako vhodné doplňujúce podmienky odhaliť. Vráťme sa k prípadu bez doplňujúcich podmienok a predpokladajme, že redukovaná Gröbnerova báza G pre ideál $\langle P, tz - 1\rangle$ nie je $\{1\}$. Aké podmienky treba pridať, aby sme platnosť tvrdenia zachránili? Dobrým kandidátom sú polynómy z vygenerovanej Gröbnerovej bázy. Skutočne, ak $g \in G$, tak ideál $\langle P, gz_1 - 1, tz - 1\rangle$ obsahuje polynómy g aj $gz_1 - 1$ a tým pádom aj polynóm

$$z_1 \cdot g - 1 \cdot (gz_1 - 1) = 1\,.$$

Preto

$$\langle P, gz_1 - 1, tz - 1\rangle = \langle 1\rangle \tag{3.12}$$

a teda implikácia

$$p_1 = 0\ ,\ \ldots\ ,\ p_m = 0\ ,\ g \neq 0 \qquad \Longrightarrow \qquad t = 0$$

platí. Dokonca nemusíme znova generovať pre $\langle P, gz_1 - 1, tz - 1\rangle$ Gröbnerovu bázu, dopredu vieme, že vyjde $\{1\}$.

Za reprezentanta doplňujúcej podmienky však nemôžeme zvoliť ľubovoľný polynóm z G. Môžeme zvoliť iba taký polynóm, ktorý nezmení pôvodné geometrické tvrdenie (v takom zmysle sme doplňujúce podmienky pôvodne zaviedli). V G môže byť napríklad niektorý polynóm p_i. Implikácia

$$p_1 = 0\ ,\ \ldots\ ,\ p_m = 0\ ,\ p_i \neq 0 \qquad \Longrightarrow \qquad t = 0$$

síce platí, ale nemá nič spoločné s pôvodným tvrdením – je to tautológia (keďže predpoklad nie je nikdy splnený). Tautológiu dostaneme vždy, keď vezmeme z G taký polynóm g, ktorého niektorá mocnina patrí do $\langle P\rangle$ (z nulovosti polynómov z P vyplýva $g = 0$ a nemôže súčasne platiť aj $g \neq 0$). Takéto polynómy zobrať nemôžeme. Z predchádzajúceho vieme, že pre ne (a práve pre ne) platí $\langle P, gz - 1\rangle = \langle 1\rangle$.

Rovnako nemôžeme z G zobrať polynómy obsahujúce premennú z – nie sú prvkami $\mathbb{F}[\mathbf{x}]$ a nemôžu tak reprezentovať špeciálne či degenerované prípady. Navyše ekvivalencia platnosti (3.9) a neriešiteľnosti (3.11) je založená na tom, že z je umelo zavedená nová premenná, ktorá sa nevyskytuje v polynómoch $p_1, \ldots, p_m, s_1, \ldots, s_\ell$.

Ostane v G ešte nejaký polynóm, keď vylúčime tieto dva typy? Príklad 3.7, ukazuje, že taký polynóm môže existovať. Hneď prvý polynóm z vygenerovanej bázy nám dá vhodnú doplňujúcu podmienku $(a_x - b_x)^2 \neq 0$ (táto je ekvivalentná s podmienkou $a_x - b_x \neq 0$, ktorú sme v príklade použili).

Taký polynóm samozrejme nemusí existovať (napríklad, ak pôvodné geometrické tvrdenie neplatí). Zaujímavejšia je otázka, či sa môže stať, že existuje vhodná doplňujúca podmienka, ale v Gröbnerovej báze sa taká nenájde. Prvýkrát bude odpoveď závisieť na zvolenom usporiadaní termov. Vo všeobecnosti sa to stať môže (napriek existencii vhodnej doplňujúcej podmienky z Gröbnerovej bázy takú neurčíme). Avšak ak zvolíme usporiadanie termov správne, veta, ktorú ponúka Kapur [9], zabezpečí, že doplňujúce podmienky stačí hľadať v Gröbnerovej báze. Ešte pred vetou si zaveďme pojem, ktorý budeme pri jej dôkaze potrebovať.

Definícia 3.1. Majme v $\mathbb{F}[\mathbf{x}]$ ideál $\langle P\rangle$. Potom *ideál radikálov* $\langle P\rangle$ je množina $\operatorname{Rad}\langle P\rangle \subseteq \mathbb{F}[\mathbf{x}]$ definovaná

$$q \in \operatorname{Rad}\langle P\rangle \qquad \Longleftrightarrow \qquad \exists r \in \mathbb{N} \quad \text{také, že} \quad q^r \in \langle P\rangle \ .$$

□

Overme, že množina $\operatorname{Rad}\langle P\rangle$ je ideál. Ak $u, v \in \operatorname{Rad}\langle P\rangle$, máme $u^a, v^b \in \langle P\rangle$ a z binomickej vety

$$(u+v)^{a+b} = \sum_{i=0}^{a+b} \binom{a+b}{i} u^i v^{a+b-i} = \underbrace{v^b \cdot \sum_{i=0}^{a} \binom{a+b}{i} u^i v^{a-i}}_{\in\langle P\rangle} + \underbrace{u^a \cdot \sum_{i=a+1}^{a+b} \binom{a+b}{i} u^{i-a} v^{a+b-i}}_{\in\langle P\rangle},$$

teda $(u+v)^{a+b} \in \langle P\rangle$ a $u+v \in \operatorname{Rad}\langle P\rangle$. Ak $q \in \operatorname{Rad}\langle P\rangle$ a $f \in \mathbb{F}[\mathbf{x}]$, máme $q^r \in \langle P\rangle$ a $(qf)^r = q^r f^r \in \langle P\rangle$, čiže $qf \in \operatorname{Rad}\langle P\rangle$.

Ideál radikálov úzko súvisí s naším problémom. Podľa vety 3.1 platnosť (3.4) je ekvivalentná s tým, že polynóm reprezentujúci dokazované tvrdenie patrí do ideálu radikálov polynómov reprezentujúcich predpoklady.

Uveďme teraz spomínanú Kapurovu vetu.

Veta 3.3. Majme $P = \{p_1, \ldots, p_m\} \subset \mathbb{F}[\mathbf{x}]$ a $t \in \mathbb{F}[\mathbf{x}]$ také, že $\langle P, tz-1\rangle \neq \langle 1\rangle$ a existuje $s \in \mathbb{F}[\mathbf{x}]$ spĺňajúce

(*i*) $\langle P, sz_1 - 1\rangle \neq \langle 1\rangle$,

(*ii*) $\langle P, sz_1 - 1, tz - 1\rangle = \langle 1\rangle$.

Nech G je Gröbnerova báza ideálu $\langle P, tz-1\rangle$ vzhľadom na lexikografické usporiadanie termov $<_L$ také, že $z >_L x_i$ (pre všetky $i = 1, \ldots, n$). Potom existuje $g \in G$ neobsahujúci premennú z, ktorý spĺňa (*i*) a (*ii*) rovnako ako s.

Dôkaz: To, že každé g z G spĺňa (*ii*), sme už vysvetlili v úvahách vedúcich k (3.12). Stačí ukázať existenciu polynómu $g \in G \cap \mathbb{F}[\mathbf{x}]$ spĺňajúceho (*i*).

V súvislosti s Hilbertovou vetou a s ostatným v predchádzajúcej podkapitole máme

$$\text{(3.4) platí nad } \mathbb{C} \qquad \Longleftrightarrow \qquad t \in \operatorname{Rad}\langle P\rangle \qquad \Longleftrightarrow \qquad \langle P, tz-1\rangle = \langle 1\rangle \ . \tag{3.13}$$

Keď v (3.13) dosadíme namiesto P množinu $P \cup \{tz-1\}$, namiesto t polynóm s a namiesto z premennú z_1, využijúc (*ii*) máme $s \in \operatorname{Rad}\langle P, tz-1\rangle$, teda $s^r \in \langle P, tz-1\rangle$ pre nejaké $r \in \mathbb{N}$.

Preto $s^r \mapsto_G^+ 0$. Polynómy, ktorými túto redukciu vykonáme, nemôžu obsahovať premennú z, pretože každý term w ľubovoľného redukujúceho polynómu spĺňa $w \leq_L \mathrm{ht}(s^r) <_L z$.

Ak by všetky redukujúce polynómy patrili do $\mathrm{Rad}\,\langle P\rangle$, patril by tam aj s^r (lebo $\mathrm{Rad}\,\langle P\rangle$ je ideál) a teda aj s. Podľa (3.13) potom $\langle P, sz_1 - 1\rangle = \langle 1\rangle$, čo je v spore s (*i*). Preto aspoň jeden z redukujúcich polynómov nie je v $\mathrm{Rad}\,\langle P\rangle$, označme ho g. Podľa (3.13) nutne $\langle P, gz_1 - 1\rangle \neq \langle 1\rangle$. □

Požiadavky (*i*) a (*ii*) kladené na s vo vete 3.3 presne vystihujú to, že $s \neq 0$ je vhodná doplňujúca podmienka ((*i*) hovorí, že z nulovosti polynómov v P nevyplýva nulovosť s, (*ii*) zabezpečí nulovosť t za predpokladov nulovosti polynómov v P a nenulovosti s). Ak nejaká vhodná podmienka existuje, podľa vety 3.3 existuje aj v Gröbnerovej báze pre $\langle P, tz - 1\rangle$ vygenerovanej vzhľadom na lexikografické usporiadanie termov (také, že z je $>_L$ od ostatných premenných).

Pre implikáciu (3.4) tak máme úplný algoritmus, ktorý určí, či platí a v prípade, že neplatí, odhalí vhodnú doplňujúcu podmienku, za ktorej platí (ak taká existuje). V závere práce sa nachádza ako algoritmus 4. Pred tým, ako ho otestujeme na náročnejších úlohách, ukážme si jeho využitie na príklade.

Príklad 3.8. Nech K, L a M sú postupne body vnútri strán AB, BC a CA trojuholníka ABC, pričom platí

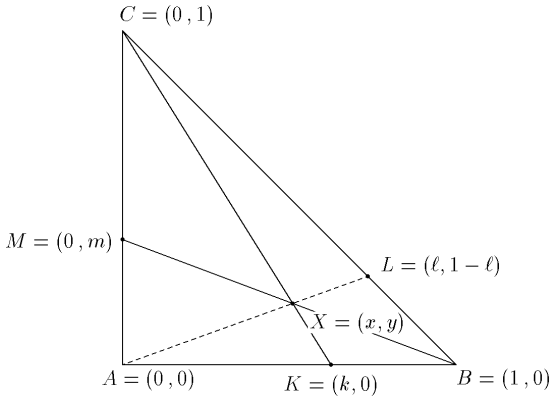
$$\frac{|AK|}{|KB|} \cdot \frac{|BL|}{|LC|} \cdot \frac{|CM|}{|MA|} = 1\,. \tag{3.14}$$

Úlohou je dokázať, že priamky AL, BM a CK sa pretínajú v jednom bode (tvrdenie vyplýva z Cevovej vety).

Každý trojuholník sa dá afinným zobrazením zobraziť na rovnoramenný pravouhlý trojuholník. Pritom hodnota výrazu na ľavej strane v (3.14) sa týmto zobrazením nezmení (je to súčin deliacich pomerov a tie afinita zachováva). Takisto sa nezmení počet priesečníkov priamok (teda ak sa tri priamky pretínajú v jednom bode, budú sa pretínať v jednom bode aj po zobrazení afinitou a naopak). Stačí teda tvrdenie dokázať pre rovnoramenný pravouhlý trojuholník ABC. V súvislosti s tým zaveďme súradnice a premenné ako na obrázku 3.4, kde $X = BM \cap CK$. Chceme ukázať, že $X \in AL$. Predpoklady tvrdenia sú $X \in MB$, $X \in CK$ a rovnosť (3.14). Prepíšeme ich pomocou súradníc na

$$p_1 = mx + y - m = 0\,, \quad p_2 = x + ky - k = 0\,, \quad p_3 = k^2(1-\ell)^2(1-m)^2 - (1-k)^2\ell^2m^2 = 0\,.$$

Dokazované tvrdenie je $t = \ell y + \ell x - x = 0$. Gröbnerova báza ideálu $\langle p_1, p_2, p_3, tz - 1\rangle$



Obr. 3.4: *Príklad 3.8*

vzhľadom na usporiadanie $z >_L x >_L y >_L m >_L k >_L \ell$ je

$$
\begin{array}{l}
mk^2 - mk\ell - mk + m\ell + k^2\ell - k^2 - k\ell + k\,, \qquad m^2k - m^2\ell + mk\ell - 2mk + m\ell - k\ell + k\,,\\
yk^3\ell - yk^3 - yk^2\ell + 2yk^2 - yk\ell - yk + y\ell - k^3\ell + k^3 + 2k^2\ell - 2k^2 - k\ell + k\,,\\
ym\ell + yk^2\ell - yk^2 - yk\ell + 2yk - y\ell - y - mk + m - k^2\ell + k^2 + k\ell - k\,, \qquad ymk - y - mk + m\,,\\
x + yk - k\,, \qquad 2zk^3\ell^2 - 2zk^3\ell - 4zk^2\ell^2 + 4zk^2\ell + 2zk\ell^2 - 2zk\ell - k^3\ell + k^3 + k^2\ell - 2k^2 + k\ell + k - \ell\,,\\
\quad \vdots
\end{array}
$$

Báza nie je $\{1\}$, hľadajme v nej vhodné doplňujúce podmienky. Prvý polynóm z bázy možno upraviť na tvar

$$g = (k-1)(mk - m\ell + k\ell - k)\,.$$

Prvá zátvorka je nenulová ($K \neq B$). Druhá zátvorka je nulová práve vtedy, keď $L \in MK$, čo v našom prípade neplatí. Máme teda vhodnú doplňujúcu podmienku $g \neq 0$. Vlastne sme zároveň okrem Cevovej vety dokázali aj Menelaovu vetu, ktorá hovorí, že ak platí (3.14), ležia body K, L a M na jednej priamke (za predpokladu, že žiadny alebo práve dva z bodov K, L, M ležia vnútri strán trojuholníka a zvyšné ležia mimo strán).

□

3.3 Použitie postupu pri úlohách MMO

Pomocou Gröbnerových báz je možné dokázať množstvo základných viet a tvrdení elementárnej geometrie, ako to urobili Kapur [9] alebo Kutzler so Stifterom [8]. Otázka je, či tento prístup bude úspešný aj pri zložitejších zadaniach.

Už pri jednoduchých zadaniach sa veľmi často stane, že tvrdenie bez doplňujúcich podmienok nedokážeme (príklady 3.7 a 3.8). Veta 3.3 nám zabezpečí, že vhodná doplňujúca podmienka bude (ak existuje) v lexikografickej Gröbnerovej báze a dáva algoritmus na jej nájdenie. V konkrétnych

prípadoch by sme sa však nemali uspokojiť len s tým, že podmienku uvedieme. Môže sa stať, že pridaná podmienka vylučuje špeciálny prípad, ktorý zadanie pripúšťa. Potom musíme tento prípad osobitne prešetriť (či už pomocou Gröbnerových báz alebo bez nich).

Môže sa dokonca stať, že podmienka, ktorú určíme z vygenerovanej bázy, vylučuje všeobecný prípad okrem nejakého špeciálneho prípadu (nemôže vylučovať úplne všetky prípady, pretože polynóm, ktorý ju reprezentuje, nepatrí do $\mathrm{Rad}\,\langle P\rangle$ – podľa toho sme ho z bázy vybrali). Pridaním takejto podmienky tak dokážeme tvrdenie len pre tento špeciálny prípad.

Ak teda chceme byť dôslední, musíme pri každej doplňujúcej podmienke určiť, akú geometrickú situáciu interpretuje (a či si môžeme dovoliť pridať ju do predpokladov). To môže byť pri polynómoch veľkých stupňov (pod stupňom polynómu rozumieme maximum spomedzi stupňov jeho termov v zmysle (2.2)) zložité.

Ďalšou prekážkou je, že výpočet Gröbnerovej bázy je časovo veľmi náročný. Pri veľkom počte premenných a vysokých stupňoch termov nemusí algoritmus v rozumnom čase skončiť. Veľmi záleží na zvolenom usporiadaní termov. V praxi pri lexikografickom usporiadaní, ktoré vyžaduje veta 3.3, je časová náročnosť výpočtu bázy niekoľkonásobne väčšia ako pri stupňovom usporiadaní (vo väčšine prípadov, nie vo všeobecnosti). V prípade, že sa nám nepodarí získať lexikografickú Gröbnerovu bázu pre $\langle P, tz-1\rangle$ a získame iba stupňovú, môžeme len dúfať, že v nej vhodnú podmienku nájdeme (oprieť o vetu 3.3 sa nemôžeme).

Keď sme si uvedomili možné ťažkosti, poďme Kapurovu metódu vyskúšať na úlohách Medzinárodných matematických olympiád (ďalej len MMO). Súťaž MMO prebieha každoročne od roku 1959 (s výnimkou roku 1980). Toto leto sa tak uskutoční v poradí 45. MMO. Súťaž je určená pre nevysokoškolských študentov do 20 rokov. Každá krajina môže na MMO vyslať družstvo 6 súťažiacich. Počet účastníkov býva veľký (400 až 500), úlohy sú náročné, aby bolo možné určiť víťazov. Každý rok spomedzi šiestich riešených úloh zväčša dve bývajú z geometrie. Tieto budú dobrou skúškou pre metódu riešenia pomocou Gröbnerových báz.

Samozrejme, nie všetky geometrické úlohy z MMO možno skúsiť riešiť naším prístupom. Mnohé nie sú dôkazové (úlohy typu *nájdite . . .* , *určte . . .* , *zostrojte . . .*). Medzi úlohami je aj veľa takých, v ktorých sa má dokázať nejaká nerovnosť – tie tiež nemôžeme riešiť (dokazované tvrdenie sa nedá napísať v tvare $t = 0$, kde t je polynóm). Medzi úlohami ostatných 20 ročníkov MMO (od roku 1984 do 2003) tak ostane 17 tých, ktoré sa dajú prepísať do tvaru (3.4). Štyri z nich sú v tvare ekvivalencie a jedna má dve časti. Spolu sa teda pokúsime dokázať Kapurovou metódou 22 geometrických implikácií z MMO.

Výsledok nášho pokusu ukazuje tabuľka 3.1. Príklady sú zoradené chronologicky. Jednotlivé stĺpce udávajú: n – počet zavedených premenných (bez umelej premennej z), $|P|$ – počet predpokladov, p – stupne polynómov reprezentujúcich predpoklady, t – stupeň polynómu reprezentujú-

Príklad	n	$\|P\|$	p	t	$<$	$\|G\|$	$\sum\|g_i\|$	podmienka
84/4 $\Rightarrow$	6	4	2	2	L	16	141	$(y-c_y)(xd_y+d_y+c_yx-c_y)$
84/4 $\Leftarrow$	6	4	2	2	L	8	46	c_x-x
85/1	6	4	2 , 6	4	–			
85/5	10	7	2	2	D	16	237	–
87/2	9	7	2	2	D	90	1242	$\ell(2a_x-1)(\ell-1)$
92/4	8	6	2 , 3	2	L	18	164	$d(d-m)(d+m)$
93/2(*a*)	4	2	3 , 4	4	D	7	54	$(a-x-b+ay-bx),(a+y-b+yb+ax)$
93/2(*b*)	7	5	2 , 4	2	D	76	3565	$-by-2bya+2av_yy-a^2x-a^2+b^2x+b^2$
94/2 $\Rightarrow$	7	5	2	2	L	11	46	$(q-1)(q+1)$
94/2 $\Leftarrow$	7	5	2	2	L	19	187	$(e_yb+q+1)^2+e_y^2$
95/1	10	7	2 , 3	2	D	40	2385	$pr(x-s+r)$
96/2	9	6	2 , 64	2	–			
97/2	8	5	2	8	–			
98/1 $\Rightarrow$	5	3	2	4	D	9	42	d_yc_y
98/1 $\Leftarrow$	5	3	2	2	D	10	76	$(c_y-y)^2+(d_x-1)^2$
99/5	10	8	2	2	–			
00/1	7	5	2 , 3	1	L	7	24	$a-b$
00/6	22	20	2	2	–			
02/2	10	9	2	6	D	89	2769	–
03/3	8	3	4	2	D	5	5595	–
03/4 $\Rightarrow$	11	9	2 , 6	2	–			
03/4 $\Leftarrow$	12	10	2	6	–			

Tabuľka 3.1: *Výsledky použitia Gröbnerových báz pri úlohách MMO*

ceho dokazované tvrdenie, $<$ – typ usporiadania, pri ktorom sa podarilo vygenerovať Gröbnerovu bázu, $|G|$ – počet polynómov vo vygenerovanej báze, $\sum|g_i|$ – počet termov vo všetkých polynómoch bázy (táto hodnota charakterizuje veľkosť nájdenej bázy lepšie ako $|G|$). V poslednom stĺpci je vhodná doplňujúca podmienka, ktorú sa podarilo vo vygenerovanej Gröbnerovej báze nájsť. Presné znenia úloh, prepísané predpoklady a tvrdenia aj vygenerované Gröbnerove bázy možno nájsť v elektronickej prílohe tejto práce (spolu s príkladmi 3.6, 3.7 a (3.14)). Bázy boli generované programom `Maple`.

Ani v jednom prípade sa úlohu nepodarilo vyriešiťbez doplňujúcich podmienok. Z 22 prípadov len v šiestich sa podarilo vygenerovať lexikografickú bázu. V takom prípade sa vždy našla vhodná

<table>
<tr><td rowspan="4">22</td><td colspan="2">6
GB–lex</td><td>6
našla sa podmienka ✓</td></tr>
<tr><td rowspan="3">16
<s>GB–lex</s></td><td rowspan="2">9
GB–deg</td><td>6
našla sa podmienka ✓</td></tr>
<tr><td>3 nenašla sa podmienka ✗</td></tr>
<tr><td>7
<s>GB–deg</s> ✗</td></tr>
</table>

GB–lex: podarilo sa vygenerovať lexikografickú Gröbnerovu bázu,
GB–deg: podarilo sa vygenerovať stupňovú Gröbnerovu bázu,
✓: vyriešené úlohy, ✗: nevyriešené úlohy.

Tabuľka 3.2: *Prehľad úspešnosti metódy pri úlohách MMO.*

doplňujúca podmienka. Vo zvyšných 16 prípadoch sa 9-krát podarilo vygenerovať stupňovú bázu. šesťkrát sa v takom prípade v báze našla vhodná doplňujúca podmienka, trikrát nie. 7-krát sa nepodarilo vygenerovať žiadnu bázu. Prehľadne zachytáva výsledky tabuľka 3.2.

Pritom vhodných doplňujúcich podmienok sa často ponúkalo viacej. Mnohé z nich boli ťažko interpretovateľné, do tabuľky 3.1 sme vybrali tie najjednoduchšie analyzovateľné. Väčšina z nich predstavuje degenerované alebo špeciálne prípady. Nájdu sa aj také, ktoré sú nulové pre komplexné hodnoty premenných (druhé implikácie príkladov 98/1 a 94/2).

V oboch častiach príkladu 93/2 a v prvej implikácii príkladu 84/4 sú doplňujúce podmienky ťažšie čitateľné. Pri detailnejšom skúmaní možno zistiť, že tieto podmienky reprezentujú geometrické rozloženie, ktoré zadanie nepripúšťa. V báze sa objavili, pretože predpoklady v P vystihujú namiesto situácie zo zadania všeobecnejšiu situáciu. (Napríklad v 93/2 vystihujú aj bod D, ktorý leží mimo trojuholníka ABC a spĺňa ostatné zadané podmienky. V zadaní je ale dané, že bod leží vnútri trojuholníka – pozri elektronickú prílohu).

Z tabuliek vidieť, že najväčším nedostatkom je malá rýchlosť výpočtu Gröbnerovej bázy (bázu sa podarilo vygenerovať v 68% prípadov, z toho lexikografickú iba v 27% prípadov). Naopak, v prípade, že sa bázu podarí vygenerovať, dosahuje metóda výborné výsledky (na našom teste 100% v prípade vygenerovania lexikografickej bázy a 67% v prípade stupňovej).

Ostáva skonštatovať, že Kapurova metóda sa dá úspešne použiť aj pri náročných úlohách.

Kapitola 4

Iné aplikácie

Gröbnerove bázy sa dajú použiť v mnohých situáciách. Podrobne sme si ukázali ich využitie pri dôkazoch v geometrii. Dotknime sa okrajovo ďalších troch aplikácií, ktorými sú počítanie vo faktorových okruhoch, riešenie sústav polynomických rovníc a výpočet najväčšieho spoločného deliteľa polynómov viacerých premenných. K týmto problémom sa dá pristupovať aj bez Gröbnerových báz. V každom prípade, je zaujímavé ukázať si ich výhody a porovnať ich s inými postupmi.

4.1 Počítanie vo faktorových okruhoch

Vďaka tomu, že v okruhu $\mathbb{F}[\mathbf{x}]$ je redukcia podľa Gröbnerovej bázy G kanonickou funkciou, máme pre každý polynóm určeného reprezentanta, ktorý leží v tej istej triede rozkladu $\mathbb{F}[\mathbf{x}]$ podľa $\langle G \rangle$. Reprezentujúce polynómy sú ireducibilné modulo G a tvoria (ich triedy) faktorový okruh $\mathbb{F}[\mathbf{x}]/\langle G \rangle$.

V tomto okruhu je jednoduché vykonávať základné operácie sčítania a násobenia. Súčet je zdedený z okruhu $\mathbb{F}[\mathbf{x}]$ (súčet dvoch ireducibilných polynómov je opäť ireducibilný modulo G, lebo neobsahuje žiadny redukovateľný term). Súčin vypočítame tak, že polynómy vynásobíme a výsledok zredukujeme cez G na polynóm ireducibilný modulo G.

Podstatnejšie je, že faktorový okruh možno zároveň chápať ako vektorový priestor. Presnejšie, je to podpriestor vektorového priestoru $\mathbb{F}[\mathbf{x}]$, ktorého báza je $\mathbb{T}_{\mathbf{x}}$ (nakoľko sčítanie a zrejme aj násobenie koeficientom z $\mathbb{F}$ v $\mathbb{F}[\mathbf{x}]/\langle G \rangle$ je to isté ako v $\mathbb{F}[\mathbf{x}]$). Z Gröbnerovej bázy možno ľahko určiť (vektorovú) bázu priestoru $\mathbb{F}[\mathbf{x}]/\langle G \rangle$. Stačí z $\mathbb{T}_{\mathbf{x}}$ (ako z bázy priestoru $\mathbb{F}[\mathbf{x}]$) vybrať tie termy, ktoré patria do priestoru $\mathbb{F}[\mathbf{x}]/\langle G \rangle$ (t. j. sú ireducibilné modulo G). Bázou je teda množina

$$U = \{[u] \ : \ u \in \mathbb{T}_{\mathbf{x}}, \ \forall g \in G \ \mathrm{ht}(g) \nmid u\} \ . \tag{4.1}$$

Naozaj, každý jej prvok je ako polynóm ireducibilný modulo G (nedá sa redukovať žiadnym

vedúcim termom z G) a každý iný term (mimo U) sa redukovať dá (existuje vedúci term v G, ktorý ho delí). Množinu U vieme priamo vypísať, keď poznáme Gröbnerovu bázu. Tento výsledok korešponduje so známym faktom z okruhu polynómov jednej premennej, že rozkladové pole

$$\mathbb{F}[x]/\langle p\rangle = \left\{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \;:\; a_i \in \mathbb{F}\right\},$$

kde $p \in \mathbb{F}[x]$ je nerozložiteľný polynóm stupňa n, je vektorový priestor dimenzie n s bázou $\{[1],[x],\ldots,[x^{n-1}]\}$.

Z množiny U vieme tiež určiť, či je priestor $\mathbb{F}[\mathbf{x}]/\langle G\rangle$ konečnorozmerný. Stačí sa pozrieť na konečnosť U. To bude užitočné v ďalšej podkapitole. Teraz si ukážme, ako možno pomocou Gröbnerovej bázy a množiny U spočítať vo faktorovom okruhu inverzný prvok k danému prvku (ak existuje). Rovnaký typ konštrukcie budeme potrebovať aj neskôr.

Príklad 4.1. Uvažujme množinu $G = \{x^2 + y + 1, y^3 + x + 1\} \subset \mathbb{Q}[x,y]$. Je to Gröbnerova báza vzhľadom na $<_D$ (stačí použiť vety 2.14 a 2.8). Podľa (4.1) máme pre vektorový priestor $\mathbb{Q}[x,y]/\langle G\rangle$ bázu

$$U = \left\{[1],[x],[y],[xy],[y^2],[xy^2]\right\}.$$

Chceme nájsť inverzný prvok povedzme k $[y]$. Keďže inverzný prvok je tiež prvkom priestoru s bázou U, dá sa napísať (ak existuje) v tvare

$$a_1[1] + a_2[x] + a_3[y] + a_4[xy] + a_5[y^2] + a_6[xy^2].$$

Stačí nájsť správne koeficienty a_i. Aby bol tento prvok inverzným k $[y]$, musí trieda polynómu

$$p = y(a_1 + a_2 x + a_3 y + a_4 xy + a_5 y^2 + a_6 xy^2) - 1.$$

byť $[0]$, t. j. $\mathrm{Red}(p,G) = 0$. Redukovaním pritom dostaneme

$$\mathrm{Red}(p,G) = (-a_5 + a_6 - 1) + (-a_5 - a_6)x + (a_1 + a_6)y + a_2 xy + a_3 y^2 + a_4 xy^2,$$

Musí teda platiť

$$-a_5 + a_6 = 1, \quad -a_5 - a_6 = 0, \quad a_1 + a_6 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4 = 0.$$

Riešením tejto sústavy dostaneme $a_1 = -1/2$, $a_2 = a_3 = a_4 = 0$, $a_5 = -1/2$, $a_6 = 1/2$. Hľadaným inverzný prvok je preto

$$[y]^{-1} = \frac{1}{2}[xy^2] - \frac{1}{2}[y^2] - \frac{1}{2}.$$

□

4.2 Riešenie sústavy polynomických rovníc

Sústreďme sa teraz na problém riešenia sústavy polynomických rovníc. Konkrétne uvažujme systém rovníc

$$p_i(x_1, \ldots, x_n) = 0\,, \quad 1 \leq i \leq k\,, \tag{4.2}$$

kde $P = \{p_1, \ldots, p_n\} \subset \mathbb{F}[\mathbf{x}]$. Zaujímame sa o riešenia v algebraickom rozšírení poľa $\mathbb{F}$. Každé riešenie tejto sústavy budeme nazývať *riešením množiny* P. Ľahko možno nahliadnuť, že ak $\langle P \rangle = \langle G \rangle$, tak množiny P a G majú tie isté riešenia. Ak G je Gröbnerova báza pre $\langle P \rangle$, dá sa očakávať, že o týchto riešeniach získame viac informácií z G ako z P.

Priamo z Gröbnerovej bázy možno určiť, či sústava (4.2) má nejaké riešenie. Podľa vety 3.2 stačí overiť, či $1 \in \langle G \rangle$, t. j. či $1 \in G$. Ak v Gröbnerovej báze (normovanej) je 1, potom sústava nemá riešenie, inak ho má.

Nezastavíme sa však len pri otázke riešiteľnosti. Priamo z G možno dokonca určiť konečnosť množiny riešení vďaka nasledujúcej vete.

Veta 4.1. Nech G je Gröbnerova báza pre $\langle P \rangle \subseteq \mathbb{F}[\mathbf{x}]$ a nech H je množina

$$H = \{\mathrm{ht}(g) \,:\, g \in G\}\ . \tag{4.3}$$

Potom sústava (4.2) má konečne veľa riešení práve vtedy, keď pre každé $i = 1, \ldots, n$ existuje $m \in \mathbb{N}$ také, že $x_i^m \in H$.

□

Dôkaz možno nájsť napríklad v [6]. Zakladá sa na skutočnosti, že vedúce termy z G spĺňajú vlastnosť z vety práve vtedy, keď množina U z (4.1) je konečná, čiže keď $\mathbb{F}[\mathbf{x}]/\langle G \rangle$ je ako vektorový priestor konečnorozmerný.

Pritom tento silný výsledok nemôže závisieť na zvolenom usporiadaní termov, podľa ktorého sme Gröbnerovu bázu generovali. Od usporiadania nezávisí ani mohutnosť množiny U, keďže dimenzia $\mathbb{F}[\mathbf{x}]/\langle G \rangle$ je nezávislá na usporiadaní termov.

Príklad 4.2. Pre Gröbnerovu bázu $G = \{x^2 + y + 1, y^3 + x + 1\}$ z príkladu 4.1 máme podľa (4.3) $H = \{x^2, y^3\}$. Keďže $1 \notin H$, sústava prislúchajúca ku G má riešenie. Podľa vety 4.1 je jej riešení konečne veľa. Vygenerovať pre G môžeme aj Gröbnerovu bázu vzhľadom na lexikografické usporiadanie. dostaneme

$$G_L = \left\{y^6 + 2y^3 + y + 2, x + y^3 + 1\right\} \qquad \text{a} \qquad H_L = \left\{x, y^6\right\}\ ,$$

z čoho možno o konečnosti počtu riešení G vyvodiť rovnaké závery.

□

Predchádzajúci príklad ukazuje dôležitý rozdiel medzi jednotlivými usporiadaniami. V lexikografickej báze sa totiž nachádza polynóm p o jednej premennej y. Každé riešenie G vynuluje aj tento polynóm, takže máme informáciu o tom, akú hodnotu môže v riešení nadobúdať y (musí to byť koreň polynómu p). Zo stupňovej bázy takúto informáciu nemáme.

Na druhej strane, vygenerovať lexikografickú bázu je oproti stupňovej náročnejšie. Je preto dobré skúsiť zistiť informáciu o riešeniach aj zo stupňovej bázy (resp. nezávisle na usporiadaní). Presnejšie, zaujíma nás, ako pomocou G určiť polynóm $p \in \mathbb{F}[\tilde{x}]$ ($\tilde{x}$ je niektorá z premenných) taký, že všetky riešenia G (presnejšie ich zložky na mieste $\tilde{x}$) sú aj koreňmi p.

Ak taký existuje (v prípade konečnosti počtu riešení je jeho existencia zrejmá), potom existuje aj v $\langle G \rangle$ (vďaka vete 3.1). V príklade 4.1 sme videli, že ak polynóm $p = \Sigma a_i t_i$ patrí do $\langle G \rangle$, podmienka $\mathrm{Red}(p, G) = 0$ vedie k systému lineárnych rovníc, ktorého vyriešením získame hodnoty a_i. To nám dáva návod, ako nájsť polynóm p najmenšieho stupňa, ktorý leží v $\langle G \rangle \cap \mathbb{F}[\tilde{x}]$.

Začneme tak, že skúsime nájsť polynóm stupňa 0, ak sa nám to nepodarí, skúsime to zo stupňom 1, atď. Pritom polynóm stupňa k hľadáme v tvare

$$p = \sum_{i=0}^{k} a_i \tilde{x}^i \,, \qquad p \in \langle G \rangle \cap \mathbb{F}[\tilde{x}] \,,$$

kde a_i sú neznáme. Postupom z príkladu 4.1 sa ich pokúsime určiť (ak hľadaný polynóm stupňa k existuje, musí sa nám to podariť).

Keď tento postup zopakujeme pre každú premennú x_i, v prípade konečnosti počtu riešení G získame n polynómov, každý v inej premennej, pričom medzi koreňmi každého budú všetky hodnoty danej premennej, ktoré sa vyskytujú v riešeniach G. Samozrejme, nie všetky n-tice, ktoré môžeme z koreňov týchto polynómov vyrobiť, sú riešeniami G.

Ak vieme niektorý z polynómov, povedzme $p \in \langle G \rangle \cap \mathbb{F}[x_1]$, rozložiť na $p = q_1^{e_1} \cdots q_m^{e_m}$, potom je lepšie postupne uvažovať Gröbnerove bázy pre $\langle G, q_j \rangle$, $j = 1, \ldots, m$. Pre každé j získame iné (menšie) jednopremenné polynómy v $x_2, \ldots, x_n$. Takýmto postupom môžeme presne určiť všetky riešenia G, potrebujeme však na to vedieť nájsť všetky korene polynómov jednej premennej (aby boli jednotlivé q_j lineárne). Našli sme tak postup (i keď niekedy nepraktický) ako P riešiť pomocou Gröbnerovej bázy vygenerovanej v ľubovoľnom usporiadaní (v prípade, že počet riešení P je konečný).

Ak pre P získame redukovanú Gröbnerovu bázu G vzhľadom na lexikografické usporiadanie, predchádzajúca situácia sa do značnej miery zjednoduší. Opäť predpokladajme, že P (teda aj G)

má konečne veľa riešení. Potom priamo v G musí podľa vety 4.1 existovať polynóm g_n majúci vedúci term $x_n^{m_n}$ a teda $g_n \in \mathbb{F}[x_n]$ (všetky jeho termy sú $<_L x_n^{m_n}$, teda nemôžu obsahovať inú premennú). Podobne musí G obsahovať pre každé $i = n, n-1, \ldots, 1$ polynóm g_i majúci vedúci term $x_i^{m_i}$, ktorý leží v $\mathbb{F}[x_i, x_{i+1}, \ldots x_n]$.

Pôvodný algoritmus hľadania riešení G môžeme teda zopakovať bez toho, aby sme museli polynómy jednej premennej hľadať. Stačí postupne brať jednotlivé korene g_n a dosadzovať ich do ostatných polynómov. Polynóm g_{n-1} sa tak stane jednopremenným a aj v ostatných g_i sa zmenší počet premenných o 1. Opakovaním postupu tak nájdeme prípustné riešenia G.

Nie všetky nájdené riešenia sú nutne riešeniami celej G. Sú len riešeniami $\{g_1, \ldots, g_n\}$, ktoré nemusia tvoriť celú bázu. Aby sme tento nedostatok odstránili, stačí zmeniť výpočet tak, že každý koreň g_n dosadíme nie iba do polynómov g_i, ale do všetkých polynómov. Zo vzniknutých polynómov potom vezmeme nie g_{n-1}, ale NSD všetkých polynómov v $G \cap \mathbb{F}[x_{n-1}]$. (Na začiatku bol v báze iba jeden polynóm z $\mathbb{F}[x_n]$, lebo bola redukovaná. Nebolo teda treba počítať NSD.) Rovnako budeme postupovať aj ďalej.

Pomerne jednoducho možno dokázať (napríklad v [10]), že

$$\langle G \rangle \cap \mathbb{F}[x_k, \ldots, x_n] = \langle G \cap \mathbb{F}[x_k, \ldots, x_n] \rangle \ .$$

Takže uvedený postup je dobrý v tom zmysle, že v $\langle G \rangle \cap \mathbb{F}[x_k, \ldots, x_n]$ nemôže byť jednoduchšia báza, t. j. taká množina, ktorá by dala menej riešení na preverovanie, ako $G \cap \mathbb{F}[x_k, \ldots, x_n]$.

Sú možné ďalšie zlepšenia nášho algoritmu. Taktiež možno kombinovať použitie Gröbnerových báz s inými metódami na riešenie sústavy polynomických rovníc a porovnávať jednotlivé prístupy. To už je ale nad rámec tejto práce. Uspokojíme sa s tým, že sme uviedli, ako možno Gröbnerove bázy využiť v tejto oblasti a poukázali tak na ich dôležitosť.

4.3 Výpočet najväčšieho spoločného deliteľa

Posledná aplikácia, ktorú si ukážeme, bude výpočet NSD pre dva alebo viac polynómov viacerých premenných. I keď nie je veľmi praktická, ilustruje význam Gröbnerových báz. Autormi postupu, ktorý uvedieme, sú Gianni a Trager [11], ktorí tiež publikovali postup, ako možno pomocou Gröbnerových báz faktorizovať polynómy viacerých premenných.

Základom výpočtu NSD je nasledujúca veta.

Veta 4.2. Nech $f_1, \ldots, f_m, g \in \mathbb{F}[y, \mathbf{x}]$ sú primitívne v premennej y (t. j. koeficienty pri mocninách y sú nesúdeliteľné) a $\mathbb{I}$ je maximálny ideál v $\mathbb{F}[\mathbf{x}]$ (t. j. $\mathbb{I}$ nie je obsiahnutý v žiadnom inom ideále rôznom od $\mathbb{I}$ a $\mathbb{F}[\mathbf{x}]$). Nech platí

$$\langle f_1, \ldots, f_m, \mathbb{I} \rangle = \langle 1 \rangle \ , \qquad \exists i,\ 1 \leq i \leq m, \text{ také, že } \langle \mathrm{hc}_y(f_i g), \mathbb{I} \rangle = \langle 1 \rangle$$

a nech $G_{(k)}$ je redukovaná Gröbnerova báza ideálu

$$\langle f_1 g, \ldots, f_m g, \mathbb{I}^k \rangle$$

vzhľadom na usporiadanie termov $<_D$. Potom pre $k > (\deg(g))^2$ je v $G_{(k)}$ jediný polynóm $\tilde{g}$, ktorý má najmenší stupeň. Tento polynóm je asociovaný s g.

□

Ak teda chceme nájsť NSD polynómov $p_1, \ldots, p_m \in \mathbb{F}[y, \mathbf{x}]$, musíme zvoliť ideál $\mathbb{I} \subset \mathbb{F}[\mathbf{x}]$ tak, aby pre niektoré i platilo $\langle \mathrm{hc}_y(p_i), \mathbb{I} \rangle = \langle 1 \rangle$. (Jednotlivé polynómy p_j predstavujú $f_j g$ z vety, g je hľadaný NSD.) V praxi je dobré zvoliť $\mathbb{I}$ v tvare

$$\mathbb{I} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle \ , \qquad a_i \in \mathbb{F} \, .$$

Následne vypočítame Gröbnerovu bázu (vzhľadom na $<_D$) pre $\langle p_1, \ldots, p_m, \mathbb{I}^k \rangle$, kde k je väčšie ako očakávaný stupeň g. Polynóm najmenšieho stupňa v báze (ak sú splnené všetky predpoklady vety 4.2) bude hľadaný NSD.

Otázkou, ako zvoliť $\mathbb{I}$, aby sme zabezpečili splnenie predpokladov vety, sa zaoberať nebudeme. Ukážme si radšej pre názornosť jeden príklad.

Príklad 4.3. Hľadajme NSD polynómov $p_1, p_2 \in \mathbb{F}[x, y, z]$, kde

$$\begin{aligned} p_1 &= xz^3 + x^2 z + xz^2 + z^3 + x^2 + 2xz + x + z \, , \\ p_2 &= 2xz^2 - yz^2 + 2x^2 - xy + z^2 + 3x - y + 1 \, . \end{aligned}$$

Zvoľme $\mathbb{I} = \langle y, z \rangle$. Potom

$$\mathbb{I}^5 = \langle y^5, y^4 z, y^3 z^2, y^2 z^3, y z^4, z^5 \rangle \ .$$

Gröbnerovu bázu pre $\langle p_1, p_2, \mathbb{I}^5 \rangle$ vzhľadom na $<_D$ tvoria polynómy

$$z^2 + x + 1 \, , \quad x^2 z + 2xz + z \, , \quad x^2 y + 2xy + y \, , \quad x^3 + 3x^2 + 3x + 1 \, , \quad xy^2 z + y^2 z \, ,$$
$$xy^3 + y^3 \, , \quad y^4 z \, , \quad y^5 \, .$$

Polynóm najmenšieho stupňa v báze je $g = z^2 + x + 1$. Keďže máme

$$p_1 = (xz + x + z)(z^2 + x + 1) \, , \qquad p_2 = (2x - y + 1)(z^2 + x + 1) \, ,$$

g je naozaj hľadaný NSD.

□

Podrobnosti týkajúce sa hľadania NSD a dôkaz vety 4.2 možno nájsť v [11].

Záver

Ukázali sme si, ako možno vyriešiť problém patrenia do ideálu v okruhu polynómov viacerých premenných. Hlavnou myšlienkou bolo zavedenie pojmu Gröbnerových báz. Pritom sme nepotrebovali žiadne hlbšie poznatky z algebry, vystačili sme si so základnými pojmami.

Uviedli sme, ako možno Gröbnerove bázy využiť vo viacerých elementárnych oblastiach. Kľúčovou sa ukázala byť Hilbertova veta o nulách. Prínos predloženej teórie sme demonštrovali na riešení dôkazových geometrických úloh z Medzinárodnej matematickej olympiády a načrtli sme algoritmy na riešenie sústav polynomických rovníc a nájdenie najväčšieho spoločného deliteľa polynómov viacerých premenných.

Gröbnerove bázy a Buchbergerov algoritmus majú fundamentálnu úlohu pri symbolických výpočtoch. Úspešne sa dajú použiť pri celej triede problémov vyššej matematiky. Ďalšie aplikácie vyžadujú hlbšie teoretické zázemie a boli by nad rámec tejto práce.

Použité algoritmy

Označenie

$\mathrm{vyber}(M)$	funkcia, ktorá vyberie niektorý prvok množiny M
$\|G\|$	počet prvkov množiny G
g_i	i-ty prvok množiny G
$\leftarrow$	priradenie
#	komentár k algoritmu

Algoritmus 1. Úplná redukcia p modulo Q.

procedure $\mathrm{Red}(p, Q)$
    # *K danému* $p \in \mathbb{F}[\mathbf{x}]$ *a* $Q \subset \mathbb{F}[\mathbf{x}]$ *nájde* q *taký, že* $p \mapsto_Q^* q$.
    $r \leftarrow p$
    $q \leftarrow 0$
    # *Najprv redukuje vedúci člen. Ak ten je ireducibilný modulo* Q,
    # *pridá ho k výsledku a ďalej redukuje bez neho.*
    # *Množina* $R_{r,Q}$ *je množina tých polynómov, ktoré redukujú vedúci člen* r.
    while $r \neq 0$ **do** {
        while $R_{r,Q} \neq \emptyset$ **do** {
            $f \leftarrow \mathrm{vyber}(R_{r,Q})$
            $r \leftarrow r - \frac{\mathrm{M}(r)f}{\mathrm{M}(f)}$ }
        $q \leftarrow q + \mathrm{M}(r)$
        $r \leftarrow r - \mathrm{M}(r)$ }
    return(q)
end

Algoritmus 2. Buchbergerov algoritmus pre nájdenie Gröbnerovej bázy.

procedure $\mathrm{Gbaza}(P)$
 # K danej množine $P \subset \mathbb{F}[\mathbf{x}]$ nájde G takú, že $\langle G \rangle = \langle P \rangle$ a G je Gröbnerova báza.
$G \leftarrow P$; $k \leftarrow |G|$
$B \leftarrow \{(i,j) \ : \ 1 \leq i < j \leq k\}$
while $B \neq \emptyset$ **do** {
$(i,j) \leftarrow \mathrm{vyber}(B)$; $B \leftarrow B - \{(i,j)\}$
$h \leftarrow \mathrm{Red}(\mathrm{S}(g_i, g_j), G)$
if $h \neq 0$ **then** {
$G \leftarrow G \cup \{h\}$; $k \leftarrow k+1$
$B \leftarrow B \cup \{(i,k) \ : \ 1 \leq i < k\}$ } }
return(G)
end

Algoritmus 3. Konštrukcia redukovanej bázy ideálu.

procedure $\mathrm{RedSet}(E)$
 # K danej množine $E \subset \mathbb{F}[\mathbf{x}]$ nájde $\tilde{E}$ takú, že $\langle E \rangle = \langle \tilde{E} \rangle$ a $\tilde{E}$ je redukovaná.
 # E nemusí byt'nutne Gröbnerova báza. Najprv odstráni prebytočné prvky.
$R \leftarrow E$; $P \leftarrow \emptyset$
while $R \neq \emptyset$ **do** {
$h \leftarrow \mathrm{vyber}(R)$; $R \leftarrow R - \{h\}$
$h \leftarrow \mathrm{Red}(h, P)$
if $h \neq 0$ **then** {
$Q \leftarrow \{q \in P \ : \ \mathrm{ht}(h) \mid \mathrm{ht}(q)\}$
$R \leftarrow R \cup Q$
$P \leftarrow P - Q \cup \{h\}$ } }
 # Zistí, či každý prvok je redukovaný modulo ostatnými
$\tilde{E} \leftarrow \emptyset$; $S \leftarrow P$
foreach $h \in P$ **do** {
$h \leftarrow \mathrm{Red}(h, S - \{h\})$
$\tilde{E} \leftarrow \tilde{E} \cup \{h\}$ }
return($\tilde{E}$)
end

Algoritmus 4. Riešenie úlohy (3.4).

procedure $\mathrm{Dokaz}(P, t)$
    # K množine predpokladov $P \subset \mathbb{F}[\mathbf{x}]$ *a tvrdeniu* $t \in \mathbb{F}[\mathbf{x}]$ *nájde*
    # vhodnú doplňujúcu podmienku $s \in \mathbb{F}[\mathbf{x}]$.
    # Gröbnerova báza sa generuje pri usporiadaní $x_i <_L z$.
    $G \leftarrow \mathrm{RedSet}(\mathrm{Gbaza}(P \cup \{tz - 1\}))$
    if $g_1 = 1$ **then**
        return(”Tvrdenie platí bez doplňujúcich podmienok.”)
    else {
        for $i \leftarrow 1$ **to** $|G|$ **do** {
            if $g_i \in \mathbb{F}[\mathbf{x}]$ **and** $g_i \notin P$ **then** {
                if $\{1\} \neq \mathrm{RedSet}(\mathrm{Gbaza}(P \cup \{g_i z - 1\}))$ **then**
                    return(”Tvrdenie platí s doplňujúcou podmienkou $g_i \neq 0$.”) } } }
    return(”Tvrdenie neplatí so žiadnou doplňujúcou podmienkou.”)
end

Literatúra

[1] S. Mac Lane, G. Birkhoff. Algebra. Alfa Bratislava, 1974.

[2] G. Hermann. The Question of Finitely Many Steps in Polynomial Ideal Theory. In *Math. Ann. 95, p. 736-788*, 1926.

[3] B. Buchberger. An Algorithm for Finding a Basis for the Residue Class Ring of a Zero–Dimensional Polynomial Ideal. Ph.D. Thesis, Univ. of Innsbruck, Math. Inst., 1965.

[4] B. Buchberger. A Theoretical Basis for the Reduction of Polynomials to Canonical Forms. In *ACM SIGSAM Bull.*, 10(3), p. 19-29, 1976.

[5] B. Buchberger. Some Properties of Gröbner-Bases for Polynomial Ideals. In *ACM SIGSAM Bull.*, 10(4), p. 19-24, 1976.

[6] T. Becker, V. Weispfenning, H. Kredel. Gröbner Bases: A Computational Approach to Commutative Algebra. Springer-Verlag New York, 1993.

[7] B. Buchberger, F. Winkler. Miscellaneous Results on the Construction of Gröbner Bases for Polynomial Ideals. In *Tech. Rep. 137*, Univ. of Linz, Math. Inst., 1979.

[8] B. Kutzler, S. Stifter. On the Application of Buchberger's Algorithm to Automated Theorem Proving. In *Journal of Symbolic Computation*, p. 389-397, 1986.

[9] D. Kapur. Geometry Theorem Proving Using Hilbert's Nullstellensatz. In *Proc. SYMSAC'86*, p. 202-208, ACM Press, 1986.

[10] K. O. Geddes, S. R. Czapor, G. Labahn. Algorithms for Computer Algebra. Kluwer Academic Publishers, 1992.

[11] P. Gianni, B. Trager. GCD's and Factoring Multivariate Polynomials Using Gröbner Basis. In *Proc. EUROCAL'85, Vol. 2, Lecture Notes in Computer Science 204*, Springer-Verlag, 1985.

[12] W. W. Adams, P. Loustaunau. An Introduction to Gröbner Bases. In *Graduate Studies in Mathematics, Vol. 3*, AMS Providence, 1994.